

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ
ДИНАМИЧЕСКИХ СИСТЕМ И ПРОЦЕССОВ

УДК 517.97

С. Б. Доулбекова, doulbekova25@mail.ruА. Керимбеков, akl7@rambler.ru

КРСУ им. первого президента Российской Федерации Б.Н. Ельцина

**О НЕЛИНЕЙНОЙ ОПТИМИЗАЦИИ КОЛЕБАТЕЛЬНЫХ ПРОЦЕССОВ
ПРИ ОГРАНИЧЕНИИ НА УПРАВЛЕНИЯ**

В статье исследована разрешимость задачи нелинейной оптимизации колебательных процессов, описываемых интегро-дифференциальными уравнениями в частных производных с интегральным оператором Фредгольма. Исследования проводятся, когда функция внешних сил нелинейна и зависит от управляющих функций, на которые налагаются ограничения. Оценкой качества управления выбран интегральный функционал общего вида.

Установлено, что искомое оптимальное управление следует искать среди решений бесконечной системы нелинейных уравнений Фредгольма 1-го рода, разрешимость которых исследована операторными методами. Доказано, что операторное уравнение имеет бесконечно много решений. Найдены достаточные условия существования решения задачи нелинейной оптимизации.

Ключевые слова: краевая задача, обобщенное решение, интеграл энергии, функционал, граничное управление, оптимальное управление.

Введение

В данной статье рассматривается задача нелинейной оптимизации колебательных процессов, описываемых интегро-дифференциальными уравнениями с интегральным оператором Фредгольма. Особенность задачи заключается в наличии ограничений на управления, а также в немонотонной зависимости функции источника от управляющих воздействий.

С использованием операторных методов исследуется существование и структура решений возникающих интегральных уравнений, формулируются достаточные условия разрешимости задачи оптимального управления и предложен подход к построению оптимального управления.

Постановка задачи оптимизации

Рассмотрим задачу нелинейной оптимизации колебательных процессов, целью которой является найти распределенное управление $u^0(t, x) \in H(Q)$, минимизирующее интегральный функционал вида

$$J[u, t, x] = \int_0^T \int_0^1 p[t, x, u, t, x] dx dt, \quad (1)$$

из множества решений следующей краевой задачи

$$V_{tt} = V_{xx} + \lambda \int_0^T K(t, \tau) V(\tau, x) d\tau + f[t, x, u, t, x], \quad 0 < x < 1, 0 < t \leq T, \quad (2)$$

$$V(0, x) = \psi_1(x), \quad V_t(0, x) = \psi_2(x), \quad 0 < x < 1, \quad (3)$$

$$V_x(t, 0) = 0, \quad V_x(t, 1) + \alpha V(t, 1) = 0, \quad 0 < t < T, \quad (4)$$

при условии, что обобщенное решение

$$V(t, x) = \sum_{n=1}^{\infty} \left[\lambda \int_0^T R_n(t, s, \lambda) q_n(s) ds + q_n(t) \right] z_n(x), \quad (5)$$

$$q_n(t) = \psi_{1n} \cos \lambda_n t + \frac{\psi_{2n}}{\lambda_n} \sin \lambda_n t + \frac{1}{\lambda_n} \int_0^t \sin \lambda_n(t - \tau) f_n(\tau, u) d\tau, \quad (6)$$

удовлетворяет соотношению

$$V(t, x) = \xi(x), \quad (7)$$

которое является дополнительным ограничением на управление.

Здесь функции $\psi_1(x) \in H_1(0,1)$, $\psi_2(x) \in H(0,1)$, $\xi(x) \in H(0,1)$, $p[t, x, u(t, x)] \in H(Q)$ и $f[t, x, u(t, x)] \in H(Q)$ заданы, и известные функции $f[t, x, u(t, x)]$ и $p[t, x, u(t, x)]$ нелинейны по отношению управляющих функций.

В связи с тем, что на практике сталкиваются с процессами описываемых функций, имеющих разрыв, часто пользуются обобщенным решением [1,3].

Определение. Обобщенное решение краевой задачи (2)-(4) есть функция $V(t, x) \in H_1(Q)$, удовлетворяющая почти всюду уравнению (2) и условиям (3) в слабом смысле, т.е. $\forall \Phi_0(x) \in H(Q), \Phi_1(x) \in H(Q)$ выполняются равенства

$$\lim_{t \rightarrow +0} \int_0^1 V(t, x) \Phi_0(x) dx = \int_0^1 \psi_1(x) \Phi_0(x) dx, \\ \lim_{t \rightarrow +0} \int_0^1 V_t(t, x) \Phi_1(x) dx = \int_0^1 \psi_2(x) \Phi_1(x) dx,$$

а коэффициенты Фурье

$$V_n(t) = \int_0^1 V(t, x) z_n(x) dx \quad (8)$$

удовлетворяют интегральному уравнению

$$V_n(t) = \lambda \int_0^t K_n(t, s) V_n(s) ds + q_n(t), \quad (9)$$

где функция

$$K_n(t, s) = \frac{1}{\lambda_n} \int_0^t \sin \lambda_n(t - \tau) K(\tau, s) d\tau, \quad K_n(0, s) = 0 \quad (10)$$

является ядром, а функция

$$q_n(t) = \psi_{1n} \cos \lambda_n t + \frac{\psi_{2n}}{\lambda_n} \sin \lambda_n t + \frac{1}{\lambda_n} \int_0^t \sin \lambda_n(t - \tau) f_n(\tau, u) d\tau \quad (11)$$

является свободным членом линейного интегрального уравнения Фредгольма 2-го рода.

Решение задачи оптимизации

Предположим, что для управления $u^0(t, x) \in H(Q)$ выполнено равенство (7). Тогда согласно (5), из равенства

$$V(T, x) = \sum_{n=1}^{\infty} \left[\lambda \int_0^T R_n(T, s, \lambda) q_n(s) ds + q_n(T) \right] z_n(x) =$$

$$= \sum_{n=1}^{\infty} \xi_n z_n(x) = \xi(x), \quad \xi_n = \int_0^1 \xi(x) z_n(x) dx,$$

учитывая линейную независимость системы собственных функций $z_n(x)$,

относительно искомого управления $u^0(t, x) \in H(Q)$, получим систему равенств

$$\lambda \int_0^T R_n(T, s, \lambda) q_n(s) ds + q_n(T) = \xi_n, \quad (12)$$

$$\lambda \int_0^T R_n(T, s, \lambda) \left(\psi_{1n} \cos \lambda_n s + \frac{\psi_{2n}}{\lambda_n} \sin \lambda_n s + \frac{1}{\lambda_n} \int_0^s \sin \lambda_n(s - \tau) f_n(\tau, x, u) d\tau \right) ds +$$

$$+ \left(\psi_{1n} \cos \lambda_n T + \frac{\psi_{2n}}{\lambda_n} \sin \lambda_n T + \frac{1}{\lambda_n} \int_0^T \sin \lambda_n(T - \tau) f_n(\tau, x, u) d\tau \right) = \xi_n. \quad (13)$$

Учитывая, что

$$f_n(t, x, u) = \int_0^1 f(t, x, u(t, x)) z_n(x) dx,$$

имеем систему из нелинейных интегральных уравнений Фредгольма 1-го рода

$$\int_0^T \int_0^1 \frac{z_n(x)}{\lambda_n} \left\{ \sin \lambda_n(T - \tau) + \lambda \int_{\tau}^T R_n(T, s, \lambda) \sin \lambda_n(s - \tau) ds \right\} f(\tau, x, u(\tau, x)) dx d\tau =$$

$$= \xi_n - \psi_{1n} \left\{ \cos \lambda_n T + \lambda \int_0^T R_n(T, s, \lambda) \cos \lambda_n s ds \right\} -$$

$$- \frac{\psi_{2n}}{\lambda_n} \left\{ \sin \lambda_n T + \lambda \int_0^T R_n(T, s, \lambda) \sin \lambda_n s ds \right\}, \quad n = 1, 2, 3, \dots, \quad (14)$$

которые, введя обозначения

$$G_n(\tau, x, \lambda) = \frac{z_n(x)}{\lambda_n} \left\{ \sin \lambda_n(T - \tau) + \lambda \int_{\tau}^T R_n(T, s, \lambda) \frac{1}{\lambda_n} \sin \lambda_n(s - \tau) ds \right\}, n = 1, 2, 3, \dots, \quad (15)$$

$$h_n(\lambda) = \xi_n - \psi_{1n} \left\{ \cos \lambda_n T + \lambda \int_0^T R_n(T, s, \lambda) \cos \lambda_n s ds \right\} -$$

$$- \frac{\psi_{2n}}{\lambda_n} \left\{ \sin \lambda_n T + \lambda \int_0^T R_n(T, s, \lambda) \sin \lambda_n s ds \right\}, n = 1, 2, 3, \dots, \quad (16)$$

перепишем в виде

$$\int_0^T \int_0^1 G(t, x, \lambda) f(t, x, u(t, x)) dx dt = h(\lambda), \quad (17)$$

где

$$G(t, x, \lambda) = G_1(t, x, \lambda), \dots, G_n(t, x, \lambda), \dots, h(\lambda) = h_1(\lambda), \dots, h_n(\lambda), \dots. \quad (18)$$

Полагая

$$f(t, x, u(t, x)) = v(t, x), \quad (19)$$

уравнение (17) примет вид

$$\int_0^T \int_0^1 G(t, x, \lambda) v(t, x) dx dt = h(\lambda), \quad n = 1, 2, 3, \dots \quad (20)$$

Доказательство следующих лемм производится непосредственными вычислениями.

Лемма 1. Вектор $h(\lambda)$ является элементом пространства ℓ_2 .

Лемма 2. Оператор $G(u) : H(Q) \rightarrow \ell_2$, где

$$G(u) = \int_0^T \int_0^1 G(t, x, \lambda) v(t, x) dx dt.$$

На основе доказанных утверждений операторное уравнение (20) будем рассматривать в пространстве ℓ_2 . Его решение ищем в виде

$$v(t, x) = \sum_{n=1}^{\infty} G_n(t, x, \lambda) \alpha_n + \gamma = G^*(t, x, \lambda) \alpha + \gamma, \quad (21)$$

где $\alpha = \alpha_1, \dots, \alpha_n, \dots$ – неизвестный вектор пространства ℓ_2 , γ – произвольная постоянная, (21), подставив в (20), имеем соотношение

$$\int_0^T \int_0^1 G(t, x, \lambda) [G^*(t, x, \lambda) \alpha + \gamma] dx dt = h(\lambda),$$

или

$$\int_0^T \int_0^1 G(t, x, \lambda) G^*(t, x, \lambda) dx dt \cdot \alpha = h(\lambda) - \gamma \int_0^T \int_0^1 G(t, x, \lambda) dx dt. \quad (22)$$

Введя обозначение

$$M = \int_0^T \int_0^1 G(t, x, \lambda) G^*(t, x, \lambda) dx dt, \quad (23)$$

$$h(\lambda, \gamma) = h(\lambda) - \gamma \int_0^T \int_0^1 G(t, x, \lambda) dx dt,$$

уравнение (22) перепишем в виде

$$M(\lambda) \cdot \alpha = h(\lambda, \gamma). \quad (24)$$

Это равенство есть бесконечномерная линейная неоднородная система алгебраических уравнений. Для исследования ее разрешимости используем операторный метод.

Лемма 3. Вектор $h(\lambda, \gamma)$ является элементом пространства ℓ_2 .

Лемма 4. Оператор $M : \ell_2 \rightarrow \ell_2$, $M \alpha = M(\lambda) \alpha$, т.е. $\forall \alpha \in \ell_2 \Rightarrow M \alpha \in \ell_2$.

Лемма 5. Оператор $M \alpha$ является положительно - определенным.

Таким образом, линейный оператор $M \alpha$ является положительно - определенным. Тогда, согласно теореме из функционального анализа [2], существует линейный ограниченный оператор $N : \ell_2 \rightarrow \ell_2$. Поэтому из системы (24) вектор α при каждом фиксированном значении произвольной постоянной γ имеет единственное решение

$$\alpha = Nh(\lambda, \gamma) = N \left(h \lambda - \gamma \int_0^T \int_0^1 G(t, x, \lambda) dx dt \right). \quad (25)$$

Это решение, подставив в (21), получим функцию

$$v(t, x) = G^*(t, x, \lambda) N \left(h \lambda - \gamma \int_0^T \int_0^1 G(t, x, \lambda) dx dt \right) + \gamma, \quad (26)$$

которая является решением системы состоящих из интегральных уравнений (20). Тогда из формул (17) и (19) можем получить решение системы из нелинейных интегральных уравнений (17) по формуле

$$f(t, x, u(t, x)) = G^*(t, x, \lambda) N \left(h \lambda - \gamma \int_0^T \int_0^1 G(t, x, \lambda) dx dt \right) + \gamma. \quad (27)$$

Пусть функция $f[t, x, u(t, x)] \in H(Q)$ не является монотонной по функциональной переменной $u(t, x)$, т.е. условие

$$f_u[t, x, u(t, x)] \neq 0 \quad (28)$$

не выполняется. Заметим, что при этом могут быть и управления $u(t, x)$, для которых выполняется условие

$$f_u[t, x, u(t, x)] = 0. \quad (29)$$

В этом случае алгебраическое уравнение (27) при каждом фиксированном γ^* может иметь несколько решений

$$u_k(t, x) = u_k(t, x, \gamma^*) \quad k = 1, 2, 3, \dots, r_{\gamma^*}, \quad (30)$$

где r_{γ^*} может быть конечным и бесконечным счетным числом. Отметим, что множество, состоящее из элементов вида (30), образует фактор-множество

$$u_{\gamma^*}(t, x) = u_1(t, x, \gamma^*), \dots, u_{r_{\gamma^*}}(t, x, \gamma^*). \quad (31)$$

Таким образом, установлено, что существует бесконечное множество управлений $u(t, x)$, при которых выполняется условие (5). Теперь из элементов этого множества выделим управление $u^0(t, x)$, такое, что функционал (1) будет принимать минимальное возможное значение.

О разрешимости задачи минимизации функционала в случае, когда $f(t, x, u(t, x))$ не является монотонной функцией. В этом случае искомое управление $u^0(t)$ следует искать среди элементов фактор-множеств (31), где γ^* – произвольная постоянная.

Сначала берем функцию

$$u_1(t, x) = u_1(t, x, \gamma). \quad (32)$$

Ее подставим в функционал (3.2.1) и получим функцию

$$\Phi_1(\gamma) = J[u_1(t, x)] = \int_0^T p[t, x, u_1(t, x)] dt = \int_0^T p[t, x, u_1(t, x, \gamma)] dt, \quad (33)$$

которую исследуем на экстремум. Точки минимума функции $\Phi_1(\gamma)$ находим из условий:

$$\begin{aligned}\Phi'_1(\gamma) &= \beta \int_0^T \int_0^1 p_u \left[t, x, u_1 \quad t, x, \gamma \right] u_{1\gamma} \quad t, x, \gamma \quad dx dt = 0, \\ \Phi''(\gamma) &= \beta \int_0^T \int_0^1 p_{uu} \left[t, x, u_1 \quad t, x, \gamma \right] u_{1\gamma} \quad t, x, \gamma \quad^2 + \\ &+ p_u \left[t, x, u \quad t, x, \gamma \right] u_{1\gamma\gamma} \quad t, x, \gamma \quad dx dt \geq 0.\end{aligned}\tag{34}$$

Пусть $\gamma = \gamma^0$ является единственным решением задачи (34). Это значение подставим в (32), получим оптимальное управление

$$u_1^0(t, x) = u_1 \quad t, x, \gamma^0,$$

для которого имеет место соотношение

$$J \left[u_1^0 \quad t, x \right] = J \left[u_1 \quad t, x, \gamma^0 \right] \leq J \left[u_1 \quad t, x, \gamma \right].\tag{35}$$

Предположим теперь, что задача (34) имеет несколько решений $\gamma_1, \dots, \gamma_m$. В этом случае, согласно (32), имеем управление

$$u_{11}(t, x) = u_1 \quad t, x, \gamma_1, \dots, u_m \quad t, x, \gamma_m,$$

для каждого из которых, решая задачу вида (34), находим управления $u_{11}^0(t, x), \dots, u_{1m}^0(t, x)$, которые удовлетворяют условиям

$$J \left[u_{11}^0(t, x) \right] = J \left[u_1 \quad t, x, \gamma_1 \right] \leq J \left[u_1 \quad t, x, \gamma \right],$$

$$J \left[u_{1m}^0 \quad t \right] = J \left[u_1 \quad t, x, \gamma_m \right] \leq J \left[u_1 \quad t, x, \gamma \right].$$

Далее из соотношения

$$J \left[\bar{u}_{10}^0 \quad t, x \right] = \min J \left[u_{11}^0(t, x) \right], \dots, J \left[u_{1m}^0(t, x) \right],\tag{37}$$

находим «оптимальное» управление $\bar{u}_{10}^0 \quad t, x$, которое будет единственным, если функционалы (36) принимают различные значения, в противном случае «оптимальными» будут несколько управлений.

Поступая аналогичным образом с управлениями

$$u_i(t, x) = u_i(t, x, \gamma), \quad i = 2, \dots, r_\gamma,$$

фактор множества (31) находим, что в случае, когда γ^0 является единственным решением соответствующей задачи $\Phi \gamma \rightarrow \min$ «оптимальным» управлением будет функция

$$u_i^0(t, x) = u_i(t, x, \gamma^0),\tag{38}$$

которая удовлетворяет соотношению (аналогично формуле (35))

$$J \left[u_i^0(t, x) \right] = J \left[u_i(t, x, \gamma^0) \right] \leq J \left[u_i(t, x, \gamma) \right], \quad i = 2, \dots, r_\gamma,\tag{39}$$

а в случае, когда задача $\Phi \gamma \rightarrow \min$ имеет решения $\gamma_1, \dots, \gamma_m$ «оптимальным управлением» будет функция $\bar{u}_{i0}^0(t, x)$, которая определяется из соотношения

$$J \left[\bar{u}_{i0}^0 \quad t, x \right] = \min J \left[u_{i1}^0 \quad t, x \right], \dots, J \left[u_{im}^0 \quad t, x \right], \quad i = 2, \dots, r_\gamma,\tag{40}$$

где функционалы $J \left[\bar{u}_{ij}^0 \quad t \right]$, $i = 2, \dots, r_\gamma$, $j = 1, \dots, m$ удовлетворяют условиям:

$$J[u_{ij}^0, t] = J[u_i(t, x, \gamma_j)] \leq J[u_i(t, x, \gamma)] , \quad i = 2, \dots, r_\gamma, \quad j = 1, \dots, m. \quad (41)$$

Теперь рассмотрим вопросы определения глобального (истинного) оптимального управления $u^0(t, x)$.

Глобальное оптимальное управление $u^0(t)$ определяется соотношением (33) (если задача $\Phi \gamma \rightarrow \min$ имеет единственное решение γ^0) и соотношением (40) (если задача $\Phi \gamma \rightarrow \min$ имеет много решение $\gamma_1, \dots, \gamma_m$).

Заключение

В данной работе рассмотрена задача нелинейной оптимизации колебательных процессов с ограничениями на состояния управляемой системы, описываемых интегро-дифференциальными уравнениями с интегральным оператором Фредгольма. Установлено, что задача сводится к исследованию бесконечной системы нелинейных интегральных уравнений первого рода, разрешимость которых исследована операторными методами.

Доказано, что соответствующее операторное уравнение допускает бесконечно много решений, образующих фактор-множество, из которого выделяются управляющие функции, минимизирующие заданный интегральный функционал. Предложен метод нахождения глобального оптимального управления как в случае единственности, так и множественности решений задачи минимизации.

Полученные результаты расширяют возможности анализа и синтеза систем управления с распределенными параметрами и нелинейными характеристиками, а также служат основой для дальнейших исследований в области оптимизации сложных динамических систем с ограничениями.

Литература.

1. Егоров А.И. Оптимальное управление тепловыми и диффузионными процессами. – М.: Наука, 1978. – 500 с.
2. Люстерник, Л. А. Элементы функционального анализа [Текст] / Л. А. Люстерник, В. И. Соболев. – М.: Наука, 1965. – 520 с.
3. Плотников В. И. Энергетическое неравенство и свойство переопределенности системы собственных функций // Изв. АН СССР. Сер. матем. – 1968. – №4. – С. 743–755.

УДК 537.527

И.Р. Урусова, к.ф.-м.н., moon4ik_29@mail.ru,
 КНУ им. Ж.Баласагына
 Т.Э. Урусова, д.ф.-м.н., urusova_tolkun@mail.ru
 НАН КР

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВИНТОВОЙ ФОРМЫ ДУГОВОГО РАЗРЯДА. СРАВНЕНИЕ С ЭКСПЕРИМЕНТОМ

В рамках трехмерной нестационарной математической модели выполнен расчет сильноточной электрической дуги во внешнем аксиальном магнитном поле. Модель записана с учетом термической и ионизационной неравновесности дуговой плазмы. Проведено сравнение результатов расчета с экспериментальными данными. Анализ результатов расчета показал удовлетворительное совпадение с экспериментом, что свидетельствует о корректности математической модели.

Ключевые слова: математическое моделирование; внешнее аксиальное магнитное поле; винтовая форма электрической дуги; сравнение с экспериментом.

Введение

Электрическая дуга во внешних магнитных полях находит широкое применение в различных технологических процессах и научных исследованиях [1, 2]. Большой интерес представляют условия формирования винтовой формы электрической дуги во внешнем аксиальном магнитном поле [3-7]. Для более глубокого понимания физики процессов необходимы дальнейшие экспериментальные и теоретические исследования, в частности, математическое моделирование и численный эксперимент.

Для моделирования винтовой формы столба дуги авторами [8, 9] предложен схемный аналог флуктуаций температуры электронов. Расчеты проводятся на основе трехмерной нестационарной модели в приближении частичного локального термодинамического равновесия электродуговой плазмы. Рассмотрены физические факторы и процессы, которые обуславливают формирование винтовой формы столба дуги. В настоящей статье проводится тестирование математической модели и алгоритма расчета электрической дуги во внешнем аксиальном магнитном поле.

Формулировка задачи и математическая модель

Рассчитывается открытая электрическая дуга постоянной силы тока I , межэлектродным расстоянием L , горящая в аргоне атмосферного давления в однородном внешнем аксиальном магнитном поле H^{Ext} . Расчеты проводятся на основе нестационарных 3-D уравнений электрической дуги в приближении частичного локального термодинамического равновесия плазмы. В декартовой системе координат (x, y, z) уравнения могут быть записаны в виде [1, 8, 9]:

уравнение непрерывности газа тяжелых частиц

$$\frac{\partial \rho}{\partial t} + \text{div}(\rho V) = 0, \quad (1)$$

уравнение непрерывности газа электронов

$$\frac{\partial N_e}{\partial t} + \text{div}(N_e V_e) = R_e, \quad (2)$$

уравнение баланса энергии газа электронов

$$\frac{\partial}{\partial t} \left(\frac{3}{2} k T_e N_e \right) + \text{div} \left(\frac{5}{2} k T_e N_e V_e \right) = \text{div}(\lambda_e \text{grad} T_e) + j^2 / \sigma - \psi - B(T_e - T) - U_i R_e, \quad (3)$$

уравнение баланса энергии газа тяжелых частиц

$$\frac{\partial}{\partial t} \frac{3}{2} k T (N_i + N_a) + \text{div} \left(\frac{5}{2} k T (N_i + N_a) V \right) = [\text{div}(\lambda \text{grad} T) + B(T_e - T)], \quad (4)$$

уравнение баланса импульса газа вдоль осей координат x, y, z

$$\frac{\partial \rho u}{\partial t} + \text{div}(\rho V u) = \text{div}(\mu \text{grad} u) - \frac{\partial p}{\partial x} + \mu_0 (j \times H)_x + s_x + (\rho - \rho_\infty) g, \quad (5)$$

$$\frac{\partial \rho v}{\partial t} + \text{div}(\rho V v) = \text{div}(\mu \text{grad} v) - \frac{\partial P}{\partial y} + \mu_0(j \times H)_y + s_y, \quad (6)$$

$$\frac{\partial \rho w}{\partial t} + \text{div}(\rho V w) = \text{div}(\mu \text{grad} w) - \frac{\partial P}{\partial z} + \mu_0(j \times H)_z + s_z, \quad (7)$$

уравнения Максвелла

$$\text{rot } E = 0, \quad \text{rot } H = j, \quad \text{div } H = 0, \quad (8)$$

закон Ома в обобщенной форме

$$\mu_0 (V_e \times H) + E = j/\sigma + (\mu_0 (j \times H) - \text{grad } P_e)/q_e N_e, \quad (9)$$

закон Дальтона

$$P/kT = N_i + N_a + N_e T_e/T. \quad (10)$$

Согласно оценкам [1], в математической модели принято, что плазма является однократно ионизованной, квазинейтральной, течение ламинарное, дозвуковое, излучение объемное; вязкая диссипация энергии и приэлектродные процессы не рассматриваются.

При записи уравнений (1–10) использованы следующие обозначения: t – время, ρ , λ_e , λ , μ , σ , ψ – соответственно плотность газа, теплопроводность электронного газа и газа тяжелых частиц, вязкость, электропроводность, излучение; m – масса атома плазмообразующего газа; N_i , N_a , N_e – концентрации ионов, атомов и электронов соответственно; $R_e = N_e(N_a K_i - N_e N_i K_r)$ – скорость генерации электронов, где K_i , K_r – константы ударной ионизации и трехчастичной рекомбинации соответственно; U_i – потенциал ионизации плазмообразующего газа; $P_e = N_e k T_e$ – парциальное давление электронов, k – постоянная Больцмана; $B = 3m_e/mk_B \nu_e N_e$ – коэффициент обмена энергией между электронами и тяжелыми частицами при упругих столкновениях, m_e – масса электрона, ν_e – частота столкновений; $\mathbf{g}$ – вектор ускорения свободного падения; q_e – элементарный заряд; μ_0 – магнитная постоянная; $\mathbf{V}$, $\mathbf{E}$, $\mathbf{j}$, $\mathbf{H}$ – соответственно векторы скорости, напряженности электрического поля, плотности электрического тока, напряженности собственного магнитного поля дуги; T , T_e – температура тяжелых частиц и электронов; P – давление; u , v , w – соответственно компоненты вектора скорости в направлениях осей координат x , y , z ; $\mathbf{V}_d$, $\mathbf{V}_t$, $\mathbf{V}_a$ – векторы скоростей дрейфа электронов, термо- и амбиполярной диффузии, определяемые по формулам: $\mathbf{V}_d = \mathbf{j}/(q_e N_e)$, $\mathbf{V}_t = -D_a/T_e \text{grad } T_e$, $\mathbf{V}_a = -D_a/N_e \text{grad } N_e$, где D_a – коэффициент амбиполярной диффузии; $\mathbf{V}_e = \mathbf{V} + \mathbf{V}_d + \mathbf{V}_t + \mathbf{V}_a$ – суммарная скорость электронов; s_x , s_y , s_z – дополнительные к $\text{div}(\mu \text{grad} u)$, $\text{div}(\mu \text{grad} v)$, $\text{div}(\mu \text{grad} w)$ вязкие слагаемые.

Коэффициенты переноса и теплофизические свойства неравновесной аргоновой плазмы атмосферного давления рассчитываются в соответствии с методикой [1].

Электромагнитная часть задачи решается в переменных φ , $\mathbf{A}$, где φ – скалярный потенциал электрического поля $\mathbf{E} = -\text{grad} \varphi$, $\mathbf{A}$ – векторный потенциал магнитного поля. Температура неплавящихся графитовых электродов определяется из уравнения теплопроводности.

Метод решения уравнений, постановка граничных и начальных условий

В соответствии с методикой [10] систему уравнений (1–10) можно представить в виде обобщенного дифференциального уравнения:

$$\frac{\partial \alpha \rho \Phi}{\partial t} + \frac{\partial \beta \rho u \Phi}{\partial x} + \frac{\partial \beta \rho v \Phi}{\partial y} + \frac{\partial \beta \rho w \Phi}{\partial z} = \frac{\partial}{\partial x} \left(\gamma \frac{\partial \Phi}{\partial x} \right) + \frac{\partial}{\partial y} \left(\gamma \frac{\partial \Phi}{\partial y} \right) + \frac{\partial}{\partial z} \left(\gamma \frac{\partial \Phi}{\partial z} \right) + \delta, \quad (11)$$

здесь Φ является одной из рассчитываемых неизвестных (N_e , T_e , T , u , v , w , φ , A_x , A_y , A_z). Для каждой переменной Φ коэффициенты α , β , γ , δ имеют свой вид.

Численное решение уравнения (11) проводится методом контрольного объема на основе конечных разностей. Полученная система алгебраических уравнений решается итерационным методом Зейделя–Гаусса с использованием нижней релаксации.

Отметим, что в вычислительном алгоритме сеточный шаг во всех направлениях по координатам x, y, z принят равным 1 мм, временной шаг равен 10^{-4} с.

Для рассчитываемых переменных постановка граничных условий проведена по периметру расчетной области $ABCDEFGH$ (рис. 1). Начальные условия задаются в некоторый условный момент времени $t = 0$.

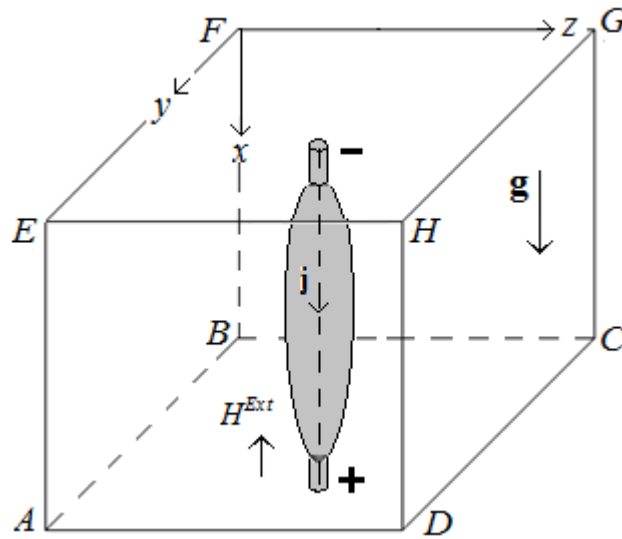


Рисунок 1 – Схема расчетной области в декартовых координатах x, y, z .
Пунктирная линия столба дуги – центральная ось

На внешних границах прямоугольной расчетной области значения температуры и концентрации электронов равны значениям температуры $T_e^{\min}$ и концентрации $N_e^{\min}$ холодного не ионизованного газа: $T_e = T_e^{\min} = 3$ К, $N_e = N_e^{\min} = 10^{17} \text{ м}^{-3}$. Температура тяжелых частиц принята равной температуре холодного газа $T = 300$ К.

Потенциал электрического поля ϕ рассчитывается из условия $\partial\phi/\partial\mathbf{n} = 0$, где $\mathbf{n}$ – нормаль к поверхности границы. На внешней токоведущей торцевой поверхности катода S_c и анода S_a потенциал электрического поля ϕ рассчитывается из условия протекания электрического тока I по нормали к поверхности. Такое же условие для переменной ϕ используется на границе «катод–плазма». Вне катода и анода ток отсутствует. Отметим, что в настоящей работе за направление электрического тока I выбрано направление от катода (–) к аноду (+).

Компоненты векторного потенциала A_x, A_y, A_z магнитного поля определяются из условия равенства нулю первой производной $\partial A/\partial\mathbf{n} = 0$ по нормали к границе.

Давление P полагается равным относительному значению $P = 1$ Па. Компоненты скорости u, v, w определяются из условия равенства нулю $\partial^2 V/\partial n^2 = 0$.

В начальный момент между электродами задается высокотемпературная ($T = 9$ К) зона с неподвижным газом в форме цилиндра.

Обсуждение результатов расчета

Расчет проводится при значениях внешних параметров разряда, близких к эксперименту [7]: тока разряда $I = 400$ А, межэлектродное расстояние $L = 150$ мм, внешнее аксиальное магнитное поле $H^{\text{Ext}} = 3.2$ кА/м направлено от анода «+» к катоду «-». Диаметр стержневых графитовых электродов равен 16 мм.

До момента времени $t = 1$ мс численный расчет выполняется в отсутствие внешнего магнитного поля, т.е. полагается $H^{\text{Ext}} = 0$. Затем, начиная с момента времени $t = 1$ мс, задается внешнее аксиальное магнитное поле величиной $H^{\text{Ext}} = 3.2$ кА/м.

Отметим, что физика процессов, обуславливающих формирование винтовой формы столба дуги изложена ранее в работах [8, 9] и в настоящей статье не рассматривается.

Результаты расчета приведены на рисунке 2, где показаны форма столба дуги в виде 3D-поверхности, ограниченной изотермой $T = 3$ кК. Для графического изображения столба дуги используется пакет Wolfram Mathematica. Анализ результатов показывает, что цилиндрическая форма столба дуги с момента времени $t = 1$ мс к моменту $t \approx 6$ мс переходит в четко выраженную винтовую форму.

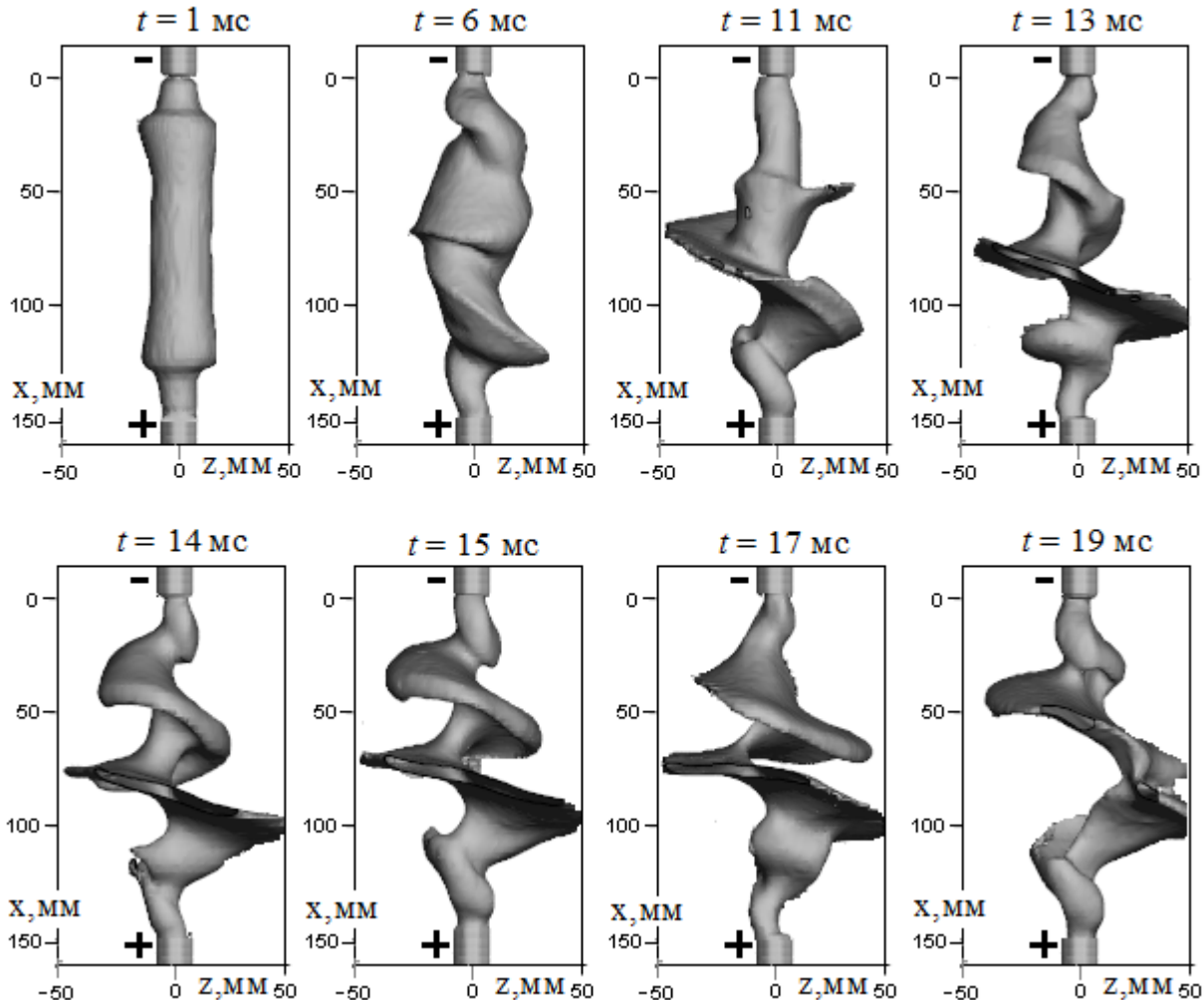


Рисунок 2 – Временная ($t = 1 \div 19$ мс) эволюция формы столба электрической дуги во внешнем аксиальном магнитном поле

Видно, что форма столба дуги является левовинтовой, т.е. против часовой стрелки. В дальнейшем на интервале времени $t \approx 6 \div 18$ мс столб дуги продолжает деформироваться, при этом винтовая форма столба дуги сохраняется. Затем с момента времени $t \approx 19$ мс наблюдается разрушение винтовой формы дуги.

На рисунке 3 показаны видеокadres формирования и распада винтовой формы дуги, полученные в ходе эксперимента [7]. В частности, в работе [7] проведено экспериментальное исследование устойчивости электродугового разряда между стержневыми графитовыми электродами в воздухе. Изучено влияние внешнего аксиального магнитного поля на устойчивость и пространственную форму протяженного дугового разряда. В экспериментах зажигание дуги обеспечивалось смыканием электродов с последующим их раздвижением до заданного межэлектродного расстояния L за время $0,2 \div 0,3$ с. Продолжительность разрядных пусков составляла 1–3 с.

Результаты эксперимента [7] показывают, что на определенном этапе горения дуги во внешнем аксиальном магнитном поле столб дуги принимает винтовую форму, при этом

форма столба дуги является левовинтовой (см. рис.3, момент времени t_1). В дальнейшем происходит разрушение винтовой структуры столба дуги (рис.3, моменты времени t_1, t_2).

Результаты численного расчета (см. рис.2) показывают качественно аналогичное поведение столба электрической дуги во внешнем аксиальном магнитном поле.

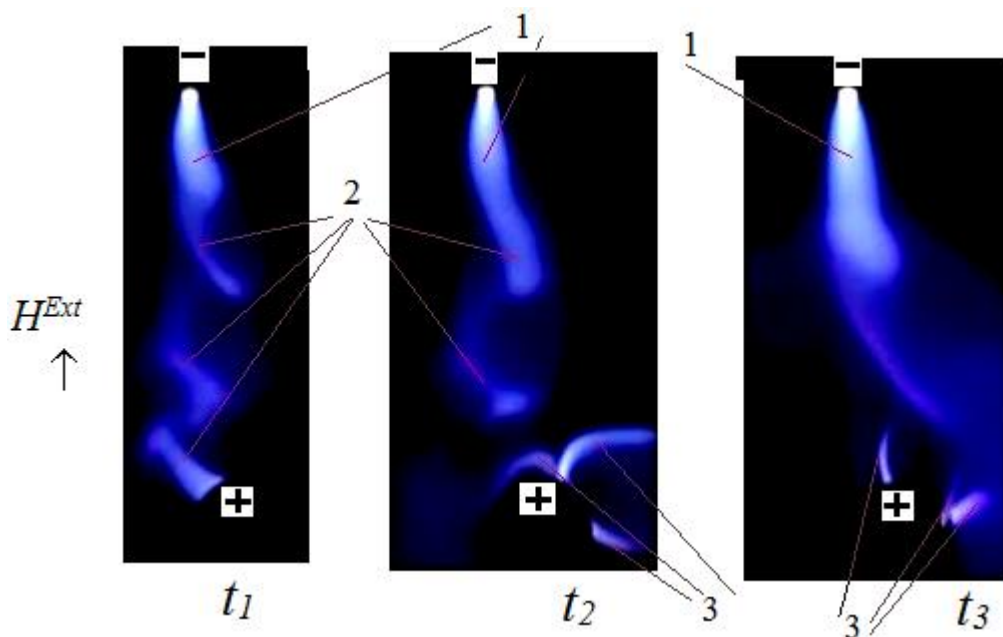


Рисунок 3 – Экспериментальные данные [7]. Видеокадры (t_1 – t_3) формирования и распада винтовых структур канала дуги во внешнем аксиальном магнитном поле H^{Ext} .

$t_3 > t_2 > t_1$ – моменты времени, соответствующие этим кадрам. 1 – области основного дугового канала, совпадающие с зоной катодного факела; 2 – витки спиральной структуры; 3 – анодные плазма-газо-пылевые факелы.

Заключение

Сравнение результатов численного моделирования настоящей работы с экспериментальными данными [7] показывает в целом удовлетворительное качественное согласие. Это свидетельствует о корректной математической модели и алгоритме расчета, которые могут быть использованы для проведения численных исследований электрических дуг во внешнем аксиальном магнитном поле.

Литература

1. Лебедев А.Д., Урюков Б.А., Энгельшт В.С. и др. Низкотемпературная плазма. –Т. 7. – Сильноточный дуговой разряд в магнитном поле. – Новосибирск: Наука, 1992. – 267 с.
2. Чередниченко В.С., Аньшаков А.С., Кузьмин М.Г. Плазменные электротехнологические установки. – Новосибирск: НГТУ, 2005. – 508 с.
3. Ментель Ю. Магнитная неустойчивость электрической дуги. В кн. Теория электрической дуги в условиях вынужденного теплообмена. – Новосибирск: Наука, 1977. – 182 с.
4. Новиков О.Я. Устойчивость электрической дуги. – Л.: Энергия, 1978. – 160 с.
5. Синкевич О.А. Нелинейная теория винтовой неустойчивости электрической дуги во внешнем магнитном поле // ДАН. – 1985. – Т. 280. № 1. – С. 99.
6. Асиновский Э.И., Кузьмин А.К., Пахомов Е.П. Измерение геометрических параметров винтовой дуги // ТВТ. – 1980. – Т. 18. № 1. – С. 9.
7. А. П. Глинов, А. П. Головин, К. В. Шалеев. Влияние внешнего магнитного поля на устойчивость протяженного дугового разряда и формирование

- многоканальных токовых структур // Прикладная физика, 2018. – № 2. – С.21–28.
8. Урусов Р.М., Урусова И.Р. О механизмах формирования винтовой формы электрической дуги во внешнем аксиальном магнитном поле // Теплофизика высоких температур, 2019. Т. 57, № 3. – С. 328–337.
 9. R. M. Urusov and I. R. Urusova «Shunting the electric arc helical spiral turns (numerical simulation)», Phys. Plasmas 27, 103510 (2020). <https://doi.org/10.1063/5.0012469>
 10. Патанкар С. Численные методы решения задач теплообмена и динамики жидкости. – М.: Энергоатомиздат, 1984. – 146 с.

УДК 51-72 : 530.1 : 536-33

Г. Ч. Тукембаева, tukembaeva.g@gmail.comБ. К. Темиров, bekjant@mail.ru

КНУ им. Ж. Баласагына

ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ МОДЕЛИ ФОГЕЛЬСОНА-ЛИХАЧЕВА

Модель Фогельсона-Лихачева (ФЛ) зарекомендовала себя в практике добычи нефти. Она обобщает уравнения Исикавы-Чанга-Лу, Пэнга-Робинсона, Редлиха-Квонга и Соаве-Редлиха-Квонга, однако является иррациональной, так как имеет дробные значения k и m в $(V+c)^k T^m$. Коэффициенты c , k , m зависят от расчетных значений P_c , T_c , V_c в критической точке K . Для исследования фазовых переходов 1-го рода определены P_c , T_c , V_c , c , k , m ФЛ-модели. Поскольку для гелия, водорода, неона, ацетилена и бензола $k=2$ на линейном участке $P(V)$ ФЛ-модель приведена к дробно-рациональному виду и представлена кубическим полиномом. В таком виде модель удобна для исследования устойчивости по критерию Гурвица и нахождения корней уравнения 3-го порядка по формуле Кардано. Анализ уравнения состояния методом А. Андропова выделяет область допустимых значений (ОДЗ) собственных чисел λ_n многочлена n -степени и область устойчивости. Интегрированием уравнения состояния вычисляется внутренняя энергия, которую несут молекулы в замкнутом объеме среды, где замкнутый объем – это элемент объема ΔV с определенной массой и плотностью вещества, по которой определяют вириальное разложение Каммерлинг-Оннеса. Тем самым рассматриваемый замкнутый объем V – это элемент объема Леви-Чивиты ΔV , к которому применима операция дифференцирования.

Для изучения фазовых переходов 1-го рода определены параметры P_c , T_c , V_c и коэффициенты c , k , m модели Фогельсона-Лихачева в случае, когда $k=2$, что отвечает гелию, водороду, неону, ацетилену и бензолу.

Ключевые слова: кубическая функция, фазовый переход 1-го рода, колебательная устойчивость, критерий Гурвица.

Введение

В работах [1]-[2] показано, что уравнения реального газа: Ван-дер-Ваальса, Бертло, Клаузиуса, второе уравнение Дитеричи, Редлиха-Квонга, Соаве-Редлиха-Квонга, Пэнга-Робинсона, Исикавы-Чанга-Лу – частные случаи модели Фогельсона-Лихачева [3], далее ФЛ-модель. Новизна ФЛ-модели заключена в произведении $(V+c)^k T^m$, где уравнению Ван-дер-Ваальса отвечают коэффициенты: $c=0$, $k=2$, $m=0$; уравнению Бертло – $c=0$, $k=2$, $m=1$; Клаузиуса – $k=2$, $m=1$. В рамках коэффициентов c , k , m ФЛ-модель обобщает уравнения Исикавы-Чанга-Лу, Пэнга-Робинсона, Редлиха-Квонга и Соаве-Редлиха-Квонга. ФЛ-модель является иррациональной, так как дробные значения k и m содержатся в $(V+c)^k T^m$. Коэффициенты c , k , m зависят от расчетных значений P_c , T_c , V_c в критической точке K . Критическая сжимаемость $Z_c=(k^2-1)/4k(1+c/V_c)$ подчинена c и k [2], где среди P_c , T_c , V_c , c , k , m найдены такие их сочетания, которые согласуются со справочными данными [4].

Наибольшее среднее относительное отклонение δ от расчетного P_c проявляется на окиси углерода, для которой $\delta=0.63\%$. Параметр k гелия, водорода, неона, ацетилена и бензола равен 2. Для других газов k меняется в пределах $k=2.00\pm 0.09$ с соответствующим каждому веществу m . Рост объема и расстояния между частицами при увеличении температуры аргументируют ангармоничностью и электронными дырками твердого тела [3]. Главное достоинство ФЛ-модели в применении многочленов степени k для описания уравнения состояния $(V+c)^k$, где коэффициент c учитывает сжимаемость реального газа. ФЛ-модель зарекомендовала себя в практике добычи нефти [5] при нагнетании пара в скважину, где модель уточнена квадратичной зависимостью и экспоненциальным членом [6], [7]. Однако фазовый переход 1-го рода авторы мотивируют ангармоничностью и электронными дырками. Для исследования таких уравнений состояния А. Андронов разработал метод с применением критерия Гурвица для определения области допустимых значений (ОДЗ) собственных чисел λ_n многочлена n -степени. Критерий устанавливает такую ОДЗ, в которой коэффициенты уравнения состояния обретают устойчивость [8]. К этому случаю относят плотность $\rho=m_0/V$ (m_0 – масса) как знакоположительную функцию вириального разложения

Камерлинг-Оннеса. Поэтому при расчете параметров ФЛ-модели требуется найти алгебраическое уравнение состояния реального газа, описываемого многочленом n -степени, в частности $n = 3$. Для этого ФЛ-модель надо привести к дробно-рациональному виду, а затем определить значения коэффициентов многочлена, в том числе физическую суть коэффициента c . Исследование таких многочленов основано на теории разностных уравнений, разработанной для нечетного порядка в [9].

Цель работы

Корректное определение параметров P_c , T_c , V_c , c , k , m в ФЛ-модели для исследования фазовых переходов 1-го рода.

Поставленная цель достигается следующим образом. Для газов коэффициент при квадратичном члене равен нулю, но больше нуля для воды и металлов. Это указывает на линейную зависимость объема от температуры в газах. Расхождение между расчетными и экспериментальными данными начинается, когда объем жидкости достигает половины V_c . Значит, исследованию подлежит фазовый переход 1-го рода под спинодалью, так как он предшествует переходу пересыщенного пара в газ в критической точке. О повышении энтропии в замкнутом объеме судят по росту температуры и внутренней энергии, обуславливающей перенос замкнутого объема из точки перегиба на возрастающем участке изотермы (из метастабильного состояния) в критическую точку на критической изотерме. Если температуру можно измерить, то внутреннюю энергию можно только вычислить. Тем самым требуется определить фактор, который в замкнутом объеме отвечает за перенос вещества из метастабильного состояния под спинодалью в критическую точку сквозь неустойчивый фазовый переход 1-го рода.

Мнимые корни характеристического уравнения дают синусоиду, действительные – спад или рост по экспоненте. Интегрирование уравнения состояния необходимо для вычисления внутренней энергии, которую несут молекулы в замкнутом объеме среды, где замкнутый объем – это элемент объема ΔV с определенной массой и плотностью вещества, по которой вычисляют вириальное разложение Камерлинг-Оннеса. Однако ΔV определяется тензорной алгеброй (символом Леви-Чивиты) [10] в дискретизации дифференциальных уравнений с частными производными конечными разностями или элементами, где направление вектора скорости разделяет элементы объема на положительные и отрицательные – $\pm \Delta V$, но в зависимости от формы объекта – на прямоугольные и криволинейные элементы объема. Знак элемента объема обнаруживается по скорости смещения dV/dt или взятии $\sqrt{}$ из ΔV . Тем самым далее рассматриваемый объем V – это элемент объема Леви-Чивиты ΔV , к которому применима операция дифференцирования.

Приведение ФЛ-модели к алгебраическому виду

Модель Фогельсона-Лихачева описывается иррациональным уравнением [3]

$$\left[P + \frac{a}{(V-c)^{k_T m}} \right] (V - b) = RT. \quad (1)$$

Универсальная газовая постоянная $R = 8.3145 \text{ Pa} \cdot \text{m}^3 \cdot \text{K}^{-1} \cdot \text{mol}^{-1}$. ФЛ-модель принимает дробно-рациональный вид, если $k=2$, которое отвечает гелию – He, водороду – H_2 , неону – Ne, ацетилену – C_2H_2 и бензолу – C_6H_6 . Остальные параметры ФЛ-модели выписаны из [3] в таблице 1. Критические параметры по справочнику [4] даны в круглых скобках для сравнения с расчетными значениями P_c , T_c , V_c , полученными в ФЛ-модели, где среднее относительное отклонение δ % вычислено по давлению P . Поэтому расчетные значения T_c , V_c разнятся со справочными так, что вычисления для бензола требуют значительной коррекции, поскольку в нормальных условиях бензол является жидкостью, а в жидкости скорость звука много больше, чем в газе.

Таблица 1

Газ	P_c , Bar	T_c , K	V_c , $10^{-3} \cdot \text{m}^3/\text{kg}$	k	m	σ	δ , %
Гелий-4	2.3	5.36	15.35	2	0.2	0.175	0.35
Водород	13 (13)	33 (33)	35	2	0.3	0.118	0.57

Неон	26 (26)	45 (45)	2.51 (2.07)	2	0.42	0.065	0.37
Ацетилен	62	309	4.39	2	1.03	0.36	0.07
Бензол	50 (49)	566 (563)	4.22 (3.3)	2	0.46	0.071	0.05

Подстановкой параметра $\sigma=c/V_c$, которая взята из ФЛ-модели, в статье [2] выведена формула коэффициента сжимаемости

$$Z_c = \frac{k^2 - 1}{4k(1 - \sigma)}. \quad (2)$$

Поскольку для He, H₂, Ne, C₂H₂ и C₆H₆ параметр $k=2$, то

$$Z_c = \frac{3}{8(1 - \sigma)}. \quad (3)$$

Для газа Ван-дер-Ваальса $Z_c^*=3/8=0.375$, для реальных газов $Z_c < 0.375$. Рассчитанные по этой формуле значения Z_c оказались больше, чем 0.375 для всех веществ, см. таблицу 2. Там же приведены константы Ван-дер-Ваальса a и b для гелия, водорода, неона, ацетилена и бензола, почерпнутые из справочника. Разница по сравнению с газом Ван-дер-Ваальса в сторону жидкости указывает на некорректный вывод параметров k , m , σ в ФЛ-модели.

Таблица 2

Вещество	Гелий	Водород H ₂	Неон	Ацетилен	Бензол
$a, \text{Pa} \cdot \text{m}^6 \cdot \text{mol}^{-2}$	0.00346	0.02452	0.0208	0.4516	1.824
$b, 10^{-6} \text{m}^3 \cdot \text{mol}^{-1}$	23.8	26.5	16.7	52.2	119.3
Z_c	$0.4545 > Z_c^*$	$0.4252 > Z_c^*$	$0.4011 > Z_c^*$	$0.5862 > Z_c^*$	$0.4044 > Z_c^*$

По Камерлинг-Оннесу вириальное разложение коэффициента сжимаемости

$$z = 1 + \sum_{i=0}^n \sum_{j=0}^m b_{ij} \frac{\omega^i}{\tau^j}. \quad (4)$$

Здесь b_{ij} – набор коэффициентов, ω и τ – приведенные плотность и температура в формуле Камерлинг-Оннеса, которая сходится к стандартной формуле фактора сжимаемости

$$Z_c = \frac{p_c V_c}{RT_c}. \quad (5)$$

Она определяется степенью многочлена, в данном случае 3-й степени. Приведенная плотность ω заставляет считаться с элементом объема согласно молекулам того вещества, которые сосредоточены в изучаемом элементе объема, переносимого средой. Значит, помимо сказанного, ФЛ-модель требует коррекции на соответствие характеристикам реального газа. Особенно критического объема V_c , так как объем в уравнении состояния газа зависит от температуры T . Причем таким решением уравнения состояния газа, которое скорректирует параметр σ . Итак, основываясь на ангармоничности и электронных дырках, авторы ФЛ-модели упустили физическую суть коэффициента c , поскольку от него зависят σ и коэффициент сжимаемости Z_c .

В случае $k=2$ характеристики критического состояния (см. (3.2) в [2])

$$p_c = \frac{RT_c}{8(b-c)}, \quad T_c T_c^m = \frac{8a}{27R(b-c)} [K], \quad (6)$$

где критическая температура T_c связана с T_c^m произведением. Поскольку константы Ван-дер-Ваальса a и b – заданные величины, но критический объем V_c – это суть уравнения, которое предстоит решить, то произведение $T_c^m T_c$ распадается на отдельные формулы

$$T_c = \frac{p_c R}{8(b-c)}, \quad T_c^m = \frac{a}{\gamma p_c R^2}, \quad \gamma = \frac{27}{64} \left[\frac{p_a^2}{K^2} \right]. \quad (7)$$

В квадратных скобках указана размерность γ , поскольку T_c^m – безразмерная величина. Тем самым дробный показатель степени m вместе с T_c^m исключены из уравнений ФЛ-модели. Теперь фиктивный параметр T_c^m ФЛ-модели выражен формулой

$$T_c^m = \frac{a}{\gamma p_c R^2}. \quad (8)$$

Тогда ФЛ-модель с целым параметром $k=2$ обретает дробно-рациональный вид:

$$p + \frac{a}{(v-c)^k T_c^m} = \frac{RT}{v-b} \xrightarrow{T_c^m = \frac{a}{\gamma p_c R^2}, k=2} p = \frac{RT(v-c)^2}{(v-b)[v^2 - 2cv - (c^2 - \gamma R^2)]}, \quad (9)$$

пригодный для математического анализа с учетом рекомендаций § 2 главы X [8]. А именно, несмотря на кажущуюся неустойчивость полинома, только критерий Гурвица устанавливает: а) действительно ли он неустойчивый; б) условно-устойчивый или в) абсолютно устойчивый. Заметим, что знаменатель содержит произведение неустойчивого полинома 1-го порядка на устойчивый полином 2-го порядка, поэтому не удовлетворяет произведению Адамара [11].

Итак, для гелия, водорода, неона, ацетилен и бензола ФЛ-модель преобразована в дробно-рациональное уравнение состояния реального газа так, что исключены m и T^m , как фиктивные параметры ФЛ-модели. Теперь решение уравнения состояния даст формулу V_c в зависимости от коэффициента c и заданных величин. Затем Z_c находим подстановкой V_c в стандартную формулу критической сжимаемости. Поскольку исследуем изотермический процесс, то сначала скорректируем T_c так, чтобы она удовлетворяла P_c , по крайней мере, с той же погрешностью δ , что и P_c . Иначе говоря, установим такую связь P_c и T_c , которая прямо зависит от V_c и c , но, с другой стороны, удовлетворяет T^m и $k=2$. Предварительно установим, как меняются знаки в дробно-рациональном уравнении состояния газа при переходе из одного квадранта в другой квадрант.

Уравнение состояния дробно-рационального вида

$$P = \frac{RT(V-c)^2}{(V-b)[V-2cV-(c^2+\gamma R^2)]} \quad (10)$$

интегрируется как простейшая рациональная дробь [12]. Тем самым удовлетворяет методу Остроградского в отличие от иррациональной ФЛ-модели. Важное достоинство нового уравнения состояния в том, что его знаменатель содержит квадратный трехчлен, не разлагающийся на действительные множители 1-й степени, т.е. является простейшей дробью второго типа (см. с. 423 [там же]). Это достигнуто приведением ФЛ-модели к дробно-рациональному виду, а именно разрывом произведения $T_c^m T_c$ на две дроби

$$T_c = \frac{P_c R}{8(b-c)}, \quad T_c^m = \frac{64a}{27 P_c R^2} \quad (11)$$

с целым параметром $k=2$. Причем каждая из дробей определяется погрешностью δ % измерений P_c в ФЛ-модели. В результате интегрирования методом Остроградского получим дифференциал внутренней энергии dU , при адиабатическом сжатии равный дифференциалу работы dA , а по найденному U вычисляется температура.

Рассмотрим дробно-рациональное уравнение относительно точки перегиба такой изотермы, для которой T меньше T_c . Тогда получим алгебраическое уравнение

$$P(V-b)[V^2 + 2cV + (c^2 + \gamma R^2)] = RT(V^2 + 2cV + c^2), \quad (12)$$

определяющее состояние изотермического процесса в I квадранте, где $V>0$, $P>0$. Во II квадранте $V<0$, $P>0$, поэтому алгебраическое уравнение сначала примет вид

$$P(-V-b)[V^2 - 2cV + (c^2 + \gamma R^2)] = RT(V^2 - 2cV + c^2), \quad (13)$$

затем с учетом знаков –

$$P(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)] = -RT(V^2 - 2cV + c^2) \quad (14)$$

и имеет неустойчивые квадратные трехчлены в обеих частях равенства. Однако это кажущаяся неустойчивость, так как произведение Адамара из двух полиномов меньшего порядка требует, чтобы результирующий кубический полином был устойчивым [11]. В III квадранте $V<0$, $P<0$, поэтому в уравнении меняются знаки:

$$-P(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)] = -RT(V^2 - 2cV + c^2), \quad (15)$$

$$P(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)] = RT(V^2 - 2cV + c^2). \quad (16)$$

Значит, III квадрант наделяет устойчивым полиномом 1-й степени $V+b$ с неустойчивыми квадратными трехчленами в обеих частях равенства. Это получилось, потому что кубическая функция симметричная относительно начала координат, как полином нечетной степени. В IV квадранте $V>0$, $P<0$, следовательно,

$$-P(V-b)[V^2 + 2cV + (c^2 + \gamma R^2)] = RT(V^2 + 2cV + c^2), \quad (17)$$

$$P(V-b)[V^2 + 2cV + (c^2 + \gamma R^2)] = -RT(V^2 + 2cV + c^2). \quad (18)$$

Поэтому, в обеих частях равенства квадратные трехчлены устойчивые с неустойчивым полиномом 1-й степени $(V-b)$, который отвечает растянутой жидкости. Таким образом, в

новой системе координат, которая определяется точкой перегиба изотермы, лежащей под критической изотермой, кубический полином не удовлетворяет произведению Адамара.

Устойчивость

В III квадранте новой системы координат имеем кубическое уравнение
 $PV^3 + [P(b - 2c) - RT]V^2 + [P(c^2 + \gamma R^2 - 2bc) + 2cRT]V + Pb(c^2 + \gamma R^2) - c^2RT = 0,$

Кубический полином в уравнении устойчивый, если коэффициенты положительные и главный диагональный минор матрицы Гурвица $\Delta_2 > 0$, т.е. выполнены неравенства:

$$P(b - 2c) - RT > 0, \quad P(c^2 + \gamma R^2 - 2bc) + 2cRT > 0, \quad Pb(c^2 + \gamma R^2) - c^2RT > 0,$$

$$\Delta_2 = \begin{bmatrix} P(b - 2c) - RT & Pb(c^2 + \gamma R^2) - c^2RT \\ P & P(c^2 + \gamma R^2 - 2bc) + 2cRT \end{bmatrix} > 0.$$

Неравенства накладывают ограничения на положительность значений

$$P > \frac{c^2RT}{b(c^2 + \gamma R^2)}, \quad b > \frac{RT}{P} + 2c, \quad 2bc > \frac{2cRT}{P} + (c^2 + \gamma R^2),$$

$$\Delta_2 = [(b - 2c)P - RT]\{[(c^2 + \gamma R^2) - 2bc]P + 2cRT\} - b(c^2 + \gamma R^2)P^2 + c^2RTP > 0.$$

Первое неравенство выражает аperiodическую устойчивость. На ее границе определитель матрицы Гурвица равен нулю [13]

$$\Delta_3 = \begin{bmatrix} P(b - 2c) - RT & Pb(c^2 + \gamma R^2) - c^2RT & 0 \\ P & P(c^2 + \gamma R^2 - 2bc) + 2cRT & 0 \\ 0 & P(b - 2c) - RT & Pb(c^2 + \gamma R^2) - c^2RT \end{bmatrix} = 0,$$

поэтому свободный член кубического уравнения равен нулю, из чего следует, что

$$P = \frac{c^2RT}{b(c^2 + \gamma R^2)}.$$

Следовательно, имеем следующее уравнение

$$V \left\{ V^2 + \left[b - 2c - \frac{c^2(RT)^2}{b(c^2 + \gamma R^2)} \right] V + \left[(c^2 + \gamma R^2) - 2bc + \frac{2c^3(RT)^2}{b(c^2 + \gamma R^2)} \right] \right\} = 0.$$

Приравняем множители нулю и получим систему двух уравнений (совокупность обозначена квадратной скобкой)

$$\begin{cases} V = 0, \\ \left[V^2 + \left[b - 2c - \frac{c^2(RT)^2}{b(c^2 + \gamma R^2)} \right] V + \left[(c^2 + \gamma R^2) - 2bc + \frac{2c^3(RT)^2}{b(c^2 + \gamma R^2)} \right] \right] = 0. \end{cases}$$

Первое уравнение дает тривиальное решение $V_1=0$. В квадратном уравнении полагаем температуру постоянной согласно изотермическому процессу и вычислим корни

$$V_{2,3} = \frac{- \left[b - 2c - \frac{c^2(RT)^2}{b(c^2 + \gamma R^2)} \right]}{2} \pm \frac{\sqrt{\left[b - 2c - \frac{c^2(RT)^2}{b(c^2 + \gamma R^2)} \right]^2 - 4(c^2 + \gamma R^2) + 8bc - \frac{8c^3(RT)^2}{b(c^2 + \gamma R^2)}}}{2}.$$

Для того, чтобы найти одну из точек огибающей, т.е. дискриминантной кривой [10], рассмотрим дискриминант алгебраического уравнения

$$D_V = \left[b - 2c - \frac{c^2(RT)^2}{b(c^2 + \gamma R^2)} \right]^2 - \frac{8c^3(RT)^2}{b(c^2 + \gamma R^2)} - 4(c^2 + \gamma R^2) + 8bc.$$

Дискриминант является биквадратным уравнением, когда $D_V=0$. Если $D_V < 0$, то корни $V_{2,3}$ – комплексные величины; если $D_V > 0$, то имеем два действительных корня $V_{2,3}$, разного знака; если же $D_V=0$, то получим 1 действительный корень, но это кратный корень $V_2=V_3$. Поскольку температура T дана по Кельвину, то может равняться нулю. В случае $D_V=0$, кратный корень является точкой возврата и описывается биквадратным уравнением

$$c^4(RT)^4 - 2c^2[b(b - 2c)(c^2 + \gamma R^2) - 4c](RT)^2 + b^2(c^2 + \gamma R^2)^2[(b - 2c)^2 - 4(c^2 + \gamma R^2 + 2bc)] = 0.$$

Решение биквадратного уравнения дает одну точку огибающей. Тем самым огибающая отделяет комплексные значения V от действительных значений V , как линия, насквозь

пронизывающая область спинодали с выходом в область идеального газа, выше критической изотермы. Иначе говоря, в I квадранте огибающая служит туннелем внутри области фазового перехода 1-го рода – аналогом туннельного эффекта.

Решением биквадратного уравнения являются корни

$$RT_{1,2,3,4} = \pm \sqrt{\frac{b(b-2c)(c^2 + \gamma R^2) - 4c \pm \sqrt{D_z}}{c^2}},$$

где дискриминант, т.е. значение на одной из точек огибающей

$$D_z = [b(b-2c)(c^2 + \gamma R^2) - 4c]^2 + b^2(c^2 + \gamma R^2)^2[4(c^2 + \gamma R^2 + 2bc) - (b-2c)^2].$$

Для реальных газов T по Кельвину является абсолютной температурой, которая не может принимать отрицательные значения для реальных веществ. Значит, среди корней есть 1 действительный корень, причем это кратный корень, если $D_z=0$. Комплексные корни отсутствуют, так как $D_z=0$, поэтому

$$RT_{1,2} = \pm \sqrt{\frac{b(b-2c)(c^2 + \gamma R^2) - 4c}{c^2}}.$$

Из-за отсутствия в реальных газах отрицательных температур берем правую часть с положительным знаком

$$RT = \sqrt{\frac{b(b-2c)(c^2 + \gamma R^2) - 4c}{c^2}}.$$

Третий закон термодинамики гласит, что абсолютная температура идеального кристалла $T=0$, поэтому числитель под корнем равен нулю, т.е.

$$b(b-2c)(c^2 + \gamma R^2) - 4c = 0.$$

Отсюда требуется решить кубическое уравнение

$$2bc^3 - b^2c^2 + 2(b\gamma R^2 + 2)c - b^2\gamma R^2 = 0,$$

$$c^3 - \frac{b}{2}c^2 + \frac{b\gamma R^2 + 2}{b}c - \frac{b\gamma R^2}{2} = 0.$$

Рассматриваемая система является динамической моделью с полутора степенями свободы (сноска на с. 266 в [8]). Согласно правилу Декарта, три переменны знака указывают на три положительных корня. Значит, дискриминант кубического уравнения $Q < 0$, поэтому используем тригонометрическое решение [10, с. 44], [14, с. 139].

Подстановкой

$$c = y + \frac{b}{6}$$

получим приведенное уравнение

$$y^3 + py + q = 0;$$

$$p = -\frac{b^3 - 12b\gamma R^2 - 24}{12b}, \quad q = -\frac{b^3 + 36b\gamma R^2 - 36}{36}.$$

Тригонометрическое решение даст следующие корни

$$y_1 = \frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \cos(\varphi/3);$$

$$y_{2,3} = \frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \cos\left(\frac{\varphi \pm 2\pi}{3}\right),$$

$$\cos \varphi = \frac{3b(b^3 + 36b\gamma R^2 - 36)}{b^3 - 12b\gamma R^2 - 24} \sqrt{\frac{b}{b^3 - 12b\gamma R^2 - 24}}; \quad 0 \leq \varphi \leq \pi.$$

Тем самым три действительных корня в виде значений параметра c выражаются формулами

$$c_1 = \frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \cos(\varphi/3) + \frac{b}{6};$$

$$c_{2,3} = \frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \cos\left(\frac{\varphi \pm 2\pi}{3}\right) + \frac{b}{6}.$$

Физическую суть параметра c дает параметрическое задание функции. Найдем производные c_1 и $c_{2,3}$ в зависимости от тригонометрической функции, так как остальные члены в правой части постоянные величины:

$$\frac{dc_1}{dt} = -\frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \sin\left(\frac{\varphi}{3}\right),$$

$$\frac{dc_{2,3}}{dt} = -\frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \sin\left(\frac{\varphi \pm 2\pi}{3}\right).$$

Получили скорость и смещения параметра c , так как $dc/dt=u$, где t – время. Поэтому гармонические смещения параметра c – это осцилляции объема, точнее, элемента объема ΔV , например, ячейки разностной схемы Согласно Андронову (см. формулу (1.23) в [8]), найденная скорость переноса элемента объема

$$u_1 = -\frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \sin\left(\frac{\varphi}{3}\right), \quad \frac{dc_1}{dt} = u_1;$$

$$u_{2,3} = -\frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \sin\left(\frac{\varphi \pm 2\pi}{3}\right), \quad \frac{dc_{2,3}}{dt} = u_{2,3}.$$

Физический смысл одной скоростей u_1, u_2, u_3 в том, что это скорость звука в газе. Она зависит от константы Ван-дер-Ваальса b , имеющей различные значения для гелия, водорода, неона, ацетилена и бензола (табл. 2). Скоростью звука является скорость u_1 с круговой частотой ω , относительно которой u_2, u_3 дают пределы изменения фазы. Ее направление положительное, поэтому в выведенных формулах знак "–" меняем на "+"

$$u_1 = \frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \sin\left(\frac{\varphi}{3}\right);$$

$$u_{2,3} = \frac{1}{3} \sqrt{\frac{b^3 - 12b\gamma R^2 - 24}{b}} \sin\left(\frac{\varphi \pm 2\pi}{3}\right).$$

Размерность такой скорости – $m^3 \cdot mol^{-1} \cdot c^{-1}$, так как зависит от t неявным образом. Внутри среды скорость звука определяется собственными колебаниями исследуемого газа, где изучаемый процесс должен обладать колебательной устойчивостью.

Найдем, каковой должна быть разность $(b-2c)$ из условия $D_z=0$

$$b^2(c^2 + \gamma R^2)^2(b-2c)^2 - b^2(c^2 + \gamma R^2)^2(b-2c)^2 - 8bc(b-2c)(c^2 + \gamma R^2) + 4b^2(c^2 + \gamma R^2)^2(c^2 + \gamma R^2 + 2bc) + 16c^2 = 0.$$

$$b^2(c^2 + \gamma R^2 + 2bc)(c^2 + \gamma R^2)^2 - 2bc(b-2c)(c^2 + \gamma R^2) + 4c^2 = 0.$$

Корни

$$(c^2 + \gamma R^2)_{1,2} = \frac{c(b-2c)}{b(c^2 + \gamma R^2 + 2bc)} \pm \frac{c\sqrt{(b-2c)^2 - 4(c^2 + \gamma R^2 + 2bc)}}{b(c^2 + \gamma R^2 + 2bc)}.$$

Если подкоренное выражение равно нулю, то получим кратный корень:

$$(b-2c)^2 = 4(c^2 + \gamma R^2 + 2bc); \quad b^2 - 4bc + 4c^2 = 4c^2 + 4\gamma R^2 + 8bc;$$

$$b^2 - 12bc - 4\gamma R^2 = 0,$$

где b – значение константы Ван-дер-Ваальса для конкретного газа, $\gamma=27/64$, R – универсальная газовая постоянная. Поскольку точка возврата динамической системы определяется кратным корнем, то значение параметра c в точке возврата

$$c = \frac{b^2 - 4\gamma R^2}{12b}.$$

Из решения биквадратного уравнения, которому отвечают кратные корни, было получено

$$RT = \sqrt{\frac{b(b-2c)(c^2 + \gamma R^2) - 4c}{c^2}}.$$

Возводим обе части в квадрат и получим

$$c^2(RT)^2 = b(b-2c)(c^2 + \gamma R^2) - 4c.$$

Поскольку правая часть

$$b(b-2c)(c^2 + \gamma R^2) - 4c = b^2c^2 + b^2\gamma R^2 - 2bc^3 - 2bc\gamma R^2 - 4c,$$

то требуется решить кубическое уравнение

$$2bc^3 + [(RT)^2 - b^2]c^2 + 2(b\gamma R^2 + 2)c - b^2\gamma R^2 = 0,$$

$$c^3 + \frac{(RT)^2 - b^2}{2b}c^2 + \frac{b\gamma R^2 + 2}{b}c - \frac{b\gamma R^2}{2} = 0.$$

Согласно правилу Декарта, один из корней является положительным корнем c_1 . Другие два корня c_2 и c_3 могут быть действительными или комплексными. Сделаем замену

$$c = y - \frac{(RT)^2 - b^2}{6b}$$

и получим приведенное уравнение

$$y^3 + py + q = 0,$$

$$p = \frac{-[(RT)^2 - b^2]^2 + 12b(b\gamma R^2 + 2)}{12b^2},$$

$$q = \frac{[(RT)^2 - b^2]^3 - 3b[(RT)^2 - b^2](b\gamma R^2 + 2) - 54b^4\gamma R^2}{108b^3},$$

$$p = \frac{12b^2\gamma R^2 + 24b + 2b^2(RT)^2 - (RT)^4 - b^4}{12b^2},$$

$$q = \frac{[(RT)^2 - b^2]^3 - 3b[(RT)^2 - b^2](b\gamma R^2 + 2) - 54b^4\gamma R^2}{108b^3}.$$

По формуле Кардано [10, с. 44], [14, с. 138-139]

$$y_1 = A + B, \quad A = \sqrt[3]{-\frac{q}{2} + \sqrt{Q}}, \quad B = \sqrt[3]{-\frac{q}{2} - \sqrt{Q}}.$$

$$Q = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2, \quad AB = -p/3$$

Дискриминант $D_z < 0$ тогда, когда

$$[b(b-2c)(c^2 + \gamma R^2) - 4c]^2 + b^2(c^2 + \gamma R^2)^2[4(c^2 + \gamma R^2 + 2bc) - (b-2c)^2] < 0,$$

т.е. должно выполняться неравенство

$$2bc(b-2c)(c^2 + \gamma R^2) > b^2(c^2 + \gamma R^2 + 2bc)(c^2 + \gamma R^2)^2 + 4c^2.$$

Следовательно, требуется исследовать случай $D_z=0$, а потому решить уравнение

$$b^2(c^2 + \gamma R^2 + 2bc)(c^2 + \gamma R^2)^2 - 2bc(b-2c)(c^2 + \gamma R^2) + 4c^2 = 0.$$

Корни этого уравнения

$$(c^2 + \gamma R^2)_{1,2} = \frac{c(b-2c)}{b(c^2 + \gamma R^2 + 2bc)} \pm \frac{c\sqrt{(b-2c)^2 - 4(c^2 + \gamma R^2 + 2bc)}}{b(c^2 + \gamma R^2 + 2bc)}$$

определяют замкнутую кривую: $c^2 + \gamma R^2$, представляющую собой шар в $\mathbf{R}$. Поэтому

$$\forall 4(c^2 + \gamma R^2 + 2bc) > (b-2c)^2$$

корни будут комплексными. Однако на дискриминантной кривой подкоренное выражение равно нулю в точке возврата

$$(b - 2c)^2 - 4c^2 - 4\gamma R^2 - 8bc = 0.$$

Итак, соотношение между b и c определяется равенством

$$\begin{aligned} b^2 - 12cb &= 4\gamma R^2, \\ -b + 12c &= -\frac{4\gamma R^2}{b}, \\ c &= \frac{b^2 - 4\gamma R^2}{12b}, \end{aligned}$$

т.е. значением параметра c в точке возврата. Подставляя $\gamma=27/64$, находим

$$c = \frac{16b^2 - 27R^2}{192b} = \frac{(4b + 3R\sqrt{3})(4b - 3R\sqrt{3})}{192b}.$$

Разность в скобках должна быть положительной, поэтому

$$b > \frac{3R\sqrt{3}}{4}.$$

Поскольку $b>0$ и $R>0$ являются заданными величинами, то $D_z=0$. Поэтому имеем 1 кратный корень

$$c^2 + \gamma R^2 = \frac{c(b - 2c)}{b(c^2 + \gamma R^2 + 2bc)},$$

которому отвечает уравнение 4-й степени

$$\begin{aligned} b(c^2 + \gamma R^2 + 2bc)(c^2 + \gamma R^2) &= c(b - 2c), \\ bc^4 + 2b^2c^3 + 2(b\gamma R^2 + 1)c^2 + b(2b\gamma R^2 - 1)c + b(\gamma R^2)^2 &= 0, \\ c^4 + 2bc^3 + \frac{2}{b}(b\gamma R^2 + 1)c^2 + (2b\gamma R^2 - 1)c + (\gamma R^2)^2 &= 0. \end{aligned}$$

Значит, $\forall c \in \mathbb{R}$

$$c \geq \frac{b^2 - 4\gamma R^2}{12b}.$$

Итак, получена одна точка огибающей и/или дискриминантной кривой, в которой

$$V = V_{2,3} = \frac{-\left[b - 2c - \frac{c^2(RT)^2}{b(c^2 + \gamma R^2)}\right]}{2},$$

так как дискриминант $D_V=0$ тогда, когда

$$(c^2 + \gamma R^2) = \frac{c(b - 2c)}{b(c^2 + \gamma R^2 + 2bc)}, \quad c = \frac{b^2 - 4\gamma R^2}{12b}.$$

Их подстановкой в выражение для $V=V_{1,2}$ находим объем

$$V = \frac{c(RT)^2(c^2 + \gamma R^2 + 2bc) - (b - 2c)^2}{2(b - 2c)},$$

Поскольку в ФЛ-модели параметр $\sigma=c/V_c$, то $\sigma>0$ определяется формулой

$$\sigma = \frac{(b - 2c)(b^2 - 4\gamma R^2)}{6b[c(RT)^2(c^2 + \gamma R^2 + 2bc) - (b - 2c)^2]}, \quad b > 2c, \quad b > \frac{3R\sqrt{3}}{4}.$$

Колебательная устойчивость

Условием существования осцилляций является неравенство $\Delta_2>0$. На границе колебательной устойчивости $\Delta_2=0$ [13], т.е.

$$\Delta_2 \equiv [(b - 2c)P - RT]\{[(c^2 + \gamma R^2) - 2bc]P + 2cRT\} - b(c^2 + \gamma R^2)P^2 + c^2RTP = 0.$$

Для изотермического процесса минору Δ_2 определителя матрицы Гурвица соответствует квадратное уравнение

$$\begin{aligned} 2c(RT)^2 - P[c^2 + 2c(b - 2c) - (c^2 + \gamma R^2) + 2bc]RT \\ - [(c^2 + \gamma R^2)(b - 2c) - 2bc(b - 2c) - b(c^2 + \gamma R^2)]P^2 = 0. \end{aligned}$$

Его корни

$$RT_{1,2} = \frac{P[c^2 + 2c(b - 2c) - (c^2 + \gamma R^2) + 2bc] \pm P\sqrt{D_{RT}}}{4c},$$

$$D_{RT} = [c^2 + 2c(b - 2c) + 2bc - (c^2 + \gamma R^2)]^2 + 8c[(c^2 + \gamma R^2)(b - 2c) - 2bc(b - 2c) - b(c^2 + \gamma R^2)].$$

Поскольку

$$P_c = \frac{RT_c}{8(b + c)},$$

то

$$32c(b + c)RT_{1,2} = RT_c[c^2 + 2c(b - 2c) - (c^2 + \gamma R^2) + 2bc] \pm RT_c\sqrt{D_{RT}}.$$

Сокращая RT , получим

$$32c(b + c) = c^2 + 2c(b - 2c) + 2bc - (c^2 + \gamma R^2) \pm \sqrt{D_{RT}},$$

Упростим выражение

$$32c(b + c) - c^2 - 2c(b - 2c) - 2bc + (c^2 + \gamma R^2) = \pm\sqrt{D_{RT}},$$

$$32bc + 32c^2 - 2c(b - 2c) - 2bc + \gamma R^2 = \pm\sqrt{D_{RT}},$$

$$32bc + 32c^2 + 4c^2 - 2bc - 2bc + \gamma R^2 = \pm\sqrt{D_{RT}},$$

$$36c^2 + 28bc + \gamma R^2 = \pm\sqrt{D_{RT}}.$$

Возведем обе части в квадрат

$$(36c^2 + 28bc + \gamma R^2)^2 = D_{RT}.$$

Выражение, полученное ранее для D_{RT} , подставим в правую часть

$$(36c^2 + 28bc + \gamma R^2)^2 = [c^2 + 2c(b - 2c) + 2bc - (c^2 + \gamma R^2)]^2 + 8c[(c^2 + \gamma R^2)(b - 2c) - 2bc(b - 2c) - b(c^2 + \gamma R^2)].$$

Опуская преобразования, имеем

$$(36c^2 + 28bc + \gamma R^2)^2 = [c^2 + 4bc - 4c^2]^2 - 10c^4 - 8bc\gamma R^2 + (c^2 + \gamma R^2)^2 - 10c^2\gamma R^2 - 16b^2c^2 + 24bc^3.$$

Из этого равенства следует уравнение

$$16c(81c^3 + 126bc^2 + (49b^2 + 5\gamma R^2)c + 4\gamma bR^2) = 0.$$

Приравнявая полином 3-го порядка нулю, получим кубическое уравнение

$$81c^3 + 126bc^2 + (49b^2 + 5\gamma R^2)c + 4\gamma bR^2 = 0.$$

Решение кубического уравнения найдем согласно [15]. Сделаем замену $c = \mu - 14/9b$.

Тогда уравнение примет вид

$$81\mu^3 + \frac{(126b)^2}{3 \cdot 81}\mu + \frac{2 \cdot (126b)^3}{27 \cdot (81)^2} - \frac{126b(49b^2 + \gamma R^2)}{3 \cdot 81} + 4\gamma bR^2 = 0.$$

Разделим уравнение на свободный член и обозначим

$$z = \mu \left\{ \frac{81}{b \left[\frac{2 \cdot 126^3 b^2}{27 \cdot (81)^2} - \frac{126(49b^2 + \gamma R^2)}{3 \cdot 81} + 4\gamma R^2 \right]} \right\}^{1/3},$$

где берется вещественное значение кубического корня. Тогда уравнение примет вид

$$z^3 - pz + 1 = 0,$$

$$p = -\frac{196b^2}{3\{b[2538\gamma R^2 - 2058b^2]\}}.$$

Поскольку $\gamma = 27/64$, то

$$p = -\frac{196b^2}{3\left(\sqrt[3]{6b^2(66339R^2 - 32928b^2)^2}\right)},$$

где $p < 0$, если $66339R^2 - 32928b^2 > 0$, поэтому уравнение: $z^3 + pz + 1 = 0$ дает один действительный корень и два комплексно-сопряженных корня. Действительный корень

отвечает полиному 1-го порядка ($V \pm b$). Он указывает на затухание в случае знака "+" или нарастание процесса в случае знака "-".

Наличие колебаний удостоверяют комплексные корни полинома 2-го порядка. Однако $p > 0$ может быть тогда, когда $66339R^2 - 32928b^2 < 0$. Поэтому уравнение: $z^3 - pz + 1 = 0$ даст три действительных корня; один из них соответствует полиному 1-го порядка, но два других – определяются квадратным трехчленом. Решение будет выражаться гиперболическими функциями sh и ch . Случай $p > 0$ подпадает под плохо обусловленные системы, когда разность $66339R^2 - 32928b^2$ близка нулю, так как от разности зависит вычисление собственных чисел λ_n матрицы Гурвица, а потому поведение и динамический портрет системы. Именно в этой связи критерий Гурвица скоординирован с собственными числами.

Заключение

Таким образом, определены параметры P_c , T_c , V_c , c , k , m в ФЛ-модели для исследования фазовых переходов 1-го рода. Иррациональная ФЛ-модель приведена к дробно-рациональному виду, что упрощает анализ известными методами исследования и применение полученных алгебраических уравнений на практике.

Литература

1. Дей Е.А., Тюменков Г.Ю. О приведенной форме термодинамических коэффициентов реальных газов // Проблемы физики, математики и техники. 2022. – № 4(53). – С. 25–29.
2. Дей Е.А., Тюменков Г.Ю. Приведенные термодинамические коэффициенты в теории реальных газов // Проблемы физики, математики и техники. – 2023. № 4(57). – С. 20–24.
3. Фогельсон, Р.Л., Лихачев Е.Р. Уравнение состояния реального газа // ЖТФ. 2004. – Т. 74. – Вып. 7. – С. 129–130.
4. Варгафтик Н.Б. Справочник по теплофизическим свойствам газов и жидкостей – М.: Наука, 1972. – 720 с.
5. Шевелёв А.П. Комплексная методология моделирования процессов тепломассопереноса в приложении к задачам подземной: дис. ... д-ра физ.-мат. наук : 01.03.14 / А.П. Шевелёв. – Тюмень, 2023. – 277 с.
6. Фогельсон, Р.Л., Лихачев Е.Р. Температурная зависимость объема жидкости // ЖТФ. 2009. – Т. 79. – Вып. 7. – С. 156–158.
7. Лихачев Е. Р. Уравнение состояния жидкости // Вестник ВГУ. Серия: Физика, математика. – 2014. – № 3. – С. 41–48.
8. Андронов А.А., Витт А.А., Хайкин С.Э. Теория колебаний. – 2-е изд. – М.: Госфизматлит., 1959. – 916 с.
9. Темиров Б.К. Осцилляция решений операторно-разностных уравнений с конечными разностями произвольных нечетных порядков. – Бишкек: Maxprint, 2014. – 178 с.
10. Корн Г., Корн Т. Справочник по математике для научных работников. – М.: Наука, 1984. – 832 с.
11. Garloff J., Wagner D.G. Hadamard Products of Stable Polynomials Are Stable // Journal of Mathematical Analysis and Applications. 1996. V. 202, Issue 3. P. 797–809. doi:10.1006/jmaa.1996.0348
12. Выгодский М.Я. Справочник по высшей математике. – М.: Наука, 1976. – 872 с.
13. Мокрова Н.В., Дорошенко А.В. Математические основы управления. – М.: Изд-во МИСИ-МГСУ, 2020. – 54 с.
14. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся втузов. – СПб.: Изд-во «Лань», 2010. – 608 с.
15. Копаев А.В., Соболев С.К. Графическое и аналитическое исследование комплексных корней кубического уравнения с одним параметром // Инженерный журнал: наука и инновации. – 2013. – Вып. 5. URL: <http://engjournal.ru/catalog/pedagogika/hidden/741.html>

УДК 530.1;536.7;544.2

Г. Ч. Тукембаева, tukembaeva.g@gmail.com

Б. К. Темиров

КНУ им. Ж. Баласагына

СИСТЕМА УРАВНЕНИЙ МЕТАСТАБИЛЬНОГО СОСТОЯНИЯ И СХЕМА ЕГО РЕШЕНИЯ

В статье исследовано метастабильное состояние – одна из актуальных проблем современной физики. В результате получена система алгебраических уравнений, описывающая метастабильное состояние гелия, водорода, неона, ацетилена и бензола, и дана схема решения, аналогичная решению биквадратного уравнения. В основе системы лежит кубическая функция, обобщающая модель Фогельсона-Лихачева (ФЛ) и уравнения Ван-дер-Ваальса, Исикавы-Чанга-Лу, Пэнга-Робинсона и Соаве-Редлиха-Квонга. Иррациональность ФЛ-модели преобразована на линейном отрезке полиномом 3-го порядка. Участок изотермы с положительным наклоном имеет единственную точку, в которой уравнение состояния определяется эллиптической кривой – кубической функцией, обобщающей уравнение Ван-дер-Ваальса. Такая система устойчивая в точке перегиба. По мере увеличения порядка полинома образуется горизонтальная площадка в точке перегиба, служащая точкой покоя. Для кубической функции ей отвечает сингулярность 2-го порядка, соответствующая метастабильному состоянию, которое устанавливается равенством нулю первой и второй производной. Перенос осей координат в точку перегиба разбивает график системы уравнений на квадранты. В III квадранте результат интегрирования уравнения состояния как простейшей дроби второго типа выражается функцией $\arctg$, что отвечает решению в виде солитона.

Ключевые слова: метастабильность, фазовый переход 1-го рода, спинодаль, устойчивость, точка перегиба.

Введение

Исследование метастабильного состояния является актуальной проблемой современной физики [1]-[3]. Иррациональная модель Фогельсона-Лихачева [4] (ФЛ-модель) обобщает уравнения Ван-дер-Ваальса, Бертло, Клаузиуса, Дитеричи, Соаве-Редлиха-Квонга, Пэнга-Робинсона, Исикавы-Чанга-Лу [5]-[6] и применена в практике добычи нефти при нагнетании пара в скважину [7]. ФЛ-модель обобщена в [8], [9] квадратичной и экспоненциальной зависимостью. В [10] выведено алгебраическое уравнение 3-го порядка, когда ФЛ-модель описывает гелий – He, водород – H_2 , неон – Ne, ацетилен – C_2H_2 и бензол – C_6H_6 , в соответствии с теорией уравнений нечетного порядка [11]. Исследование заложено А. Андроновым, где с помощью критерия Гурвица определена область допустимых значений собственных чисел λ_n многочлена n -степени – знакоположительной функции вириального разложения Камерлинг-Оннеса [12] плотности $\rho = m_0/V$ (m_0 – масса, V – объем) в метастабильном состоянии. Полином 3-го порядка в качестве уравнения состояния определяет поведение эллиптической кривой, которая проецируется на плоскость в виде точки самопересечения, но в трехмерном пространстве точка самопересечения разделена кратчайшим расстоянием между двумя прямыми [13]. Поэтому исследование эллиптических 3D- систем обобщает 2D- системы [14].

Цель работы – исследование полинома 3-го порядка в метастабильном состоянии.

Поставленная цель достигается следующим образом. В метастабильном состоянии первая и вторая производные кубической функции равны нулю. Следовательно, критическая точка K на критической изотерме является точкой перегиба, в том числе на субкритических изотермах, лежащих под критической изотермой (см. рис. 1), где P – давление, V – объем, который представляет собой элемент объема в методах конечных разностей или объемов. Кривая $abKcd$ – бинодаль (под ее колоколом область двухфазного равновесия жидкость – пар), eKf – спинодаль (под ее колоколом нереализуемые состояния), bc – коннода (линия конденсации), $abKe$ – область перегретой жидкости и $dcKf$ – переохлажденного пара. Площади закрасенных фигур под и над изобарой bc выбирают так, что они равны друг другу

согласно правилу Максвелла, предложенного в 1885 г. Тем не менее относительно точки перегиба правило может не выполняться. Рассматриваемое на рисунке 1 уравнение состояния имеет вид [10]

$$P = \frac{RT(V + c)^2}{(V - b)[V^2 + 2cV + (c^2 + \gamma R^2)]'}$$

R – универсальная газовая постоянная. Для нахождения точки перегиба вычислим первую и вторую производные выражения в правой части и приравняем их нулю. Поскольку вторая производная найдена дифференцированием первой производной, то полученные выражения являются системой уравнений, в которой необходимо сначала найти критические точки первой производной. Тогда критические точки второй производной содержат критические точки первой производной, но так как обе производные имеют четный порядок, то решение ищем по схеме биквадратного уравнения [15].

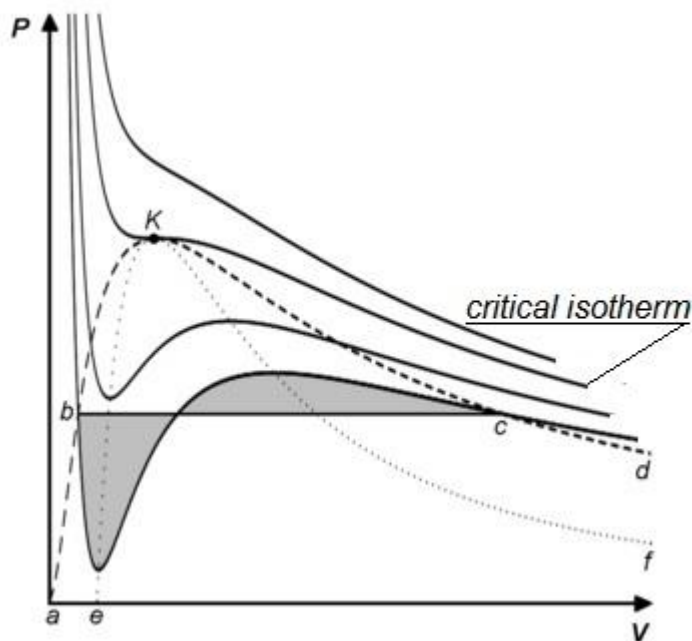


Рисунок 1 – Общий вид изотерм.

Точка K – критическая точка на критической изотерме (critical isotherm)

Четность вызвана кубической функцией в знаменателе, т.е. произведением полиномов 1-го и 2-го порядка, поэтому при дифференцировании дроби полином 1-го порядка равен константе, неравной нулю. Значит, получим уравнение 4-го порядка, точное решение которого дано Декартом-Эйлера и Феррари [16]. Вторая производная представляет собой уравнение 8-го порядка, но так как содержит найденные корни уравнения 4-го порядка, то решение ищем по схеме биквадратного уравнения с той разницей, что из уравнения 8-го порядка получается уравнение 4-го порядка. Таким образом, на возрастающих участках изотерм (под критической изотермой) исследуем устойчивость по критерию Гурвица в точках перегиба. Особенностью изотерм является кажущаяся неустойчивость, вызванная положительным наклоном возрастающего участка. Однако он устойчивый в точке перегиба, так как по мере увеличения порядка уравнения в ее окрестности образуется горизонтальная площадка покоя шара. Вне площадки шар чувствителен к малым возмущениям. Следовательно, точка перегиба – это единственная устойчивая точка на возрастающем участке изотермы. Найденная точка перегиба необходима для вывода решения в виде $\arctg$, т.е. солитона.

Схема решения в метастабильном состоянии

Разные квадранты вызывают перемену знаков P и V , так как точка перегиба – это центр симметрии кубической функции. Кубическое уравнение имеет смысл в I и III квадрантах, а потому начало координат перенесем в точку перегиба на возрастающем участке изотермы.

Она расположена под критической изотермой, далее называемой субкритической изотермой, где изотермический процесс принимает метастабильное состояние. Координаты точки устанавливаются по первой и второй производной dP/dV и d^2P/dV^2 . Равенство их нулю дает систему уравнений метастабильного состояния.

Точку перегиба под критической изотермой ищем численными методами, поэтому используем метод динамического программирования, так как конечная точка перегиба принадлежит критической изотерме. Тогда попятным движением назад, задавая температуры $T < T_c$, построим алгоритм динамического программирования. На шаге n имеем температуру T_n , на конечном шаге N совпадающую с критической температурой: $T_N = T_c$. Далее поиск сводится к поточечному заданию температуры $T_{n-1} < T_n$ и построению кривой, например, в виде сплайна. Тем самым строим огибающую или дискриминантную кривую, т.е. геометрическое место точек, в которых изотермический процесс имеет метастабильное состояние, а потому не подвержен фазовому переходу 1-го рода, который происходит в I квадранте. В динамике такой алгоритм будет ограничен соотношением шагов по времени и расстоянию. Окружение каждой из точек огибающей является элементом объема ΔV ; который граничит с комплексным пространством $\mathbf{C}$, но с другой стороны, с действительным пространством $\mathbf{R}$. Тогда на границе дискриминант равен нулю, следовательно, когда дискриминант меньше нуля, то корни комплексные. Однако когда дискриминант больше нуля, то корни действительные. Поскольку изотермы описываются полиномами, то они исследуются как уравнения, поэтому дискриминант приравниваем нулю на границе, отделяющей комплексные корни от действительных корней, для которых дискриминант меньше или больше нуля, соответственно.

Для уравнения состояния, полученного в [10]

$$P = \frac{RT(V + c)^2}{(V - b)[V^2 + 2cV + (c^2 + \gamma R^2)]},$$

первая производная

$$\frac{dP}{dV} = \frac{d}{dV} \left[\frac{RT(V^2 + 2cV + c^2)}{(V - b)(V^2 + 2cV + c^2 + \gamma R^2)} \right].$$

Ее вычисление как дроби дает

$$\frac{dP}{dV} = \frac{2RT(V + c)(V - b)(V^2 + 2cV + c^2 + \gamma R^2)}{(V - b)^2(V^2 + 2cV + c^2 + \gamma R^2)^2} - \frac{RT(V^2 + 2cV + c^2)[(V^2 + 2cV + c^2 + \gamma R^2) + 2(V - b)(V + c)]}{(V - b)^2(V^2 + 2cV + c^2 + \gamma R^2)^2}.$$

После преобразований

$$\frac{dP}{dV} = \frac{-RT[V^4 + 2(A_2 - A_1)V^3 + (B_2 - 2B_1)V^2 + (C_2 - 2C_1)V + (D_2 + 2D_1)]}{(V - b)^2(V^2 + 2cV + c^2 + \gamma R^2)^2},$$

где числовые коэффициенты

$$\begin{aligned} A_1 &= 3c - b, \quad B_1 = 3c^2 - 3bc + \gamma R^2, \quad C_1 = c^3 - 3bc^2 + c\gamma R^2 - b\gamma R^2, \quad D_1 = bc^3 + bc\gamma R^2, \\ A_2 &= 5c - b, \quad B_2 = 12c^2 - 6bc + \gamma R^2, \quad C_2 = 6c^3 - 6bc^2 + 2c\gamma R^2, \\ D_2 &= c^4 - 2bc^3 + \gamma c^2 R^2. \end{aligned}$$

Приравнивая первую производную нулю, поскольку R – универсальная газовая постоянная и T – температура не равны нулю, получим уравнение 4-го порядка

$$\begin{aligned} V^4 + 2(A_2 - A_1)V^3 + (B_2 - 2B_1)V^2 + (C_2 - 2C_1)V + D_2 + 2D_1 &= 0, \\ V^4 + 2[5c - b - (3c - b)]V^3 + [12c^2 - 6bc + \gamma R^2 - 2(3c^2 - 3bc + \gamma R^2)]V^2 &+ \\ + [6c^3 - 6bc^2 + 2c\gamma R^2 - 2(c^3 - 3bc^2 + c\gamma R^2 - b\gamma R^2)]V + c^4 - 2bc^3 + \gamma c^2 R^2 &+ \\ + 2(bc^3 + bc\gamma R^2) &= 0. \end{aligned}$$

Раскрыв скобки, имеем уравнение 4-го порядка

$$V^4 + 4cV^3 + (6c^2 - \gamma R^2)V^2 + (4c^3 + 2b\gamma R^2)V + c(c^3 + \gamma cR^2 + 2b\gamma R^2) = 0$$

на возрастающем участке субкритической изотермы $T < T_c$, который в термодинамике считается неустойчивым. Однако полином 4-го порядка, определяющий это уравнение, является устойчивым, если выполняется критерий Гурвица:

$$4c > 0, \quad 6c^2 > \gamma R^2, \quad 4c^3 + 2b\gamma R^2 > 0, \quad c(c^3 + \gamma c R^2 + 2b\gamma R^2) > 0,$$

$$\Delta_3 = \begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 & 0 \\ 1 & 6c^2 - \gamma R^2 & c(c^3 + \gamma c R^2 + 2b\gamma R^2) \\ 0 & 4c & 4c^3 + 2b\gamma R^2 \end{bmatrix} > 0, \quad c(c^3 + \gamma c R^2 + 2b\gamma R^2)\Delta_3 > 0.$$

Значит, на субкритической изотерме имеет место условно-устойчивое состояние, причем оно в точке перегиба.

Рассматриваемое на субкритической изотерме уравнение

$$V^4 + a_1 V^3 + a_2 V^2 + a_3 V + a_4 = 0,$$

где $a_1 = 4c$, $a_2 = 6c^2 - \gamma R^2$, $a_3 = 4c^3 + 2b\gamma R^2$, $a_4 = c(c^3 + \gamma c R^2 + 2b\gamma R^2)$, исследуем по Гурвицу. В общем, матрица Гурвица $\Delta_n = \Delta_{ij}$ имеет трехдиагональный вид с нулями в последнем столбце Δ_{in} , кроме элемента $a_{nn} = a_n$, поэтому

$$\Delta_n = a_n \Delta_{n-1} \rightarrow \Delta_{nn} = a_{nn} \Delta_{n-1}.$$

Для данного уравнения $n=1, \dots, 4$, следовательно, согласно критерию Лъенара-Шипара: $\Delta_2 > 0$, $\Delta_4 > 0$. В развернутом виде

$$\Delta_2 \equiv \begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 \\ 1 & 6c^2 - \gamma R^2 \end{bmatrix} > 0;$$

$$\Delta_4 \equiv c(c^3 + \gamma c R^2 + 2b\gamma R^2)\Delta_3 > 0,$$

$$\Delta_3 \equiv \begin{bmatrix} a_1 & a_3 & 0 \\ 1 & a_2 & a_4 \\ 0 & a_1 & a_3 \end{bmatrix} = \begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 & 0 \\ 1 & 6c^2 - \gamma R^2 & c(c^3 + \gamma c R^2 + 2b\gamma R^2) \\ 0 & 4c & 4c^3 + 2b\gamma R^2 \end{bmatrix}.$$

С другой стороны, собственные числа минора Δ_3 определяются из уравнения

$$\lambda^3 - \lambda^2 \text{tr} \Delta_3 - \frac{\lambda}{2} [\text{tr}(\Delta_3)^2 - \text{tr} \Delta_3] - \det \Delta_3,$$

$$\lambda^3 - [4c^3 + 6c^2 + 4c + \gamma R^2(2b - 1)]\lambda^2 - \frac{1}{2} \{ [4c^3 + 6c^2 + 4c + \gamma R^2(2b - 1)]^2 - 4c^3 + 6c^2 - 4c - \gamma R^2(2b - 1) \} \lambda - \det \begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 & 0 \\ 1 & 6c^2 - \gamma R^2 & c(c^3 + \gamma c R^2 + 2b\gamma R^2) \\ 0 & 4c & 4c^3 + 2b\gamma R^2 \end{bmatrix}.$$

Матрица $[2 \times 2]$ главного диагонального минора

$$\Delta_2 = \begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 \\ 1 & 6c^2 - \gamma R^2 \end{bmatrix}.$$

Для нее поворот Гивенса [17] выражается формулами

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}, \quad \cos \theta = \frac{a_k}{\sqrt{a_k^2 + a_i^2}}, \quad \sin \theta = \frac{-a_i}{\sqrt{a_k^2 + a_i^2}},$$

что указывает на возможные комплексно-сопряженные корни, образуемые минором Δ_3 . В целом поворот Гивенса указывает, что преобразованию координат сопутствует поворот осей [13]. Элемент a_{22} может быть больше нуля, равен нулю или меньше нуля в зависимости от разности $6c^2 - \gamma R^2$. В $\det \Delta_3$ требуется исключить a_{12} и a_{23} или a_{21} и a_{32} , т.е. привести матрицу Δ_3 к треугольному виду. Тогда собственные числа λ_n расположатся на главной диагонали матрицы Δ_3 . Для аналитического разбора используем след $-\text{tr} \Delta_3$.

Согласно теореме Виета, сумма корней трека матрицы $\text{tr} \Delta_3$ определяется решением кубического уравнения

$$4c^3 + 6c^2 + 4c + \gamma R^2(2b - 1) = 0,$$

которое исследуем по [18]. Заменой $c = \mu - 3/4$ получим уравнение

$$4\mu^3 + 3\mu + \frac{1}{27^2} - 2 + \gamma R^2(2b - 1) = 0,$$

зависящее от разности в свободном члене. Обозначив

$$p = -\frac{3}{\sqrt[3]{4\left[\frac{1}{27^2} - 2 + \gamma R^2(2b - 1)\right]^2}}, \quad z = \mu \left[\frac{4}{\frac{1}{27^2} - 2 + \gamma R^2(2b - 1)} \right]^{1/3},$$

$$p = -\frac{81}{\sqrt[3]{4\left[\frac{1 + 2 \cdot 27^2 b \gamma R^2 - 27^2(2 + \gamma R^2)}{27}\right]^2}}, \quad z = \mu \left[\frac{4}{\frac{1}{27^2} + 2b\gamma R^2 - (2 + \gamma R^2)} \right]^{1/3},$$

$$p = -\frac{243}{\sqrt[3]{4\left[1 + 2 \cdot 27^2 b \gamma R^2 - 27^2(2 + \gamma R^2)\right]^2}}, \quad z = 9\mu \left[\frac{4}{1 + 1458b\gamma R^2 - 729(2 + \gamma R^2)} \right]^{1/3},$$

получим кубическое уравнение

$$z^3 - pz + 1 = 0.$$

Преобразование Гивенса к элементу a_{32} находим по формуле

$$d_{32} = \frac{16c^2}{\sqrt{(6c^2 - \gamma R^2)^2 + c^2(c^3 + \gamma c R^2 + 2b\gamma R^2)^2}},$$

которая усложнит вычисления, поэтому остановимся на прямой прогонке для

$$V^4 + a_1 V^3 + a_2 V^2 + a_3 V + a_4 = 0$$

с устойчивым полиномом, для которого выполняется критерий Гурвица. Коэффициенты сведены в вектор-столбец $[\beta_i]$ для контроля устойчивости. Запишем дополненную матрицу

$$\Delta_3 = \begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 & 0 \\ 1 & 6c^2 - \gamma R^2 & c(c^3 + \gamma c R^2 + 2b\gamma R^2) \\ 0 & 4c & 4c^3 + 2b\gamma R^2 \end{bmatrix}.$$

Обнулим $a_{32}=4c$. Тогда останется матрица $[2 \times 2]$ главного диагонального минора Δ_2 , для которого достаточное условие устойчивости сводится к $\Delta_2 > 0$. Однако изменятся элементы дополненной матрицы.

Поменяем первую и вторую строки

$$\begin{bmatrix} 1 & 6c^2 - \gamma R^2 & c^4 + \gamma c^2 R^2 + 2bc\gamma R^2 \\ 4c & 4c^3 + 2b\gamma R^2 & 0 \\ 0 & 4c & 4c^3 + 2b\gamma R^2 \end{bmatrix} \begin{bmatrix} \beta_2 \\ \beta_1 \\ \beta_3 \end{bmatrix}.$$

Тогда можно обнулить a_{13} , чтобы образовать нули в третьем столбце Δ_2 . В любом случае получим матрицу $[2 \times 2]$ минора Δ_2 . Умножим вторую строку на $-4c$

$$\begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 & 0 \\ -4c & -4c(6c^2 - \gamma R^2) & -4c(c^4 + \gamma c^2 R^2 + 2bc\gamma R^2) \\ 0 & 4c & 4c^3 + 2b\gamma R^2 \end{bmatrix} \begin{bmatrix} \beta_1 \\ -4c\beta_2 \\ \beta_3 \end{bmatrix}$$

и сложим с третьей строкой

$$\begin{bmatrix} 4c & 4c^3 + 2b\gamma R^2 & 0 \\ -4c & -4c(6c^2 - \gamma R^2) & -4c(c^4 + \gamma c^2 R^2 + 2bc\gamma R^2) \\ 0 & 4c & 4c^3 + 2b\gamma R^2 \end{bmatrix} \begin{bmatrix} \beta_1 \\ -4c\beta_2 \\ \beta_3 \end{bmatrix}.$$

Замечание. Элементы вектор-столбца взяты по абсолютной величине

$$\begin{bmatrix} |a_1| \\ |a_2| \\ |a_3| \end{bmatrix} = \begin{bmatrix} |4c| \\ |6c^2 - \gamma R^2| \\ |4c^3 + 2b\gamma R^2| \end{bmatrix}.$$

Вторая производная уравнения состояния

$$\frac{d^2 P}{dV^2} = \frac{d}{dV} \left\{ \frac{-RT[V^4 + 2(A_2 - A_1)V^3 + (B_2 - 2B_1)V^2 + (C_2 - 2C_1)V + (D_2 + 2D_1)]}{(V - b)^2(V^2 + 2cV + c^2 + \gamma R^2)^2} \right\}.$$

Для ее вычисления используем первую производную в фигурных скобках, поэтому

$$\frac{d^2P}{dV^2} = RT \left\{ \frac{2f(V)(V^4 + 2A_3V^3 + 2B_3V^2 + 2C_3V + D_3)}{(V-b)^4(V^2 + 2cV + c^2 + \gamma R^2)^4} - \frac{[4V^3 + 6(A_2 - A_1)V^2 + 2(B_2 - 2B_1)V + (C_2 - 2C_1)]}{(V-b)^4(V^2 + 2cV + c^2 + \gamma R^2)^4} \right\}.$$

Здесь

$$f(V) = V^4 + 2(A_2 - A_1)V^3 + (B_2 - 2B_1)V^2 + (C_2 - 2C_1)V + (D_2 + 2D_1),$$

числовые коэффициенты

$$A_3 = 2c + 1, \quad B_3 = 3c^2 + c - 2b + \gamma R^2, \quad C_3 = 2c^3 + 2\gamma R^2c + b^2 - 2bc,$$

$$D_3 = c^4 + 2\gamma R^2c^2 + 2b^2c + \gamma^2 R^4.$$

С их учетом вторая производная

$$\frac{d^2P}{dV^2} = RT \left\{ \frac{2\varphi(V) - [4V^3 + 6(A_2 - A_1)V^2 + 2(B_2 - 2B_1)V + (C_2 - 2C_1)]}{(V-b)^4(V^2 + 2cV + c^2 + \gamma R^2)^4} \right\},$$

где

$$\begin{aligned} 2\varphi(V) = & 2V^8 + 4A_3V^7 + 4(A_2 - A_1)V^7 + 8A_3(A_2 - A_1)V^6 + 2(2B_3 + B_2 - 2B_1)V^6 \\ & + 8B_3(A_2 - A_1)V^5 + 4A_3(B_2 - 2B_1)V^5 + 2(2C_3 + C_2 - 2C_1)V^5 \\ & + 8C_3(A_2 - A_1)V^4 + 4B_3(B_2 - 2B_1)V^4 + 4A_3(C_2 - 2C_1)V^4 \\ & + 2(D_3 + D_2 + 2D_1)V^4 + 2D_3(A_2 - A_1)V^3 + 4C_3(B_2 - 2B_1)V^3 \\ & + 4B_3(C_2 - 2C_1)V^3 + 4A_3(D_2 + 2D_1)V^3 + 2D_3(B_2 - 2B_1)V^2 + 4C_3(C_2 - 2C_1)V^2 \\ & + 4B_3(D_2 + 2D_1)V^2 + 2D_3(C_2 - 2C_1)V + 4C_3(D_2 + 2D_1)V + 2D_3(D_2 + 2D_1) \end{aligned}$$

или в развернутом виде

$$\begin{aligned} 2\varphi(V) - [4V^3 + 6(A_2 - A_1)V^2 + 2(B_2 - 2B_1)V + (C_2 - 2C_1)] = & \\ = & 2V^8 + 4(A_3 + A_2 - A_1)V^7 + 2(4A_3A_2 - 4A_3A_1 + 2B_3 + B_2 - 2B_1)V^6 \\ & + 2(2A_3B_2 + 4A_2B_3 - 4A_1B_3 - 4A_3B_1 + 2C_3 + C_2 - 2C_1)V^5 \\ & + 2(4A_2C_3 - 4A_1C_3 + 2B_3B_2 - 4B_3B_1 + 2A_3C_2 - 4A_3C_1 + D_3 + D_2 + 2D_1)V^4 \\ & + 2(D_3A_2 - D_3A_1 + 2B_2C_3 - 4B_1C_3 + 2B_3C_2 - 4B_3C_1 + 2A_3D_2 + 4A_3D_1 - 2)V^3 \\ & + 2[3A_1 - 3A_2 + B_2D_3 - 2B_1D_3 + 2C_3C_2 - 4C_3C_1 + (2B_3D_2 + 4B_3D_1)]V^2 \\ & + 2(2B_1 - B_2 - 2C_1D_3 + C_2D_3 + 2C_3D_2 + 4C_3D_1)V + 2C_1 - C_2 + 4D_1D_3 \\ & + 2D_2D_3. \end{aligned}$$

После сокращения на 2 и приравнивания полиномов 4-го и 8-го порядков нулю, получим систему из 2 уравнений, которую запишем следующим образом:

$$V^4 + 2(A_2 - A_1)V^3 + (B_2 - 2B_1)V^2 + (C_2 - 2C_1)V + D_2 + 2D_1 = 0;$$

$$\begin{aligned} V^8 + 2(A_3 + A_2 - A_1)V^7 + (4A_3A_2 - 4A_3A_1 + 2B_3 + B_2 - 2B_1)V^6 \\ + (2A_3B_2 + 4A_2B_3 - 4A_1B_3 - 4A_3B_1 + 2C_3 + C_2 - 2C_1)V^5 \\ + (4A_2C_3 - 4A_1C_3 + 2B_3B_2 - 4B_3B_1 + 2A_3C_2 - 4A_3C_1 + D_3 + D_2 + 2D_1)V^4 \\ + (D_3A_2 - D_3A_1 + 2B_2C_3 - 4B_1C_3 + 2B_3C_2 - 4B_3C_1 + 2A_3D_2 + 4A_3D_1 - 2)V^3 \\ + [3A_1 - 3A_2 + B_2D_3 - 2B_1D_3 + 2C_3C_2 - 4C_3C_1 + (2B_3D_2 + 4B_3D_1)]V^2 \\ + (2B_1 - B_2 - 2C_1D_3 + C_2D_3 + 2C_3D_2 + 4C_3D_1)V + C_1 - \frac{1}{2}C_2 + 2D_1D_3 + D_2D_3 \\ = 0. \end{aligned}$$

Поскольку решение уравнения 4-го порядка ранее найдено, то его корни содержит уравнение 8-го порядка. Значит, подстановка корней уравнения 4-го порядка в уравнение 8-го порядка даст уравнение 4-го порядка, решение которого находим по Декарту-Эйлеру или Феррари [16], т.е. по схеме решения биквадратного уравнения [15].

Решение в виде функции $\arctg$

Уравнение состояния, рассмотренное на рисунке 1, в виде произведения двух полиномов принимает вид

$$P(V-b)[V^2 + 2cV + (c^2 + \gamma R^2)] = RT(V^2 + 2cV + c^2),$$

где $V > 0$, $P > 0$. Оно описывает процесс в I квадранте, в том числе в новой системе координат, которую получим переносом осей в точку перегиба 0 субкритической изотермы (см. рис. 2). Коэффициенты b , c и R заданы, $\gamma = 27/64$ [Pa²/K²].

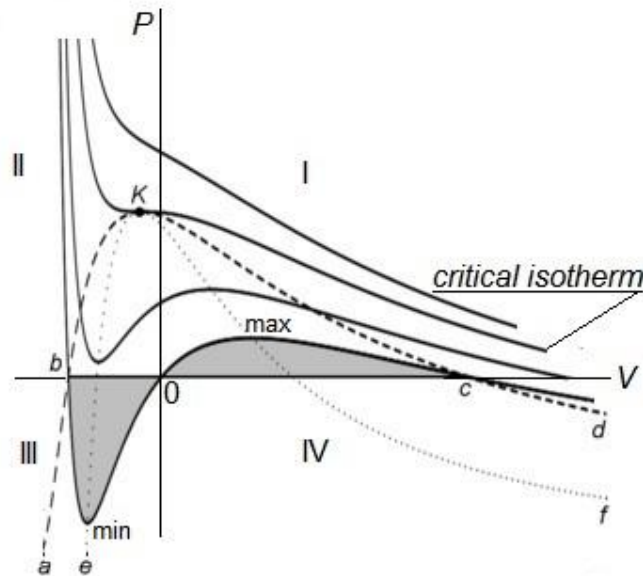


Рисунок 2 – Перенос координат в точку перегиба.
Спинодаль eKf пересекает точки экстремума

В таком случае кубическая функция симметрична относительно центра координат, перенесенного в точку перегиба, т.е. в I и III квадрантах, как положено для нечетной функции. В III квадранте, согласно $V < 0$ и $P < 0$, в уравнении состояния меняются знаки

$$\begin{aligned} -P(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)] &= -RT(V^2 - 2cV + c^2), \\ P(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)] &= RT(V^2 - 2cV + c^2). \end{aligned}$$

Значит, III квадрант наделяет устойчивым полиномом 1-й степени $(V+b)$. Это важно, так как произведение Адамара устойчивое, если имеет устойчивые полиномы в качестве сомножителей [19], что в большей степени зависит от устойчивости полинома 1-й степени. Тогда уравнение состояния в III квадранте имеет следующий вид

$$P = \frac{RT(V+c)^2}{(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)]}$$

Оно интегрируется как простейшая рациональная дробь [12]. Предполагается гладкость P и V , чтобы выполнялось интегрирование по частям, поэтому удовлетворяет методу Остроградского в отличие от иррациональной ФЛ-модели. Важное достоинство нового уравнения состояния в том, что его знаменатель содержит квадратный трехчлен, не разлагающийся на действительные множители 1-й степени, т.е. является простейшей дробью второго типа (см. с. 423 [там же]).

Интегрированием получим внутреннюю энергию для изотермического процесса

$$U = TS - \int \left(\frac{RT(V+c)^2}{(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)]} \right) dV,$$

S – энтропия, $R=8.3145 \text{ Pa} \cdot \text{m}^3 \cdot \text{K}^{-1} \cdot \text{mol}^{-1}$ [10]. Разложение дроби на простейшие имеет вид

$$\frac{RT(V+c)^2}{(V+b)[V^2 - 2cV + (c^2 + \gamma R^2)]} = \frac{A}{V+b} + \frac{MV+N}{V^2 - 2cV + (c^2 + \gamma R^2)},$$

Поэтому дроби интегрируются отдельно. В общем, результат интегрирования дает формула

$$U = TS - A \ln|V+b| - \int \frac{(MV+N)dV}{V^2 - 2cV + (c^2 + \gamma R^2)} + C.$$

Замена $z=V-c$, но $k^2=\gamma R^2$ приводит знаменатель к виду $z^2 + k^2$.

Следовательно, в общем виде результат выражается следующим образом

$$U = TS - A \ln|V + b| - \frac{M}{2} \ln[V^2 - 2cV + (c^2 + \gamma R^2)] - \frac{N - cM}{R\sqrt{\gamma}} \operatorname{arctg} \frac{V + c}{R\sqrt{\gamma}} + C.$$

Заключение

Итак, на участке изотермы с положительным наклоном существует единственная точка, в которой уравнение состояния определяется эллиптической кривой – кубической функцией, обобщающей уравнение Ван-дер-Ваальса. Система устойчивая, так как рассматривается в точке перегиба. По мере увеличения порядка полинома образуется горизонтальная площадка в точке перегиба, служащая точкой покоя. Для кубической функции ей отвечает сингулярность 2-го порядка, соответствующая метастабильному состоянию, которое устанавливается равенством нулю первой и второй производной. Перенос осей координат в точку перегиба разбивает на квадранты. В III квадранте результат интегрирования уравнения состояния как простейшей дроби второго типа выражается в виде функции arctg , что отвечает солитону.

Литература

1. Бойко В.Г., Могель Х.-Й., Сысоев В.М., Чалый А.В. Особенности метастабильных состояний при фазовых переходах жидкость – пар // Успехи физ. наук. –1991. –Т. 161, № 2. – С. 77–111.
2. Виноградов В.Е. Исследование вскипания перегретых и растянутых жидкостей : автореф... дис. докт. физ.-мат. наук / 01.04.14 – Теплофизика и теоретическая теплотехника. – Екатеринбург, 2006. – 43 с.
3. Зудин Ю.Б., Уртенев Д.С. Рост парового пузырька в перегретой жидкости (эффект запаривания давления) // Изв. РАН. Энергетика. –2023. – № 6. – С. 61–78.
4. Фогельсон, Р.Л., Лихачев Е.Р. Уравнение состояния реального газа // ЖТФ. – 2004. –Т. 74, вып. 7. – С. 129–130.
5. Дей Е.А., Тюменков Г.Ю. О приведенной форме термодинамических коэффициентов реальных газов // Проблемы физики, математики и техники. – 2022. – № 4(53). – С. 25–29.
6. Дей Е.А., Тюменков Г.Ю. Приведенные термодинамические коэффициенты в теории реальных газов // Проблемы физики, математики и техники. – 2023. – № 4(57). – С. 20–24.
7. Шевелёв А.П. Комплексная методология моделирования процессов тепломассопереноса в приложении к задачам подземной гидродинамики : дис. ... д-ра физ.-мат. наук : 01.03.14 / А.П. Шевелёв. – Тюмень, 2023. – 277 с.
8. Фогельсон, Р.Л., Лихачев Е.Р. Температурная зависимость объема жидкости // Журн. техн. физики. –2009. – Т. 79, вып. 7. – С. 156–158.
9. Лихачев Е. Р. Уравнение состояния жидкости // Вестник ВГУ. Серия: Физика, математика. – 2014. – № 3. – С. 41–48.
10. Тукембаева Г.Ч., Темиров Б.К. Идентификация параметров модели Фогельсона-Лихачева // Проблемы автоматизации и управления. – 2025. – № 1.
11. Темиров Б.К. Осцилляция решений операторно-разностных уравнений с конечными разностями произвольных нечетных порядков. – Бишкек: Maxprint, 2014. – 178 с.
12. Андронов А.А., Витт А.А., Хайкин С.Э. Теория колебаний. – 2-е изд. – М.: Госфизматлит., 1959. – 916 с.
13. Выгодский М.Я. Справочник по высшей математике. – М.: Наука, 1976. – 872 с.
14. Эрроусмит Д., Плейс К. Обыкновенные дифференциальные уравнения. Качественная теория с приложениями. – М.: Мир, 1986. – 243 с.
15. Темиров Б.К. Осцилляция решений операторно-разностных уравнений с конечными разностями четного порядка : автореф... дис. канд. физ.-мат. наук / 01.01.02 – Дифференциальные уравнения. – Бишкек, 1995. – 14 с.
16. Корн Г., Корн Т. Справочник по математике для научных работников. – М.: Наука, 1984. – 832 с.

17. Куксенко С.П., Газизов Т.Р. Итерационные методы решения системы линейных алгебраических уравнений с плотной матрицей. – Томск: Томский гос. ун-т, 2007. – 208 с.
18. Копаев А.В., Соболев С.К. Графическое и аналитическое исследование комплексных корней кубического уравнения с одним параметром // Инженерный журнал: наука и инновации. – 2013. – Вып. 5. URL: <http://engjournal.ru/catalog/pedagogika/hidden/741.html>
19. Garloff J., Wagner D.G. Hadamard Products of Stable Polynomials Are Stable // Journal of Mathematical Analysis and Applications. 1996. V. 202, Issue 3. P. 797-809. doi:10.1006/jmaa.1996.0348

УДК: 621.311.1:502.172.3

С.М. Асанова¹, a_sm07@kstu.kg, Т.Ж. Жабудаев¹, Д.У. Асанова², М.С. Асанов¹,
А.Б. Калмурзаев², К. Сатаркулов², satarkulov46k@mail.ru

¹КГТУ им. И.Раззакова,

²Институт машиноведения и автоматики НАН КР

МЕТОДИКА РАЗРАБОТКИ АЛГОРИТМА ОПТИМАЛЬНОГО СИТУАЦИОННОГО УПРАВЛЕНИЯ ЭНЕРГЕТИЧЕСКИМ БАЛАНСОМ В АВТОМАТИЗИРОВАННЫХ РАСПРЕДЕЛЕННЫХ ГИБРИДНЫХ ЭНЕРГОКОМПЛЕКСАХ

Принятая в настоящей работе структура системы накопления и распределения потоков мощностей НРПМ позволяет обеспечить простоту изменения ее конфигурации путем добавления/исключения в ее состав тех или иных компонентов (балластные источники БИ, балластные нагрузки БН, генерирующие установки с ВИЭ и нагрузки разного типа), а также добавление/исключение возможности взаимодействия НРПМ с глобальной сетью ГС. Для принятой структуры построена математическая модель с учетом ситуаций, возникающих в процессе циркуляции потоков в системе НРПМ, сформулирована задача синтеза алгоритма оптимального ситуационного управления АОСУ энергетическим балансом в ней и предложена схема ее решения, которая позволяет получить многоуровневый алгоритм $G_{АОСУ, g_m}$, $m = 0, 1, \dots, M - 1$, состоящий из последовательно функционирующих алгоритмов, т.е.

$G_{АОСУ, g_m}: G_{ШСР, g_m} \xrightarrow{i_{с.л}^{(1)}(g_m)} G_{АКБ1, g_m} \xrightarrow{i_{с.л}^{(2)}(g_m)} G_{АКБ2, g_m} \xrightarrow{i_{с.л}^{(3)}(g_m)} G_{БИ, БН, g_m} \xrightarrow{i_{ГС}^{(+,-)}(g_m)}$, выполняющих следующие функции: $G_{ШСР, g_m}$ – поддержание текущей величины напряжения конденсатора $u_{ШСР}(\theta_m)$ (узла – шины сборки и распределения ШСР) путем выдачи оптимального управляющего воздействия в виде балансирующего тока $i_{с.л}^{(1)}(\theta_m)$; $G_{АКБ1, g_m}$, $G_{АКБ2, g_m}$, $G_{БИ, БН, g_m}$ – оптимальные ситуационные алгоритмы для последовательной реализации балансирующего тока $i_{с.л}^{(1)}(\theta_m)$ с использованием элементов системы НРПМ, соответственно, (АКБ1(1), АКБ1(2)), (АКБ2(1), АКБ2(2)), (БИ, БН) с целью поддержания перетока $i_{ГС}^{(+,-)}(\theta_m)$ между ГС и НРПМ в окрестности номинального $i_{ГС}^{ном}(\theta_m)$. Алгоритм $G_{АОСУ, g_m}$ обладает, что при подборе и изменении конфигурации системы НРПМ на этапе проектирования систем АРГЭК для различных регионов с соответствующими им ВИЭ его структура легко модифицируется, что важно при создании системы автоматизированного проектирования автоматизированных распределенных гибридных энергокомплексов АРГЭК.

Ключевые слова: автоматизированные распределенные гибридные энергокомплексы; возобновляемые источники энергии; интеллектуальные системы; надежность; энергетический баланс; аккумуляторная батарея; мощность; алгоритм; оптимизация; прогнозирование; ситуация; управление.

Введение

На современном этапе одной из важнейших задач развития экономики регионов тех или иных стран (в частности, Кыргызской Республики) является повышение эффективности работы их систем электроэнергетики. Этого можно достичь, решив множество задач, возникающих при проектировании и эксплуатации электроэнергетической системы.

Приоритетным и перспективным направлением развития и повышения эффективности современной энергетики является разработка и внедрение региональных автоматизированных распределенных гибридных энергокомплексов (АРГЭК) с возобновляемыми источниками энергии (ВИЭ), функционирующих во взаимодействии с глобальной (общегосударственной) сетью (ГС) [1]. Частный случай, когда система АРГЭК не имеет доступа к ГС, рассмотрена, например, в работах [2-4].

В вышеуказанной работе [1] разработано и приведено содержательное описание методики проектирования интеллектуальных систем АРГЭК, включающее в себя следующие этапы:

- разработка структуры распределенной гибридной системы генерации (РГСГ), состоящая, в свою очередь, из распределенных систем ветряных генераторов (ВГ), гидрогенераторов (ГГ) и солнечных батарей (СБ), вырабатываемые мощности которых

передаются с помощью двухпроводной локальной сети (ЛС_{РГСТ}) с древовидной структурой, где корнем графа сети является шина сборки и распределения (ШСР) системы накопления и распределения потоков мощностей (НРПМ), а концевыми узлами – узлы присоединения генерирующих агрегатов с системы солнечных батарей. В работе [5] рассмотрена задача синтеза оптимальной структуры системы РГСТ, обеспечивающей требуемый уровень генерируемой мощности, минимальную стоимость и необходимую функциональную надежность. В работе [6] рассмотрена задача автоматического распознавания обрыва провода на участках локальной сети ЛС_{РГСТ}, построенной с использованием многофункционального провода, состоящего из силового провода и изолированной жилы информационного провода [7];

- разработка трехфазной сложнзамкнутой локальной сети ЛС_{ПЭ} со следующими свойствами: с заданным уровнем надежности; распознающей обрывы проводов на ее участках [6]; с управляемой структурой, позволяющей изменять маршруты движения потоков мощностей от узла ШСР до распределенных потребителей энергии (ПЭ) при существенных изменениях нагрузок в тех или иных узлах нагрузки, а также при обрывах линий отдельных участков с целью минимизации потерь мощности в рассматриваемой сети ЛС_{ПЭ} [8];

- разработка структуры управляемой системы накопления и распределения потоков мощностей (НРПМ) с целью обеспечения физической реализуемости и повышения надежности процесса управления энергетическим балансом в нем [9]. При этом обеспечение физической реализуемости процесса управления энергетическим балансом, т.е. поддержание текущей потребляемой мощности потребителями в окрестности требуемой номинальной мощности, достигается за счет поддержания напряжения конденсатора, подключенного к узлу ШСР, в окрестности номинального, а повышение надежности – за счет подключения к узлу ШСР накопителя АКБ с двухуровневой двухконтурной структурой АКБ_{*i*(*j*)}, $i \in \{1, 2\}$, $j \in \{1, 2\}$, где i – номер уровня; j – номер контура; АКБ₁(j), $j \in \{1, 2\}$ – двухконтурный накопитель 1-го уровня для управления балансом мощностей в НРПМ при номинальном режиме АРГЭК, при изменении мощностей ВИЭ и потребления в пределах их доверительных интервалов, оцененных на этапе проектирования; АКБ₂(j), $j \in \{1, 2\}$ – двухконтурный накопитель 2-го уровня для согласования режимов работ НРПМ и ГС и для управления совместно с накопителем АКБ₁(j), $j \in \{1, 2\}$ 1-го уровня, ГС, ДГ, БН, балансом мощностей в НРПМ при аварийном режиме АРГЭК, а также при выходе мощностей ВИЭ и потребления за пределы их доверительных интервалов. При этом поочередная работа параллельных контуров в режиме зарядки/разрядки продлевает срок службы системы АКБ.

Настоящая работа основывается на работах [1,5,6,8,9,10,16], является дальнейшим их развитием и посвящена разработке алгоритма оптимального ситуационного управления энергетическим балансом в управляемой системе НРПМ с целью поддержания текущей потребляемой мощности региональными потребителями в окрестности требуемой номинальной, а также поддержания текущего перетока мощности между НРПМ и ГС в окрестности заданной величины для сохранения динамической устойчивости электроэнергетической системы (ЭЭС) в целом (при существенных отклонениях возможно обрушение энергосистемы вплоть до «блекаута») с использованием математического аппарата вычислительных сетей Петри (ВСП) [13-15].

1. Функциональная схема замкнутой цифровой системы управления энергетическим балансом в управляемой системе НРПМ

Как было сказано выше, в работе [9] произведен выбор и обоснование структуры системы НРПМ как объекта управления с позиции обеспечения физической реализуемости и повышения надежности процесса управления энергетическим балансом в ней, где предложенная структура обеспечивает простоту изменения ее конфигурации путем

добавления и исключения элементов в зависимости от мощности ВИЭ в рассматриваемых регионах. Такая структура является также удобной при разработке систем автоматизированного проектирования (САПР) замкнутых цифровых систем управления сложными электросетевыми комплексами как при нормальных, так и при аварийных режимах ее функционирования.

Построение алгоритма оптимального ситуационного управления (АОСУ) энергетическим балансом в управляемой системе НРПМ производится в рамках структуры замкнутой цифровой системы управления, функциональная схема которой показана на рисунке 1.

1.1. Управляемая система НРПМ (объект управления) на рисунке 1 представлена в виде графа ее структуры [1], где:

- θ_m , $m = 0, 1, 2 \dots$ – дискретные моменты времени с дискретой $\Delta\theta$;
- $i_\Gamma(\theta_m)$ – неуправляемый ток, соответствующий неуправляемой суммарной мощности $W_\Gamma(\theta_m)$:

$$W_\Gamma(\theta_m) = W_{ВГ}(\theta_m) + W_{СБ}(\theta_m) + W_{ГГ}(\theta_m), \quad (1)$$

вырабатываемой системой РГСГ, состоящей из региональных распределенных систем ветряных генераторов ВГ, солнечных батарей СБ и гидрогенераторов ГГ. Ток $i_\Gamma(\theta_m)$ имеет стохастический (непредсказуемый) характер ввиду стохастичности ВИЭ. Для снятия проблемы синхронизации мощностей переменного тока, вырабатываемых генерирующими агрегатами системы РГСГ, они преобразованы в мощности постоянного тока;

- $i_\Pi(\theta_m)$ – неуправляемый ток, соответствующий неуправляемой суммарной потребляемой мощности переменного тока $W_\Pi(\theta_m)$:

$$W_\Pi(\theta_m) = \sum_{j \in N_{\Pi\Delta}} W_{\Pi\Delta j}(\theta_m) + \Delta W_{\text{ЛС}}(\theta_m), \quad (2)$$

потребляемой подмножеством электроприборов, случайным образом формирующимся из элементов некоторого универсального множества и подключающимся к узлам нагрузки трехфазной локальной сети ЛС_{ПЭ}, предназначенной для транспортировки мощности $W_\Pi(\theta_m)$ до потребителей энергии (ПЭ), где $N_{\Pi\Delta}$ – множество номеров узлов нагрузки ЛС_{ПЭ}; $W_{\Pi\Delta j}(\theta_m)$ – мощность j -го узла нагрузки; $\Delta W_{\text{ЛС}}(\theta_m)$ – потеря мощности в ЛС_{ПЭ}. Потребляемый ток $i_\Pi(\theta_m)$ имеет стохастический (непредсказуемый) характер ввиду стохастичности потребляемой мощности $W_\Pi(\theta_m)$;

- $u_{\text{ШСР}}(\theta_m)$ – напряжение конденсатора с емкостью $C_{\text{ШСР}}$, подключенного к узлу ШСР и предназначенного для поддержания текущей потребляемой мощности $W_\Pi(\theta_m)$ (тока $i_\Pi(\theta_m)$) в окрестности номинального значения $W_\Pi^{\text{ном}}(\theta_m)$ ($i_\Pi^{\text{ном}}(\theta_m)$) путем поддержания текущего напряжения $u_{\text{ШСР}}(\theta_m)$ в окрестности номинального $u_{\text{ШСР}}^{\text{ном}}$;

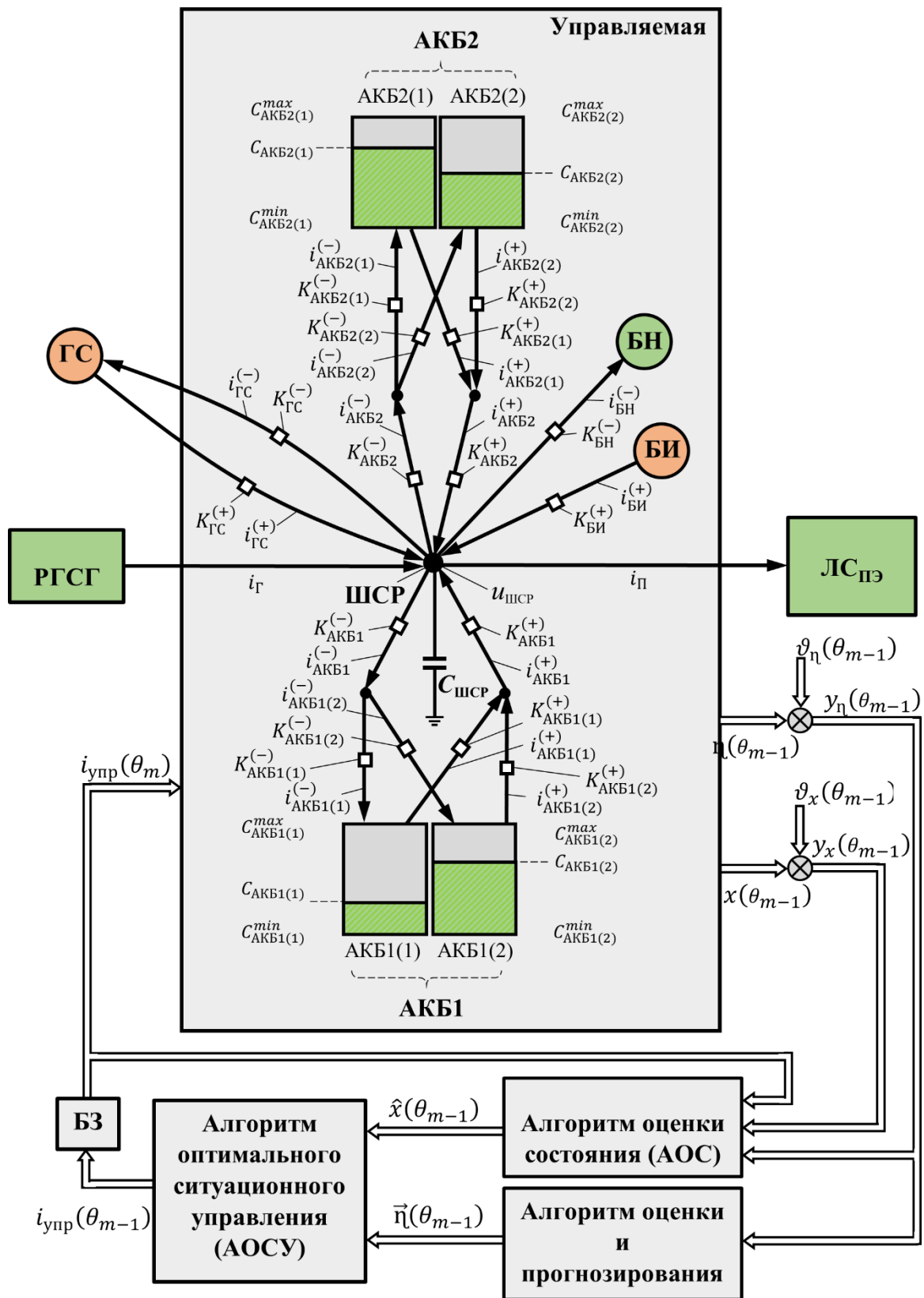


Рисунок 1 – Функциональная схема замкнутой цифровой системы управления энергетическим балансом в системе НРПМ

- $i_{\text{АКБ1}}^{(-)}(\theta_m)$, $i_{\text{АКБ1}}^{(+)}(\theta_m)$ – соответственно зарядный, разрядный управляемые токи системы аккумуляторных батарей 1-го уровня АКБ1, предназначенные для управления энергетическим балансом в управляемой системе НРПМ при нормальных режимах функционирования систем РГСГ, ЛСПЭ и изменении потенциальных мощностей ВИЭ и

мощности потребления $W_{\Pi}(\theta_m)$ в пределах их доверительных интервалов, оцененных на основе статистических данных на этапе синтеза оптимальной структуры системы РГСГ [9]. Включение в режим зарядки/разрядки и отключение АКБ1 моделируется состоянием условных двухпозиционных ключей $K_{\text{АКБ1}}^{(-)}(\theta_m) \in \{0, 1\}$, $K_{\text{АКБ1}}^{(-)}(\theta_m) \in \{0, 1\}$ следующим образом: $K_{\text{АКБ1}}^{(-)}(\theta_m) = 1$, $K_{\text{АКБ1}}^{(-)}(\theta_m) = 0$ – режим зарядки; $K_{\text{АКБ1}}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ1}}^{(-)}(\theta_m) = 1$ – режим разрядки; $K_{\text{АКБ1}}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ1}}^{(-)}(\theta_m) = 0$ – отключение АКБ1 (0 – дуга графа отключена, 1 – включена);

- АКБ1(1), АКБ1(2) – две идентичные аккумуляторные батареи накопителя 1-го уровня АКБ1, поочередно работающие в режиме зарядки/разрядки;

- $i_{\text{АКБ1}(1)}^{(-)}(\theta_m)$, $i_{\text{АКБ1}(2)}^{(-)}(\theta_m)$ – соответственно зарядный управляемый ток 1-го контура АКБ1(1), разрядный управляемый ток 2-го контура АКБ1(2) накопителя 1-го уровня АКБ1, когда параллельные контуры АКБ1(1), АКБ1(2) работают в режиме соответственно зарядки, разрядки. Включение в данный режим моделируется состоянием условных двухпозиционных ключей $K_{\text{АКБ1}(1)}^{(-)}(\theta_m) \in \{0, 1\}$, $K_{\text{АКБ1}(1)}^{(-)}(\theta_m) \in \{0, 1\}$, $K_{\text{АКБ1}(2)}^{(-)}(\theta_m) \in \{0, 1\}$, $K_{\text{АКБ1}(2)}^{(-)}(\theta_m) \in \{0, 1\}$ следующим образом: $K_{\text{АКБ1}(1)}^{(-)}(\theta_m) = 1$, $K_{\text{АКБ1}(1)}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ1}(2)}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ1}(2)}^{(-)}(\theta_m) = 1$;

- $i_{\text{АКБ1}(1)}^{(-)}(\theta_m)$, $i_{\text{АКБ1}(2)}^{(-)}(\theta_m)$ – соответственно разрядный управляемый ток 1-го контура АКБ1(1), зарядный управляемый ток 2-го контура АКБ1(2) накопителя 1-го уровня АКБ1, когда параллельные контуры АКБ1(1), АКБ1(2) работают в режиме соответственно разрядки, зарядки. Включение в данный режим моделируется состоянием условных двухпозиционных ключей следующим образом: $K_{\text{АКБ1}(1)}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ1}(1)}^{(-)}(\theta_m) = 1$, $K_{\text{АКБ1}(2)}^{(-)}(\theta_m) = 1$, $K_{\text{АКБ1}(2)}^{(-)}(\theta_m) = 0$;

- $C_{\text{АКБ1}(j)}(\theta_m)$, $C_{\text{АКБ1}(j)}^{\max}$, $C_{\text{АКБ1}(j)}^{\min}$, $j \in \{1, 2\}$ – соответственно текущее состояние (остаточная емкость), полная емкость, минимальная емкость, характеризующая максимальную (допустимую) глубину разряда j -го контура АКБ1(j) накопителя 1-го уровня АКБ1.

- $i_{\text{АКБ2}}^{(-)}(\theta_m)$, $i_{\text{АКБ2}}^{(-)}(\theta_m)$ – соответственно зарядный, разрядный управляемые токи системы аккумуляторных батарей 2-го уровня АКБ2, предназначенные для управления энергетическим балансом в управляемой системе НРПМ совместно с управляемыми токами зарядки/разрядки системы АКБ1 1-го уровня, при аварийных режимах функционирования систем РГСГ, ЛС_{ПЭ} и выходе потенциальных мощностей ВИЭ (1) и мощности потребления $W_{\Pi}(\theta_m)$ (2) за пределы их доверительных интервалов, оцененных на основе статистических данных на этапе синтеза оптимальной структуры системы РГСГ [9]. Включение в режим зарядки/разрядки и отключение АКБ2 моделируется состоянием условных двухпозиционных ключей $K_{\text{АКБ2}}^{(-)}(\theta_m) \in \{0, 1\}$, $K_{\text{АКБ2}}^{(-)}(\theta_m) \in \{0, 1\}$ следующим образом: $K_{\text{АКБ2}}^{(-)}(\theta_m) = 1$, $K_{\text{АКБ2}}^{(-)}(\theta_m) = 0$ – режим зарядки; $K_{\text{АКБ2}}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ2}}^{(-)}(\theta_m) = 1$ – режим разрядки; $K_{\text{АКБ2}}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ2}}^{(-)}(\theta_m) = 0$ – отключение АКБ2 (0 – дуга графа отключена, 1 – включена);

- АКБ2(1), АКБ2(2) – две идентичные аккумуляторные батареи накопителя 2-го уровня АКБ2, поочередно работающие в режиме зарядки/разрядки;

- $i_{\text{АКБ2}(1)}^{(-)}(\theta_m)$, $i_{\text{АКБ2}(2)}^{(-)}(\theta_m)$ – соответственно зарядный управляемый ток 1-го контура АКБ2(1), разрядный управляемый ток 2-го контура АКБ2(2) накопителя 2-го уровня АКБ2, когда параллельные контуры АКБ2(1), АКБ2(2) работают в режиме соответственно зарядки, разрядки. Включение в данный режим моделируется состоянием условных двухпозиционных ключей $K_{\text{АКБ2}(1)}^{(-)}(\theta_m) \in \{0, 1\}$, $K_{\text{АКБ2}(1)}^{(-)}(\theta_m) \in \{0, 1\}$, $K_{\text{АКБ2}(2)}^{(-)}(\theta_m) \in \{0, 1\}$,

$K_{\text{АКБ2}(2)}^{(-)}(\theta_m) \in \{0, 1\}$ следующим образом: $K_{\text{АКБ2}(1)}^{(-)}(\theta_m) = 1$, $K_{\text{АКБ2}(1)}^{(-)}(\theta_m) = 0$,
 $K_{\text{АКБ2}(2)}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ2}(2)}^{(-)}(\theta_m) = 1$;

- $i_{\text{АКБ2}(1)}^{(-)}(\theta_m)$, $i_{\text{АКБ2}(2)}^{(-)}(\theta_m)$ – соответственно разрядный управляемый ток 1-го контура АКБ2(1), зарядный управляемый ток 2-го контура АКБ2(2) накопителя 2-го уровня АКБ2, когда параллельные контуры АКБ2(1), АКБ2(2) работают в режиме соответственно разрядки, зарядки. Включение в данный режим моделируется состоянием условных двухпозиционных ключей следующим образом: $K_{\text{АКБ2}(1)}^{(-)}(\theta_m) = 0$, $K_{\text{АКБ2}(1)}^{(-)}(\theta_m) = 1$,
 $K_{\text{АКБ2}(2)}^{(-)}(\theta_m) = 1$, $K_{\text{АКБ2}(2)}^{(-)}(\theta_m) = 0$;

- $C_{\text{АКБ2}(j)}(\theta_m)$, $C_{\text{АКБ2}(j)}^{\max}$, $C_{\text{АКБ2}(j)}^{\min}$, $j \in \{1, 2\}$ – соответственно текущее состояние (остаточная емкость), полная емкость, минимальная емкость, характеризующая максимальную (допустимую) глубину разряда j -го контура АКБ2(j) накопителя 2-го уровня АКБ2;

- $i_{\text{БИ}}^{(-)}(\theta_m)$, $i_{\text{БН}}^{(-)}(\theta_m)$ – соответственно управляемый ток, соответствующий управляемой резервной мощности $W_{\text{БИ}}^{(-)}(\theta_m)$, вырабатываемой балансирующим источником (БИ) энергии и управляемый ток, соответствующий управляемой мощности $W_{\text{БН}}^{(-)}(\theta_m)$, потребляемой резервной балансирующей нагрузкой БН. Здесь БИ и БН используются как резервные оборудования для управления энергетическим балансом в системе НРПМ совместно с АКБ1, АКБ2 при аварийных режимах функционирования систем РГСГ, ЛС_{ПЭ} и при существенном выходе мощностей ВИЭ (1) и мощности потребления $W_{\text{П}}(\theta_m)$ (2) за пределы их доверительных интервалов, оцененных на основе статистических данных на этапе синтеза оптимальной структуры РГСГ [9]. Включение/отключение БН и БИ моделируется состоянием условных двухпозиционных ключей следующим образом: $K_{\text{БН}}^{(-)}(\theta_m) = 0$, $K_{\text{БИ}}^{(-)}(\theta_m) = 1$ – БН отключена, БИ включен; $K_{\text{БН}}^{(-)}(\theta_m) = 1$, $K_{\text{БИ}}^{(-)}(\theta_m) = 0$ – БН включена, БИ отключен; $K_{\text{БН}}^{(-)}(\theta_m) = 0$, $K_{\text{БИ}}^{(-)}(\theta_m) = 0$ – БН и БИ отключены.

- $i_{\text{ГС}}^{(-)}(\theta_m)$, $i_{\text{ГС}}^{(-)}(\theta_m)$ – соответственно управляемый ток, соответствующий управляемому перетоку мощности $W_{\text{ГС}}^{(-)}(\theta_m)$ от ГС к НРПМ, управляемый ток, соответствующий управляемому перетоку мощности $W_{\text{ГС}}^{(-)}(\theta_m)$ от НРПМ к ГС. При этом результирующий ток $i_{\text{ГС}}^{(-,-)}(\theta_m)$:

$$i_{\text{ГС}}^{(-,-)}(\theta_m) = K_{\text{ГС}}^{(-)}(\theta_m) \cdot i_{\text{ГС}}^{(-)}(\theta_m) - K_{\text{ГС}}^{(-)}(\theta_m) \cdot i_{\text{ГС}}^{(-)}(\theta_m) \quad (3)$$

должен соответствовать в каждый текущий момент времени θ_m заданному результирующему графику перетока мощности $W_{\text{ГС}}^{(-,-)}(\theta_m)$ между ГС и НРПМ для сохранения динамической устойчивости ЭЭС в целом. Включение в режимы перетока от ГС к НРПМ, от НРПМ к ГС и отключение НРПМ от ГС моделируется состоянием условных двухпозиционных ключей следующим образом: $K_{\text{ГС}}^{(-)}(\theta_m) = 0$, $K_{\text{ГС}}^{(-)}(\theta_m) = 1$ – переток от ГС к НРПМ; $K_{\text{ГС}}^{(-)}(\theta_m) = 1$, $K_{\text{ГС}}^{(-)}(\theta_m) = 0$ – переток от НРПМ к ГС; $K_{\text{ГС}}^{(-)}(\theta_m) = 0$, $K_{\text{ГС}}^{(-)}(\theta_m) = 0$ – отключение НРПМ от ГС;

- из вышесказанного следует, что приоритетность включения элементов системы НРПМ к процессу управления энергетическим балансом в ней отражает следующая последовательность:

$$C_{\text{ШСР}} \longrightarrow \text{АКБ1} \longrightarrow \text{АКБ2} \longrightarrow (\text{БИ, БН}) \longrightarrow \text{ГС}. \quad (4)$$

1.2. Контур управления функциональной схемы замкнутой цифровой системы, показанной на рисунке 1, в общем случае, включает:

- $x(\theta_m)$ – вектор состояния управляемой системы НРПМ:

$$x(\theta_m) = (u_{\text{ШСР}}(\theta_m), C_{\text{АКБ1(1)}}(\theta_m), C_{\text{АКБ1(2)}}(\theta_m), C_{\text{АКБ2(1)}}(\theta_m), C_{\text{АКБ2(2)}}(\theta_m)); \quad (5)$$

- $\eta(\theta_m)$ – вектор возмущения, действующий на управляемую систему НРПМ:

$$\eta(\theta_m) = (i_{\Gamma}(\theta_m), i_{\Pi}(\theta_m)); \quad (6)$$

- $y_x(\theta_m), y_{\eta}(\theta_m)$ – соответственно вектор наблюдения за состоянием $x(\theta_m)$ (5), вектор наблюдения за возмущением $\eta(\theta_m)$ (6):

$$y_x(\theta_m) = x(\theta_m) + \vartheta_x(\theta_m), \quad (7)$$

$$y_{\eta}(\theta_m) = \eta(\theta_m) + \vartheta_{\eta}(\theta_m), \quad (8)$$

где $\vartheta_x(\theta_m), \vartheta_{\eta}(\theta_m)$ – векторы ошибок измерения с соответствующими размерностями;

- $i_{\text{упр}}(\theta_m)$ – вектор управления энергетическим балансом в управляемой системе НРПМ:

$$i_{\text{упр}}(\theta_m) = (i_{\text{АКБ1(1)}}^{(-)}(\theta_m), i_{\text{АКБ1(1)}}^{(-)}(\theta_m), i_{\text{АКБ1(2)}}^{(-)}(\theta_m), i_{\text{АКБ1(2)}}^{(-)}(\theta_m), i_{\text{АКБ2(1)}}^{(-)}(\theta_m), i_{\text{АКБ2(1)}}^{(-)}(\theta_m), i_{\text{АКБ2(2)}}^{(-)}(\theta_m), i_{\text{АКБ2(2)}}^{(-)}(\theta_m), i_{\text{БН}}^{(-)}(\theta_m), i_{\text{БИ}}^{(-)}(\theta_m)); \quad (9)$$

- АОС – модуль в контуре управления, реализующий алгоритм $G_{\text{АОС}, \theta_m}$ оценки состояния управляемой системы НРПМ. В каждый текущий момент времени θ_m на вход данного модуля поступают вектор наблюдения $y_x(\theta_m)$ (7) за вектором состояния $x(\theta_m)$ (5), вектор наблюдения $y_{\eta}(\theta_m)$ (8) за вектором возмущения $\eta(\theta_m)$ (6), вектор управления $i_{\text{упр}}(\theta_m)$ энергетическим балансом в управляемой системе НРПМ. Выходом является оптимальная оценка $\hat{x}(\theta_m)$ текущего вектора состояния $x(\theta_m)$ (5) системы НРПМ;

- АОП – модуль в контуре управления, реализующий алгоритм $G_{\text{АОП}, \theta_m}$ оценки и прогнозирования вектора возмущения, действующего на управляемую систему НРПМ. В каждый текущий момент времени θ_m на вход данного модуля поступает вектор наблюдения $y_{\eta}(\theta_m)$ (8) за вектором возмущения $\eta(\theta_m)$ (6). Выходом является оценка текущего вектора возмущения (6) и его прогноз на определенный интервал времени:

$$\vec{\eta}(\theta_m) = \{\hat{\eta}(\theta_l | \theta_m) \mid l \in \{m, m+1, \dots, m+M-1\}\} = \{(i_{\Gamma}(\theta_l | \theta_m), i_{\Pi}(\theta_l | \theta_m)) \mid l \in \{m, m+1, \dots, m+M-1\}\}, \quad (10)$$

где θ_m, θ_{m-M-1} – соответственно начало, конец интервала времени оценки и прогнозирования; $\hat{\eta}(\theta_m) = \hat{\eta}(\theta_m | \theta_m)$ при $l = m$ – текущая оценка вектора возмущения (6); $\hat{\eta}(\theta_l | \theta_m), l > m$ – прогноз вектора возмущения (6);

- АОСУ – модуль в контуре управления, реализующий структурно и логически самоорганизующегося многокомпонентного алгоритма оптимального ситуационного управления энергетическим балансом в управляемой системе НРПМ с целью поддержания тока $i_{\Pi}(\theta_m)$, соответствующего текущей потребляемой мощности $W_{\Pi}(\theta_m)$ (2) региональными потребителями, в окрестности номинального тока $i_{\Pi}^{\text{ном}}(\theta_m)$, соответствующего требуемой номинальной мощности $W_{\Pi}^{\text{ном}}(\theta_m)$, за счет поддержания текущего напряжения $u_{\text{ШСР}}(\theta_m)$ в окрестности номинального $u_{\text{ШСР}}^{\text{ном}}$, а также обеспечение равенства текущего результирующего тока $i_{\Gamma}^{(-,-)}(\theta_m)$ (3) заданному (желаемому) току $i_{\Gamma}^{(-,-)*}(\theta_m)$, соответствующему графику перетока мощности $W_{\Gamma}^{(-,-)*}(\theta_m)$ между ГС и НРПМ

для сохранения динамической устойчивости ЭЭС в целом. В каждый текущий момент времени θ_m на вход данного модуля поступают в общем случае вектор оптимальной оценки состояния $\hat{x}(\theta_m)$ из выхода модуля АОС, оценка и прогноз $\vec{\eta}(\theta_m)$ (10) вектора возмущения (6) из выхода АОП. Выходом является вектор управления $i_{упр}(\theta_m)$ (9). Тогда обобщенная структура алгоритма управления $G_{АОС\vec{\eta},\theta_m}$ примет следующий вид:

$$i_{упр}(\theta_m) = G_{АОС\vec{\eta},\theta_m}[\hat{x}(\theta_m), \vec{\eta}(\theta_m)]. \quad (11)$$

Такая структура соответствует многошаговой задаче оптимизации. При одношаговой задаче оптимизации необходимость в решении задачи прогнозирования вектора возмущения (6) отпадает. Тогда структура алгоритма примет следующий вид:

$$i_{упр}(\theta_m) = G_{АОС\hat{\eta},\theta_m}[\hat{x}(\theta_m), \hat{\eta}(\theta_m)], \quad (12)$$

где $\hat{\eta}(\theta_m) = (\hat{\eta}_r(\theta_m), \hat{\eta}_n(\theta_m))$ – оценка текущего вектора возмущения (6). Если же ошибки измерения цифровых датчиков существенно малы, то:

$$i_{упр}(\theta_m) = G_{АОС\eta,\theta_m}[x(\theta_m), \eta(\theta_m)], \quad (13)$$

т.е. необходимость в решении задач оценки векторов состояния (5), возмущения (6) отпадает.

- БЗ – блок задержки, моделирующий время запаздывания $\tau_{к\vec{\eta}}$ в контуре управления (КУ), т.е. время $\tau_{к\vec{\eta}}$ от момента фиксации (измерения) $\theta_m - \tau_{к\vec{\eta}}$ вектора текущей информации:

$$y_{к\vec{\eta}}(\theta_m - \tau_{к\vec{\eta}}) = (y_x(\theta_m - \tau_{к\vec{\eta}}), y_\eta(\theta_m - \tau_{к\vec{\eta}})) \quad (14)$$

до момента θ_m реализации вектора управляющих воздействий $i_{упр}(\theta_m)$ (9), определенного, на основе информации $y_{к\vec{\eta}}(\theta_m - \tau_{к\vec{\eta}})$ (14), (5), (6), с помощью вычислительных алгоритмов:

$$G_{к\vec{\eta},\theta_m - \tau_{к\vec{\eta}}} : G_{АОС,\theta_m - \tau_{к\vec{\eta}}} \longrightarrow G_{АОП,\theta_m - \tau_{к\vec{\eta}}} \longrightarrow G_{АОС\vec{\eta},\theta_m - \tau_{к\vec{\eta}}} \quad (15)$$

реализованных на одной микропроцессорной системе. При этом величина запаздывания $\tau_{к\vec{\eta}}$ зависит от структуры организации процесса передачи информации $y_{к\vec{\eta}}(\theta_m - \tau_{к\vec{\eta}})$ (14) по цифровому каналу связи и вычислительного процесса при реализации алгоритма $G_{к\vec{\eta},\theta_m - \tau_{к\vec{\eta}}}$ (15), а также зависит от следующих параметров: от размерностей $r_{y_{к\vec{\eta}}} = r_{y_x} + r_{y_\eta} = |y_x| + |y_\eta|$, $r_{i_{упр}} = |i_{упр}|$, соответственно, векторов $y_{к\vec{\eta}}$ (14), $i_{упр}$ (9); от количества вычислительных операций $O_{ГКУ} = O_{ГАОС} + O_{АОП} + O_{АОС\vec{\eta}}$ алгоритма (15); от длины $n_{код}$ кодовой комбинации $(n_{код}, k_{код})$ кода контролирующей ошибки, используемого для передачи каждого элемента векторов y , $i_{упр}$ по цифровому каналу, где $k_{код}$ – число информационных символов первичного кода цифрового датчика, от которого зависит точность квантования по уровню измеряемой величины;

- условие физической реализуемости процесса, протекающего в контуре управления, на цифровых устройствах в дискретные моменты времени θ_m , $m = 0, 1, 2, \dots$ с дискретой $\Delta\theta$:

$$\Delta\theta \geq \tau_{к\vec{\eta}}. \quad (16)$$

- системное быстроедействие цифрового контура управления определяется парой $(\Delta\theta, \tau_{к\vec{\eta}})$.

Далее примем $\Delta\theta = \tau_{\text{КС}}$, что соответствует режиму запаздывания на один такт дискретного времени θ_m , $m = 0, 1, 2, \dots$ с дискретой

$$\Delta\theta = \theta_{m-1} - \theta_m = \tau_{\text{КС}}. \quad (17)$$

2. Формулировка задачи синтеза алгоритма оптимального ситуационного управления энергетическим балансом в управляемой системе НРПМ

Здесь рассматривается задача разработки (синтеза) модуля АОСУ в рамках структуры замкнутой цифровой системы управления (ЗЦСУ) энергетическим балансом в управляемой системе НРПМ, функциональная схема которой показана на рисунке 1. Формулируется исходная содержательная постановка задачи синтеза модуля АОСУ на основе вышеприведенного описания функциональной схемы ЗЦСУ при предположении, что текущая исходная информация об оценке и прогнозирования $\hat{x}(\theta_m)$, $\bar{u}(\theta_m)$ определена.

Задача 1 – исходная содержательная постановка задачи синтеза. Найти алгоритм цифрового управления $G_{\text{АОСУ}, \theta_m}$ в виде (11), вырабатывающий в каждый текущий момент времени θ_m , $m = 0, 1, 2, \dots, \infty$ на основе текущей информации $\hat{x}(\theta_m)$, $\bar{u}(\theta_m)$, вектор управляющих воздействий $i_{\text{уп}}(\theta_m)$ (9) путем формирования текущей структуры управляемой системы НРПМ за счет выбора соответствующего состояния каждого ключа из множества $K_{\text{НРПМ}}$:

$$K_{\text{НРПМ}} = \left\{ K_{\text{АКБ1}}^{(-)}(\theta_m), K_{\text{АКБ1}}^{(-)}(\theta_m), K_{\text{АКБ1(1)}}^{(-)}(\theta_m), K_{\text{АКБ1(1)}}^{(-)}(\theta_m), K_{\text{АКБ1(2)}}^{(-)}(\theta_m), K_{\text{АКБ1(2)}}^{(-)}(\theta_m), \right. \\ K_{\text{АКБ2}}^{(-)}(\theta_m), K_{\text{АКБ2}}^{(-)}(\theta_m), K_{\text{АКБ2(1)}}^{(-)}(\theta_m), K_{\text{АКБ2(1)}}^{(-)}(\theta_m), K_{\text{АКБ2(2)}}^{(-)}(\theta_m), K_{\text{АКБ2(2)}}^{(-)}(\theta_m), \\ \left. K_{\text{БН}}^{(-)}(\theta_m), K_{\text{БИ}}^{(-)}(\theta_m), K_{\text{ГС}}^{(-)}(\theta_m), K_{\text{ГС}}^{(-)}(\theta_m) \right\}, \quad (18)$$

и выбора величин токов вектора $i_{\text{уп}}(\theta_m)$ (9), соответствующих включенным дугам графа структуры НРПМ (отключенным дугам соответствуют токи с нулевым значением), с целью поддержания текущего потребляемого тока $i_{\text{П}}(\theta_m)$, соответствующего мощности потребления $W_{\text{П}}(\theta_m)$ (2), в окрестности номинального значения $i_{\text{П}}^{\text{НОМ}}(\theta_m)$, соответствующего номинальной мощности $W_{\text{П}}^{\text{НОМ}}(\theta_m)$, за счет поддержания текущего напряжения $u_{\text{ШСР}}(\theta_m)$ в окрестности номинального $u_{\text{ШСР}}^{\text{НОМ}} = \text{const}$, а также поддержания тока $i_{\text{ГС}}^{(-)}(\theta_m)$ в окрестности номинального $i_{\text{ГС}}^{\text{НОМ}}(\theta_m)$, характеризующего заданный график перетока мощности $W_{\text{ГС}}^{\text{НОМ}}(\theta_m)$ между ГС и НРПМ, для сохранения динамической устойчивости ЭЭС в целом, т.е. с целью обеспечения следующих соотношений ($\varepsilon_{\text{ШСР}}$, $\varepsilon_{\text{ГС}}$ – допустимые величины отклонения):

$$u_{\text{ШСР}}^{\text{НОМ}} - \varepsilon_{\text{ШСР}} \leq u_{\text{ШСР}}(\theta_m) \leq u_{\text{ШСР}}^{\text{НОМ}} + \varepsilon_{\text{ШСР}} \quad (19)$$

$$i_{\text{ГС}}^{\text{НОМ}}(\theta_m) - \varepsilon_{\text{ГС}} \leq i_{\text{ГС}}^{(-)}(\theta_m) \leq i_{\text{ГС}}^{\text{НОМ}}(\theta_m) + \varepsilon_{\text{ГС}}, \quad (20)$$

$$\forall m \in \{0, 1, 2, \dots, \infty\},$$

с учетом следующих условий:

- модель состояния (напряжения) конденсатора, характеризующая баланс токов узла ШСР;
- модель процесса функционирования АКБ $i(j)$, $i \in \{1, 2\}$, $j \in \{1, 2\}$, ДГ, БН;
- условие физической реализуемости процесса, протекающего в контуре управления, на цифровых устройствах в дискретные моменты времени θ_m , $m = 0, 1, 2, \dots$ с дискретой $\Delta\theta$.

Формальное описание этих условий приведено ниже, при разработке схемы решения данной задачи.

3. Схема решения задачи синтеза алгоритма оптимального ситуационного управления энергетическим балансом в управляемой системе НРПМ

Схема решения задачи синтеза модуля АОСУ, т.е. задачи 1, включает следующие этапы.

Этап 1 – построение математической модели баланса токов в управляемой системе НРПМ. Для синтеза модуля АОСУ строится математическая модель, описывающая состояние (напряжение) конденсатора в дискретные моменты времени, и характеризующая баланс токов узла ШСР:

$$\begin{aligned}
 u_{\text{ШСР}}(\theta_{m-1}) = u_{\text{ШСР}}(\theta_m) + \frac{\Delta\theta}{C_{\text{ШСР}}} & \left[\left(K_{\text{АКБ1}}^{(-)}(\theta_m) \cdot i_{\text{АКБ1}}^{(-)}(\theta_m) - K_{\text{АКБ1}}^{(-)}(\theta_m) \cdot i_{\text{АКБ1}}^{(-)}(\theta_m) \right) + \right. \\
 & + \left(K_{\text{АКБ2}}^{(-)}(\theta_m) \cdot i_{\text{АКБ2}}^{(-)}(\theta_m) - K_{\text{АКБ2}}^{(-)}(\theta_m) \cdot i_{\text{АКБ2}}^{(-)}(\theta_m) \right) + \\
 & + \left(K_{\text{БИ}}^{(-)}(\theta_m) \cdot i_{\text{БИ}}^{(-)}(\theta_m) - K_{\text{БИ}}^{(-)}(\theta_m) \cdot i_{\text{БИ}}^{(-)}(\theta_m) \right) + \\
 & \left. + \left(K_{\text{ГС}}^{(-)}(\theta_m) \cdot i_{\text{ГС}}^{(-)}(\theta_m) - K_{\text{ГС}}^{(-)}(\theta_m) \cdot i_{\text{ГС}}^{(-)}(\theta_m) \right) \right] + \frac{\Delta\theta}{C_{\text{ШСР}}} (i_{\text{Г}}(\theta_m) - i_{\text{П}}(\theta_m)). \quad (21)
 \end{aligned}$$

Этап 2 – учет информации в математической модели о приоритетности включения элементов НРПМ в процесс управления энергетическим балансом в ней. Здесь, на основе исходного графа структуры управляемой системы НРПМ, показанного на рисунке 1, уравнения (21), характеризующего баланс токов относительно узла ШСР и понятия балансирующего тока, введенного в работе [9], строится структурированный эквивалентный граф с многоуровневой структурой в соответствии с информацией о приоритетности включения элементов НРПМ (4) в процесс управления энергетическим балансом в ней. Граф с таким свойством показан на рисунке 2, где произведена структуризация узла ШСР.

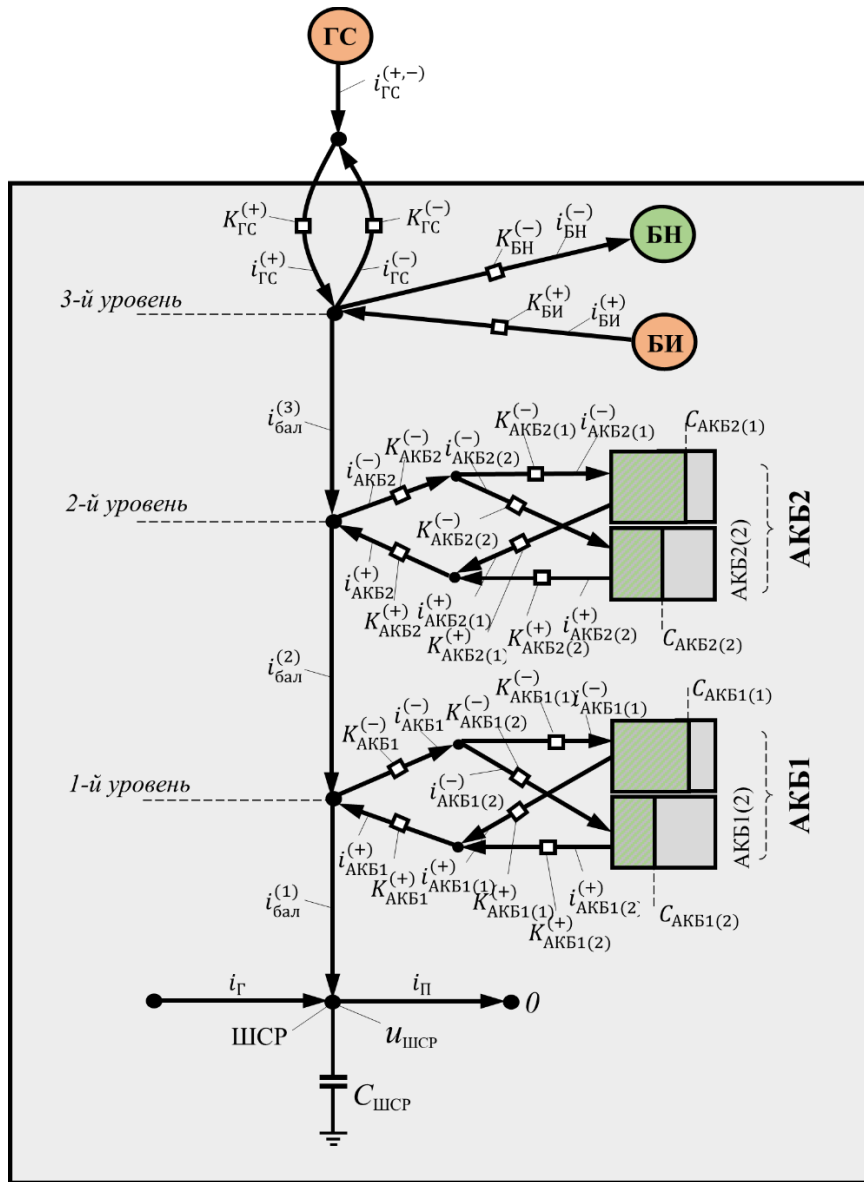


Рисунок 2 – Эквивалентный граф структуры управляемой системы НРПМ, содержащий информацию о приоритетности участия ее элементов в процессе управления энергетическим балансом в ней

В соответствии с многоуровневой структурой эквивалентного графа модель (21) представляется как модель с многоуровневой структурой:

- уравнение состояния (напряжения) узла ШСР – уравнение состояния (напряжения) конденсатора

$$u_{\text{ШСР}}(\theta_{m-1}) = u_{\text{ШСР}}(\theta_m) + \frac{\Delta\theta}{C_{\text{ШСР}}} \cdot i_{\text{оэл}}^{(1)}(\theta_m) + \frac{\Delta\theta}{C_{\text{ШСР}}} (i_{\Gamma}(\theta_m) - i_{\Pi}(\theta_m)); \quad (22)$$

- уравнение баланса токов узла 1-го уровня

$$i_{\text{оэл}}^{(1)}(\theta_m) = (K_{\text{АКБ1}}^{(-)}(\theta_m) \cdot i_{\text{АКБ1}}^{(-)}(\theta_m) - K_{\text{АКБ1}}^{(+)}(\theta_m) \cdot i_{\text{АКБ1}}^{(+)}(\theta_m)) + i_{\text{оэл}}^{(2)}(\theta_m); \quad (23)$$

- уравнение баланса токов узла 2-го уровня

$$i_{\text{оэл}}^{(2)}(\theta_m) = (K_{\text{АКБ2}}^{(-)}(\theta_m) \cdot i_{\text{АКБ2}}^{(-)}(\theta_m) - K_{\text{АКБ2}}^{(+)}(\theta_m) \cdot i_{\text{АКБ2}}^{(+)}(\theta_m)) + i_{\text{оэл}}^{(3)}(\theta_m); \quad (24)$$

- уравнение баланса токов узла 3-го уровня

$$i_{\delta\alpha\lambda}^{(3)}(\theta_m) = \left(K_{\text{БИ}}^{(-)}(\theta_m) \cdot i_{\text{БИ}}^{(-)}(\theta_m) - K_{\text{БН}}^{(-)}(\theta_m) \cdot i_{\text{БН}}^{(-)}(\theta_m) \right) + i_{\text{ГС}}^{(-,-)}(\theta_m); \quad (25)$$

- требование к перетоку (3) между ГС и управляемой системой НРПМ:

$$i_{\text{ГС}}^{\text{ном}}(\theta_m) = i_{\text{ГС}}^{(-,-)}(\theta_m), \quad (26)$$

где $i_{\delta\alpha\lambda}^{(j)}(\theta_m)$, $j \in \{1, 2, 3\}$ – балансирующий ток j -го уровня иерархии.

Последовательная подстановка выражений (26) $\rightarrow$ (25) $\rightarrow$ (24) $\rightarrow$ (23) $\rightarrow$ (22) дает исходную модель (21), что свидетельствует об эквивалентности исходного графа (см. рис. 1) и структурированного многоуровневого графа (см. рис. 2) с позиции энергетического баланса, однако они не эквивалентны с позиции содержания в них информации о приоритетности включения элементов системы НРПМ (4) в процесс управления энергетическим балансом в ней.

Балансирующий ток 1-го уровня $i_{\delta\alpha\lambda}^{(1)}(\theta_m)$ в уравнении (22) выступает как результирующее управляющее воздействие для поддержания напряжения $u_{\text{ШСР}}(\theta_m)$ узла ШСР в окрестности номинального $u_{\text{ШСР}}^{\text{ном}}$, а выражения (23) - (26) являются уравнениями реализации балансирующего тока $i_{\delta\alpha\lambda}^{(1)}(\theta_m)$ путем формирования текущей структуры управляемой системы НРПМ за счет выбора соответствующих состояний условных ключей из (18) и выбора величин токов вектора управляющих воздействий $i_{\text{упр}}(\theta_m)$ (9), соответствующих включенным дугам (отключенным дугам соответствуют токи с нулевым значением).

Этап 3 – учет запаздывания в контуре цифрового управления. Уравнение напряжения конденсатора (узла ШСР) (22) записывается с учетом задержки на один такт (17) балансирующего тока $i_{\delta\alpha\lambda}^{(1)}(\theta_m)$, за счет запаздывания вектора управляющих воздействий $i_{\text{упр}}(\theta_m)$ (9) в контуре управления КУ:

$$\begin{cases} u_{\text{ШСР}}(\theta_{m-1}) = u_{\text{ШСР}}(\theta_m) + \frac{\Delta\theta}{C_{\text{ШСР}}} \cdot i_{\text{БЗ}}(\theta_m) + \frac{\Delta\theta}{C_{\text{ШСР}}} (i_{\text{Г}}(\theta_m) - i_{\text{П}}(\theta_m)), \\ i_{\text{БЗ}}(\theta_{m-1}) = i_{\delta\alpha\lambda}^{(1)}(\theta_m), \end{cases} \quad (27)$$

где $i_{\text{БЗ}}(\theta_{m-1})$ – запаздавший на один такт дискретного времени балансирующий ток $i_{\delta\alpha\lambda}^{(1)}(\theta_{m-1})$.

Этап 4 – формирование уравнения состояния и требований к режимам зарядки/разрядки системы аккумуляторных батарей (см. рис. 2):

- уравнение состояния аккумуляторных батарей АКБ $i(j)$, $i \in \{1, 2\}$, $j \in \{1, 2\}$

$$C_{\text{АКБ}i(j)}(\theta_{m-1}) = C_{\text{АКБ}i(j)}(\theta_m) + \Delta\theta \cdot i_{\text{АКБ}i(j)}^{(-)}(\theta_m) - \Delta\theta \cdot i_{\text{АКБ}i(j)}^{(-)}(\theta_m), \quad (28)$$

где:

$$i_{\text{АКБ}i(j)}^{(-)}(\theta_m) = K_{\text{АКБ}i}^{(-)}(\theta_m) \cdot K_{\text{АКБ}i(j)}^{(-)} \cdot i_{\text{АКБ}i}^{(-)}(\theta_m), \quad (29)$$

$$i_{\text{АКБ}i(j)}^{(-)}(\theta_m) = K_{\text{АКБ}i}^{(-)}(\theta_m) \cdot K_{\text{АКБ}i(j)}^{(-)} \cdot i_{\text{АКБ}i}^{(-)}(\theta_m); \quad (30)$$

требования к режимам зарядки/разрядки аккумуляторных батарей АКБ $i(j)$, $i \in \{1, 2\}$, $j \in \{1, 2\}$ [2]:

$$C_{\text{АКБ}i(j)}^{\min} \leq C_{\text{АКБ}i(j)}(\theta_m) \leq C_{\text{АКБ}i(j)}^{\max}, \quad C_{\text{АКБ}i(j)}^{\min} = 0,3 \cdot C_{\text{АКБ}i(j)}^{\max}; \quad (31)$$

$$i_{AKBi(j)}^{(-)}(\theta_m) \leq 0,1 \cdot C_{AKBi(j)}^{max}; \quad (32)$$

$$i_{AKBi(j)}^{(-)}(\theta_m) \leq 0,15 \cdot C_{AKBi(j)}^{max}. \quad (33)$$

Этап 5 – выявление и анализ ситуаций и построение графа переходов в двухконтурном накопителе (см. рис. 3). Здесь формируется набор ситуаций, возникающих в зависимости от состояний параллельных контуров (АКБі(1), АКБі(2)) двухконтурного накопителя АКБі, $i \in \{1, 2\}$, работающих поочередно в режиме заряда/разряда, даются их формальные определения, строится граф переходов из одной ситуации в другую и формулируются правила переключения параллельных контуров из одного режима работы в другой.

Ниже используется следующая конструкция системы обозначений:

$$\left\{ \begin{array}{l} S_{AKBi}^{(\theta_m)} \left(\frac{a}{R_{(a)}} / \frac{b}{R_{(b)}} \right), \\ a, b \in \{1, 2\}, (a, b) \in \{(1, 2), (2, 1)\}, \\ R_{(a)}, R_{(b)} \in \{\uparrow, \downarrow, \bar{\uparrow}, \bar{\downarrow}\}, \\ (R_{(a)}/R_{(b)}) \in \{(\uparrow/\downarrow), (\downarrow/\uparrow), (\bar{\uparrow}/\bar{\downarrow}), (\bar{\downarrow}/\bar{\uparrow}), (\uparrow/\bar{\downarrow}), (\downarrow/\bar{\uparrow}), (\bar{\uparrow}/\downarrow), (\bar{\downarrow}/\uparrow)\}, \end{array} \right. \quad (34)$$

где $S(\cdot)$ – некоторая ситуация, возникающая в двухконтурном накопителе; a, b – номера контуров; $R_{(a)}, R_{(b)}$ – режимы функционирования контуров с номерами, соответственно, a, b ; $\uparrow, \downarrow, \bar{\uparrow}, \bar{\downarrow}$ – соответственно нормальный режим заряда, нормальный режим разряда, полная (предельная) заряда, полная (предельная) разряда соответствующего контура с номером a или b , т.е. контура АКБі(a) или АКБі(b); $*/$ – некоторое обозначение (или предложение) $*$ в числителе косой черты соответствует контуру с номером a , т.е. контуру АКБі(a), а некоторое обозначение (или предложение) $*$ в знаменателе косой черты – контуру с номером b , т.е. контуру АКБі(b); $(\uparrow/\downarrow), (\downarrow/\uparrow)$ – режимы соответственно полная заряда/полная разряда, (полная разряда/полная заряда); $(\bar{\uparrow}/\bar{\downarrow}), (\uparrow/\bar{\downarrow}), (\downarrow/\bar{\uparrow}), (\bar{\downarrow}/\bar{\uparrow})$ – режимы соответственно (полная заряда/разряда), (заряда/полная разряда), (полная разряда/заряда), (разряда/полная заряда).

Ниже, используя принятую конструкцию системы обозначения ситуаций (34), даются формальные определения всем возможным ситуациям, возникающим в процессе функционирования параллельных контуров (АКБі(a), АКБі(b)) двухконтурного накопителя АКБі, $i \in \{1, 2\}$.

Определение 1 – определение ситуаций, соответствующих нормальным режимам заряда и разряда параллельных контуров (АКБі(a), АКБі(b)):

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\uparrow} / \frac{b}{\downarrow} \right)$ называется нормальной при режиме $(\uparrow/\downarrow)$, если вектор состояния $(C_{AKBi(a)}(\theta_m), C_{AKBi(b)}(\theta_m))$ удовлетворяет следующему условию:

$$(C_{AKBi(a)}(\theta_m) < C_{AKBi(a)}^{max} / C_{AKBi(b)}(\theta_m) > C_{AKBi(b)}^{min}); \quad (35)$$

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\downarrow} / \frac{b}{\uparrow} \right)$ называется нормальной при режиме $(\downarrow/\uparrow)$, если

$$(C_{AKBi(a)}(\theta_m) > C_{AKBi(a)}^{min} / C_{AKBi(b)}(\theta_m) < C_{AKBi(b)}^{max}). \quad (36)$$

Определение 2 – определение ситуаций, соответствующих симметрично-предельным режимам заряда и разряда параллельных контуров (АКБі(a), АКБі(b)):

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\bar{\uparrow}} / \frac{b}{\bar{\downarrow}} \right)$ называется симметрично-предельной при режиме $(\uparrow/\downarrow)$, если

$$(C_{AKBi(a)}(\theta_m) = C_{AKBi(a)}^{max} / C_{AKBi(b)}(\theta_m) = C_{AKBi(b)}^{min}); \quad (37)$$

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\underline{1}} / \frac{b}{\underline{1}} \right)$ называется симметрично-предельной при режиме ($\downarrow/\uparrow$), если

$$(C_{AKBi(a)}(\theta_m) = C_{AKBi(a)}^{min} / C_{AKBi(b)}(\theta_m) = C_{AKBi(b)}^{max}). \quad (38)$$

Определение 3 – определение ситуаций, соответствующих асимметрично-предельным режимам зарядки и разрядки параллельных контуров (AKBi(a), AKBi(b)):

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\underline{1}} / \frac{b}{\underline{1}} \right)$ называется асимметрично-предельно/нормальной при режиме ($\uparrow/\downarrow$), если

$$(C_{AKBi(a)}(\theta_m) = C_{AKBi(a)}^{max} / C_{AKBi(b)}(\theta_m) > C_{AKBi(b)}^{min}); \quad (39)$$

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\underline{1}} / \frac{b}{\underline{1}} \right)$ называется асимметрично-нормально/предельной при режиме ($\uparrow/\downarrow$), если

$$(C_{AKBi(a)}(\theta_m) < C_{AKBi(a)}^{max} / C_{AKBi(b)}(\theta_m) = C_{AKBi(b)}^{min}); \quad (40)$$

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\underline{1}} / \frac{b}{\underline{1}} \right)$ называется асимметрично-предельно/нормальной при режиме ($\downarrow/\uparrow$), если

$$(C_{AKBi(a)}(\theta_m) = C_{AKBi(a)}^{min} / C_{AKBi(b)}(\theta_m) < C_{AKBi(b)}^{max}); \quad (41)$$

- ситуация $S_{AKBi}^{(\theta_m)} \left(\frac{a}{\underline{1}} / \frac{b}{\underline{1}} \right)$ называется асимметрично-нормально/предельной при режиме ($\downarrow/\uparrow$), если

$$(C_{AKBi(a)}(\theta_m) > C_{AKBi(a)}^{min} / C_{AKBi(b)}(\theta_m) = C_{AKBi(b)}^{max}). \quad (42)$$

Переход одной ситуации из набора ситуаций, удовлетворяющих условиям (35)-(42), в другую ситуацию того же набора отражает граф переходов, конкретная структура которого зависит от принятой структуры системы управления процессом функционирования параллельных контуров (AKBi(a), AKBi(b)), т.е. от количества устройств управления токами зарядки и управления токами разрядки, и от схемы соединения их с параллельными контурами (AKBi(a), AKBi(b)). Возможны два варианта такой структуры. Граф структуры одного из вариантов показан на рисунках 1, 2 в составе графа структуры управляемой системы НРПМ (подробное описание этой структуры приведено ниже, в рамках второго варианта).

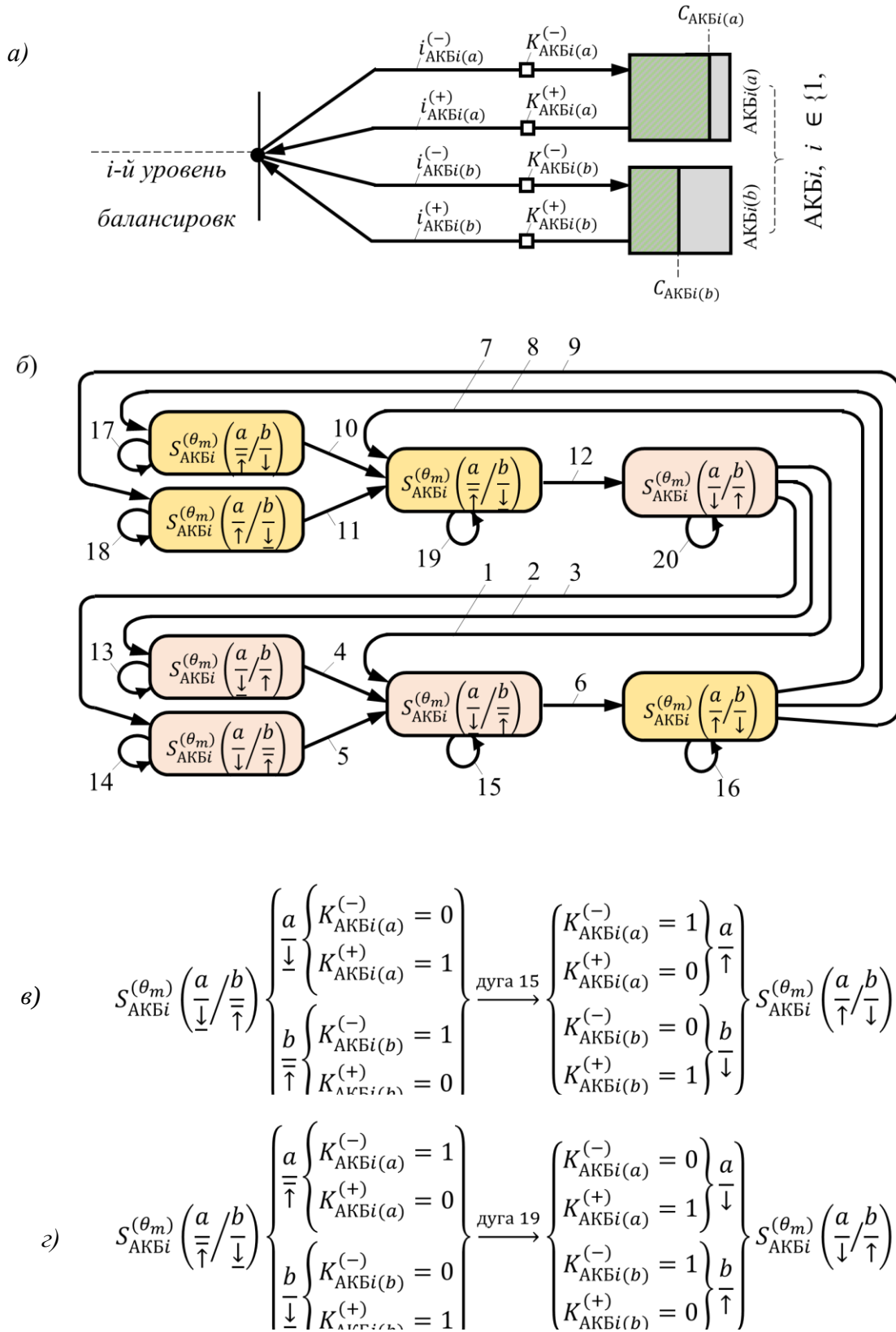


Рисунок 3 – Граф переходов, соответствующий варианту 1

Вариант 1. Граф структуры системы управления параллельными контурами (АКБі(а), АКБі(б)), поочередно работающими в режиме зарядки/разрядки, показан на рисунке 3, а, где нумерация контуров принята как $a = 1$, $b = 2$; ветвям с токами зарядки $i_{AKBi(a)}^{(-)}(\theta_m)$, $i_{AKBi(b)}^{(-)}(\theta_m)$ соответствуют устройства зарядки соответственно $УЗ_{AKBi(a)}^{(-)}$, $УЗ_{AKBi(b)}^{(-)}$, а ветвям с

токами разрядки $i_{AKBi(a)}^{(-)}(\theta_m)$, $i_{AKBi(b)}^{(-)}(\theta_m)$ соответствуют устройства разрядки соответственно $УР_{AKBi(a)}^{(-)}$, $УР_{AKBi(b)}^{(-)}$ (в данном варианте требуется четыре устройства для организации поочередной работы параллельных контуров в режиме зарядки/разрядки).

Состояние вектора условных управляемых ключей ($K_{AKBi(a)}^{(-)}(\theta_m)$, $K_{AKBi(b)}^{(-)}(\theta_m)$, $K_{AKBi(b)}^{(-)}(\theta_m)$, $K_{AKBi(a)}^{(-)}(\theta_m)$) несет информацию о текущем режиме работы параллельных контуров (AKBi(a), AKBi(b)). Эти ключи предназначены для переключения этих контуров из одного режима в другой путем изменения соответствующим образом их состояния.

На рисунке 3, б показан граф переходов из одной ситуации в другую, где:

- вершинам соответствуют ситуации из вышеопределенного набора (см. определения 1 - 3), а дуги 1-12 отражают переходы из одной ситуации в другую;

- если текущему состоянию параллельных контуров (AKBi(a), AKBi(b)) соответствует режим $(\bar{\uparrow}/\underline{\downarrow})$, то ситуация $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$ является началом полного цикла, ситуация $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$

- концом первого полуцикла, ситуация $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$ – началом второго полуцикла, а ситуация $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$ – концом полного цикла поочередной работы этих контуров в режиме зарядка/разрядка;

- дуге 20 соответствует процесс разрядки/зарядки соответственно дефицитного/избыточного тока в узле i -го уровня балансировки, в результате чего в зависимости от закона изменения вектора возмущения $\eta(\theta_m)$ (6) ситуация $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$ может перейти непредсказуемым образом в одну из следующих ситуаций: $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$, $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$, $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$;

- дугам 13, 14 соответствуют процессы соответственно дозарядки контура b , дозарядки контура a с целью перевода ситуации $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$, $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$ в ситуацию $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$;

- дуге 15 соответствует процесс переключения из режима $(\underline{\downarrow}/\bar{\uparrow})$ в режим $(\bar{\uparrow}/\underline{\downarrow})$ с целью перевода ситуации $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$ в ситуацию $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$ (правило переключения показано на рисунке 3, в);

- дуге 16 соответствует процесс зарядки/разрядки соответственно избыточного/дефицитного тока в узле i -го уровня балансировки, в результате чего в зависимости от закона изменения вектора возмущения $\eta(\theta_m)$ (6) ситуация $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$ может перейти непредсказуемым образом в одну из следующих ситуаций: $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$, $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$, $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$;

- дугам 17, 18 соответствуют процессы соответственно доразрядки контура b , доразрядки контура a с целью перевода ситуации $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$, $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$ в ситуацию $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$;

- дуге 19 соответствует процесс переключения из режима $(\bar{\uparrow}/\underline{\downarrow})$ в режим $(\underline{\downarrow}/\bar{\uparrow})$ с целью перевода ситуации $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\bar{\uparrow}/\underline{\downarrow}})$ в ситуацию $S_{AKBi}^{(\theta_m)}(\frac{\alpha/b}{\underline{\downarrow}/\bar{\uparrow}})$ (правило переключения показано на рисунке 3, з);

- правила переключения режимов функционирования параллельных контуров (AKBi(a), AKBi(b)), показанных на рисунке 3, в, з (вариант 1), интерпретируются следующим образом: если параллельные контуры в процессе их функционирования оказались в симметрично-

предельной ситуации $S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\downarrow}} / \frac{b}{\underline{\uparrow}} \right)$ при режиме $(\downarrow/\uparrow)$ или $S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\uparrow}} / \frac{b}{\underline{\downarrow}} \right)$ при режиме $(\uparrow/\downarrow)$, то путем задания состояния вектора ключей $(K_{\text{АКБ}i(a)}^{(-)}(\theta_m), K_{\text{АКБ}i(a)}^{(-)}(\theta_m), K_{\text{АКБ}i(b)}^{(-)}(\theta_m), K_{\text{АКБ}i(b)}^{(-)}(\theta_m))$ следует перевести их в нормальную ситуацию, соответственно, $S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\uparrow}} / \frac{b}{\underline{\downarrow}} \right)$ или $S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\downarrow}} / \frac{b}{\underline{\uparrow}} \right)$, по следующему правилу:

$$(K_{\text{АКБ}i(a)}^{(-)}(\theta_m), K_{\text{АКБ}i(a)}^{(-)}(\theta_m), K_{\text{АКБ}i(b)}^{(-)}(\theta_m), K_{\text{АКБ}i(b)}^{(-)}(\theta_m)) =$$

$$= \begin{cases} (1, 0, 0, 1), \text{если параллельные контуры оказались в ситуации } S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\downarrow}} / \frac{b}{\underline{\uparrow}} \right), \\ \quad \text{т. е. выполнено условие (38), и необходимо перевести} \\ \quad \text{в ситуацию } S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\uparrow}} / \frac{b}{\underline{\downarrow}} \right); \\ (0, 1, 1, 0), \text{если параллельные контуры оказались в ситуации } S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\uparrow}} / \frac{b}{\underline{\downarrow}} \right), \\ \quad \text{т. е. выполнено условие (37), и необходимо перевести} \\ \quad \text{в ситуацию } S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\underline{\downarrow}} / \frac{b}{\underline{\uparrow}} \right), \end{cases} \quad (43)$$

при этом $a = 1, b = 2$.

Вариант 2. Граф структуры системы управления параллельными контурами (АКБ i (1), АКБ i (2)), поочередно работающими в режиме зарядки/разрядки, показан на рисунке 4, а, где ветвям с токами $i_{\text{АКБ}i}^{(-)}(\theta_m), i_{\text{АКБ}i}^{(-)}(\theta_m)$ соответствуют устройства, соответственно, зарядки $УЗ_{\text{АКБ}i}^{(-)}$, разрядки $УР_{\text{АКБ}i}^{(-)}$, реализующие эти токи; $УЗ_{\text{АКБ}i}^{(-)}$ выполняет функции двух устройств $УЗ_{\text{АКБ}i(a)}^{(-)}, УЗ_{\text{АКБ}i(b)}^{(-)}$ из варианта 1, производя поочередно зарядку параллельных контуров, а $УР_{\text{АКБ}i}^{(-)}$ выполняет функции устройств $УР_{\text{АКБ}i(a)}^{(-)}, УР_{\text{АКБ}i(b)}^{(-)}$ из варианта 1, производя поочередно разрядку параллельных контуров накопителя АКБ i i -го уровня путем формирования текущей структуры за счет выбора соответствующего состояния вектора условных управляемых ключей $(K_{\text{АКБ}i(1)}^{(-)}(\theta_m), K_{\text{АКБ}i(1)}^{(-)}(\theta_m), K_{\text{АКБ}i(2)}^{(-)}(\theta_m), K_{\text{АКБ}i(2)}^{(-)}(\theta_m))$. Такая структура использована в рамках структуры управляемой системы НРПМ (см. рис. 1 и 2)

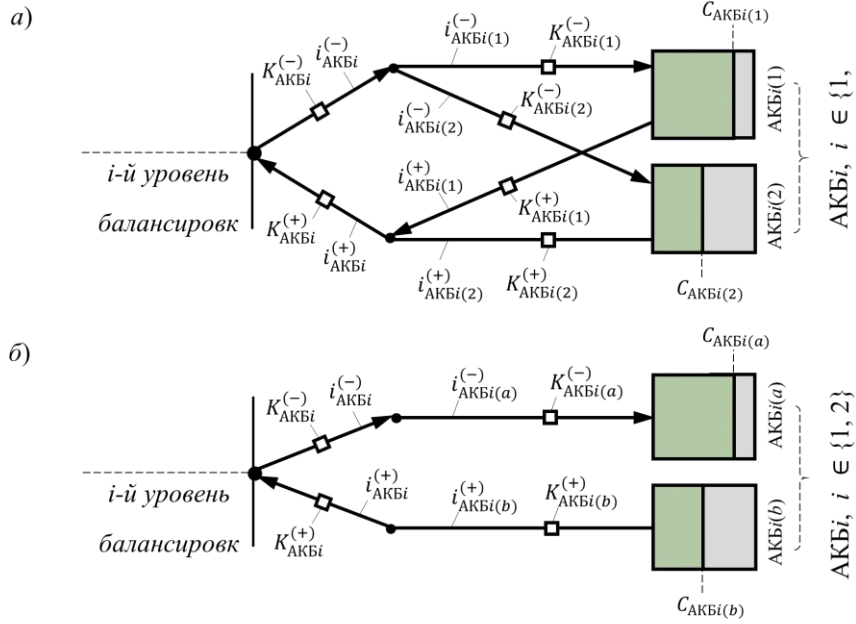
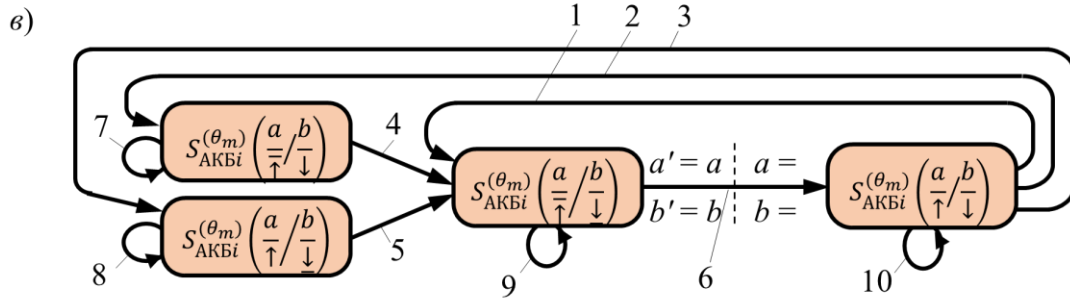


Рисунок 4 – Граф переходов, соответствующий варианту 2 (а, б)



г)

$$S_{AKBi}^{(\theta_m)}\left(\begin{matrix} a \\ \uparrow \\ b \end{matrix} / \begin{matrix} \downarrow \\ b \end{matrix}\right) \left\{ \begin{matrix} a \\ \uparrow \end{matrix} \left\{ \begin{matrix} K_{AKBi(a)}^{(-)} = 1 \\ K_{AKBi(a)}^{(+)} = 0 \end{matrix} \right. \right. \xrightarrow[\text{дуга б}]{\begin{matrix} a' = a \\ b' = b \end{matrix}} \left\{ \begin{matrix} K_{AKBi(a)}^{(-)} = 1 \\ K_{AKBi(a)}^{(+)} = 0 \end{matrix} \right\} \begin{matrix} a \\ \uparrow \end{matrix} \right\} S_{AKBi}^{(\theta_m)}\left(\begin{matrix} a \\ \uparrow \\ b \end{matrix} / \begin{matrix} \downarrow \\ b \end{matrix}\right)$$

Рисунок 4 – Граф переходов, соответствующий варианту 2 (в, г)

Для идентификации текущих режимов функционирования параллельных контуров введем новое понятие, как указатель, формальное определение которого дано ниже.

Определение 4 – пара $(a, b) \in \{(1, 2), (2, 1)\}$ называется вектором указателей, идентифицирующий текущий режим функционирования параллельных контуров (АКБ $i(1)$, АКБ $i(2)$) накопителя АКБ i , если состояние элемента a данного вектора указывает на номер контура, работающего в текущий момент времени в режиме зарядки, а состояние элемента b указывает на номер контура, работающего в режиме разрядки.

Введенный вектор указателей (a, b) позволяет упростить структуру исходного графа (рис. 4, а) и представить в виде структуры, показанной на рис. 4, б. На рисунке 4, в показан граф переходов из одной ситуации в другую, соответствующий вновь полученной структуре (рис. 4, б). Вершины и дуги данного графа интерпретируются, как и в первом варианте (см. рис. 3, б), и отражает этот граф полуцикл процесса зарядки/разрядки параллельных контуров

(АКБ₁(1), АКБ₁(2)), т.е. полную зарядку контура, на номер которого указывает текущее состояние указателя a , и полную разрядку контура, на номер которого указывает текущее состояние указателя b . Смена режимов зарядки/разрядки параллельных контуров производится при этом за счет переключения состояния вектора указателей $(a, b) \in \{(1, 2), (2, 1)\}$ (см. рис. 4, z).

Правила переключения режимов функционирования параллельных контуров (АКБ₁(a), АКБ₁(b)), показанных на рисунке 4, z (вариант 2), интерпретируются следующим образом: если параллельные контуры, при их функционировании в текущем полупериоде процесса зарядки/разрядки, оказались в симметрично-предельной ситуации $S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\uparrow} / \frac{b}{\downarrow} \right)$, то для переключения в очередной полупериод режима зарядки/разрядки следует перевести их в нормальную ситуацию $S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\uparrow} / \frac{b}{\downarrow} \right)$ по следующему правилу:

$$(a, b) = \begin{cases} (2, 1), \text{ если при текущем значении вектора указателей } (a, b) = (1, 2) \\ \quad \text{параллельные контуры оказались в ситуации } S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\uparrow} / \frac{b}{\downarrow} \right), \\ \quad \text{т. е. выполнено условие (37), и необходимо перевести в ситуацию} \\ \quad S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\uparrow} / \frac{b}{\downarrow} \right) \text{ при } (a, b) = (2, 1); \\ (1, 2), \text{ если при текущем значении вектора указателей } (a, b) = (2, 1) \\ \quad \text{параллельные контуры оказались в ситуации } S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\uparrow} / \frac{b}{\downarrow} \right), \\ \quad \text{т. е. выполнено условие (37), и необходимо перевести в ситуацию} \\ \quad S_{\text{АКБ}i}^{(\theta_m)} \left(\frac{a}{\uparrow} / \frac{b}{\downarrow} \right) \text{ при } (a, b) = (2, 1); \end{cases} \quad (44)$$

- переключение состояния вектора ключей:

$$(K_{\text{АКБ}i(1)}^{(-)}(\theta_m), K_{\text{АКБ}i(1)}^{(-)}(\theta_m), K_{\text{АКБ}i(2)}^{(-)}(\theta_m), K_{\text{АКБ}i(2)}^{(-)}(\theta_m)) = \\ = \begin{cases} (1, 0, 0, 1), \text{ если } (a, b) = (1, 2); \\ (0, 1, 1, 0), \text{ если } (a, b) = (2, 1). \end{cases} \quad (45)$$

Этап 6 – декомпозиция исходной задачи синтеза алгоритма оптимального ситуационного управления энергетическим балансом в управляемой системе НРПМ. Исходную задачу синтеза (задача 1 в разделе 2) с учетом приоритетности включения элементов системы НРПМ к процессу управления энергетическим балансом в ней (4), и сведений, приведенных в рамках данного раздела, можно разбить на ряд последовательно решаемых подзадач.

Примечание 1. Ниже рассматривается частный случай исходной задачи синтеза (задача 1), т.е. рассматривается одношаговая задача оптимизации, которой соответствует алгоритм управления со структурой (13).

Задача 1.1 – задача поддержания текущей величины напряжения конденсатора $u_{\text{ШСР}}(\theta_m)$ в окрестности номинального напряжения $u_{\text{ШСР}}^{\text{ном}}$. Данная задача формулируется следующим образом: требуется найти такой алгоритм $G_{\text{ШСР}, \theta_m}$, вырабатывающий в каждый текущий момент времени θ_m , на основе текущей информации $u_{\text{ШСР}}(\theta_m)$, $i_{\Gamma}(\theta_m)$, $i_{\Pi}(\theta_m)$ (см. (5), (6)), управляющее воздействие в виде балансирующего тока 1-го уровня $i_{\text{бэл}}^{(1)}(\theta_m)$ (см. рис. 2):

$$i_{\text{бэл}}^{(1)}(\theta_m) = G_{\text{ШСР}, \theta_m} [u_{\text{ШСР}}(\theta_m), i_{\Gamma}(\theta_m), i_{\Pi}(\theta_m), u_{\text{ШСР}}^{\text{ном}}], \quad (46)$$

минимизирующий отклонение $u_{\text{ШСР}}(\theta_m)$ от $u_{\text{ШСР}}^{\text{ном}}$ с учетом (27), т.е. в каждый текущий момент времени θ_m решается следующая задача оптимизации:

$$\min_{i_{\text{ЗЛ}}^{(1)}(\theta_m)} J_{\text{ШСР}, \theta_m}^{(1)} = (u_{\text{ШСР}}(\theta_{m-1}) - u_{\text{ШСР}}^{\text{ном}})^2 \text{ с учетом (27)}. \quad (47)$$

$$= G_{\text{ШСР}, \theta_m} [u_{\text{ШСР}}(\theta_m), i_{\Gamma}(\theta_m), i_{\Pi}(\theta_m), u_{\text{ШСР}}^{\text{ном}}]$$

Примечание 2. Подзадача (47) является классической задачей теории оптимального управления, для решения которой можно использовать метод динамического программирования, основанный на принципе оптимальности Р. Беллмана [11,12].

Задача 1.2 – задача поддержания текущей величины балансирующего тока 2-го уровня $i_{\text{ЗЛ}}^{(2)}(\theta_m)$ в окрестности номинального $i_{\Gamma\text{С}}^{\text{ном}}(\theta_m)$. Данная задача формулируется следующим образом: требуется найти такой алгоритм $G_{\text{АКБ1}, \theta_m}$, вырабатывающий в каждый текущий момент времени θ_m , на основе текущей информации $C_{\text{АКБ1}(1)}(\theta_m)$, $C_{\text{АКБ1}(2)}(\theta_m)$ (см. (5)) и балансирующего тока 1-го уровня $i_{\text{ЗЛ}}^{(1)}(\theta_m)$, являющегося результатом решения задачи 1.1, определенные компоненты вектора управления $i_{\text{упр}}(\theta_m)$ (9), а именно:

$$i_{\text{АКБ1}}(\theta_m) = (i_{\text{АКБ1}(1)}^{(-)}(\theta_m), i_{\text{АКБ1}(1)}^{(-)}(\theta_m), i_{\text{АКБ1}(2)}^{(-)}(\theta_m), i_{\text{АКБ1}(2)}^{(-)}(\theta_m)) =$$

$$= G_{\text{АКБ1}, \theta_m} [C_{\text{АКБ1}(1)}(\theta_m), C_{\text{АКБ1}(2)}(\theta_m), i_{\text{ЗЛ}}^{(1)}(\theta_m), i_{\Gamma\text{С}}^{\text{ном}}(\theta_m)], \quad (48)$$

минимизирующие отклонение балансирующего тока 2-го уровня $i_{\text{ЗЛ}}^{(2)}(\theta_m)$ от $i_{\Gamma\text{С}}^{\text{ном}}(\theta_m)$ с учетом (23), (28)-(33) и с учетом набора ситуаций и правил переходов из одной ситуации в другую (34)-(45) при $i = 1, j \in \{1, 2\}$, т.е. в каждый текущий момент времени θ_m решается следующая задача оптимизации:

$$\min_{i_{\text{ЗЛ}}^{(2)}(\theta_m)} J_{\text{ЗЛ}, \theta_m}^{(2)} = (i_{\text{ЗЛ}}^{(2)}(\theta_m) - i_{\Gamma\text{С}}^{\text{ном}}(\theta_m))^2 \text{ с учетом (23),}$$

$$= G_{\text{АКБ1}, \theta_m} [C_{\text{АКБ1}(1)}(\theta_m), C_{\text{АКБ1}(2)}(\theta_m), i_{\text{ЗЛ}}^{(1)}(\theta_m), i_{\Gamma\text{С}}^{\text{ном}}(\theta_m)] \quad (28) - (33), \text{ и с учетом набора ситуаций и правил}$$

$$\text{переходов из одной ситуации в другую (34) - (45)}$$

$$\text{при } i = 1, j \in \{1, 2\} \}. \quad (49)$$

Задача 1.3 – задача поддержания текущей величины балансирующего тока 3-го уровня $i_{\text{ЗЛ}}^{(3)}(\theta_m)$ в окрестности номинального $i_{\Gamma\text{С}}^{\text{ном}}(\theta_m)$. Данная задача формулируется следующим образом: требуется найти такой алгоритм $G_{\text{АКБ2}, \theta_m}$, вырабатывающий в каждый текущий момент времени θ_m , на основе текущей информации $C_{\text{АКБ2}(1)}(\theta_m)$, $C_{\text{АКБ2}(2)}(\theta_m)$ (см. (5)) и балансирующего тока 2-го уровня $i_{\text{ЗЛ}}^{(2)}(\theta_m)$, являющегося результатом решения задачи 1.2, определенные компоненты вектора управления $i_{\text{упр}}(\theta_m)$ (9), а именно:

$$i_{\text{АКБ2}}(\theta_m) = (i_{\text{АКБ2}(1)}^{(-)}(\theta_m), i_{\text{АКБ2}(1)}^{(-)}(\theta_m), i_{\text{АКБ2}(2)}^{(-)}(\theta_m), i_{\text{АКБ2}(2)}^{(-)}(\theta_m)) =$$

$$= G_{\text{АКБ2}, \theta_m} [C_{\text{АКБ2}(1)}(\theta_m), C_{\text{АКБ2}(2)}(\theta_m), i_{\text{ЗЛ}}^{(2)}(\theta_m), i_{\Gamma\text{С}}^{\text{ном}}(\theta_m)], \quad (50)$$

минимизирующие отклонения балансирующего тока 3-го уровня $i_{\text{ЗЛ}}^{(3)}(\theta_m)$ от $i_{\Gamma\text{С}}^{\text{ном}}(\theta_m)$ с учетом (24), (28)-(33) и с учетом набора ситуаций и правил переходов из одной ситуации в другую (34)-(45) при $i = 2, j \in \{1, 2\}$, т.е. в каждый текущий момент времени θ_m решается следующая задача оптимизации:

$$\min_{\substack{i_{\text{АКБ2}}(\theta_m) = \\ = G_{\text{АКБ2}, \theta_m} [C_{\text{АКБ2}(1)}(\theta_m), C_{\text{АКБ2}(2)}(\theta_m), \\ i_{\text{зап}}^{(2)}(\theta_m), i_{\text{ГС}}^{\text{ном}}(\theta_m)]}} \left\{ J_{\text{оэл}, \theta_m}^{(3)} = (i_{\text{оэл}}^{(3)}(\theta_m) - i_{\text{ГС}}^{\text{ном}}(\theta_m))^2 \right\} \text{ с учетом (24),} \\ (28) - (33), \text{ и с учетом набора ситуаций и правил} \\ \text{переходов из одной ситуации в другую (34) - (45)} \\ \text{при } i = 2, j \in \{1, 2\} \}. \quad (51)$$

Задача 1.4 – задача поддержания текущей величины перетока $i_{\text{ГС}}^{(-,-)}(\theta_m)$ в окрестности номинального $i_{\text{ГС}}^{\text{ном}}(\theta_m)$. Данная задача формулируется следующим образом: требуется найти такой алгоритм $G_{\text{ГС}, \theta_m}$, вырабатывающий в каждый текущий момент времени θ_m , на основе балансирующего тока 3-го уровня $i_{\text{оэл}}^{(3)}(\theta_m)$, являющегося результатом решения задачи 1.3, определенные компоненты вектора управления $i_{\text{уп}}(\theta_m)$ (9), а именно:

$$i_{\text{БИ}, \text{БН}}(\theta_m) = (i_{\text{БИ}}^{(-)}(\theta_m), i_{\text{БН}}^{(-)}(\theta_m)) = G_{\text{БИ}, \text{БН}, \theta_m} [i_{\text{оэл}}^{(3)}(\theta_m), i_{\text{ГС}}^{\text{ном}}(\theta_m)], \quad (52)$$

минимизирующие отклонение перетока $i_{\text{ГС}}^{(-,-)}(\theta_m)$ от номинального $i_{\text{ГС}}^{\text{ном}}(\theta_m)$ за счет минимальной частоты переключения устройств БН, БИ с учетом допуска (20), т.е. в каждый текущий момент времени θ_m решается следующая задача оптимизации:

$$\min_{\substack{i_{\text{БИ}, \text{БН}}(\theta_m) = \\ = G_{\text{БИ}, \text{БН}, \theta_m} [i_{\text{оэл}}^{(3)}(\theta_m), i_{\text{ГС}}^{\text{ном}}(\theta_m)]}} \left\{ J_{\text{ГС}, \theta_m} = (i_{\text{ГС}}^{(-,-)}(\theta_m) - i_{\text{ГС}}^{\text{ном}}(\theta_m))^2 \right\} \text{ с учетом (20)}. \quad (53)$$

Таким образом, алгоритм оптимального ситуационного управления $G_{\text{АОСУ}, \theta_m}$ энергетическим балансом в управляемой системе НРПМ, получается в результате последовательного решения подзадач 1.1 - 1.4, т.е. (47), (49), (51), (53), укрупненная функциональная схема которого показана на рисунке 5.

Примечание 3. Для решения подзадач (49), (51), (53) используется аппарат вычислительных сетей Петри [13-15], в результате чего получаются самоорганизующиеся алгоритмы оптимального ситуационного управления $G_{\text{АОСУ}, \theta_m}$.

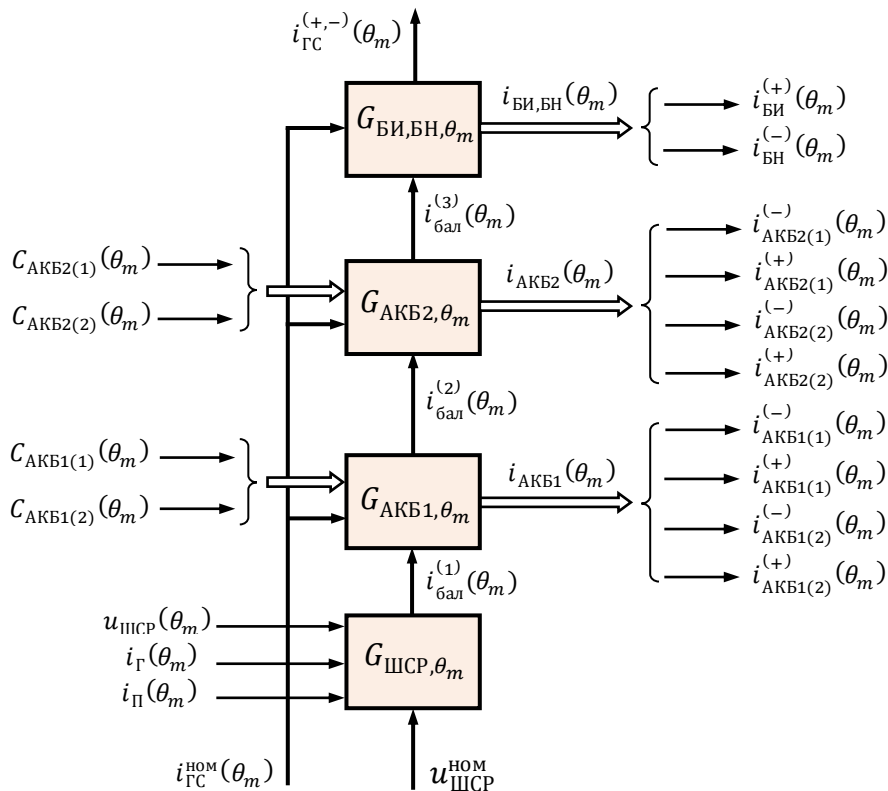


Рисунок 5 – Укрупненная функциональная схема алгоритма оптимального ситуационного управления $G_{\text{АДС}}, \theta_{\text{н}}$ энергетическим балансом в управляемой системе НРПМ

Заключение

В настоящей работе принята структура системы накопления и распределения потоков мощностей НРПМ позволяет обеспечить простоту изменения ее конфигурации путем добавления/исключения в ее состав тех или иных компонентов (балластные источники БИ, балластные нагрузки БН, генерирующие установки с ВИЭ и нагрузки разного типа), а также добавление/исключение возможности взаимодействия НРПМ с глобальной сетью ГС.

Для принятой структуры построена математическая модель с учетом ситуаций, возникающих в процессе циркуляции потоков в системе НРПМ, сформулирована задача синтеза алгоритма оптимального ситуационного управления АОСУ энергетическим балансом в ней и предложена схема ее решения, которая позволяет получить многоуровневый алгоритм $G_{\text{АОСУ}, \theta_m}$, $m = 0, 1, \dots, M - 1$, состоящий из последовательно функционирующих алгоритмов, т.е. $G_{\text{АОСУ}, \theta_m} :$

$G_{\text{ШСР}, \theta_m} \xrightarrow{i_{\text{ЗЛ}}^{(1)}(\theta_m)} G_{\text{АКБ1}, \theta_m} \xrightarrow{i_{\text{ЗЛ}}^{(2)}(\theta_m)} G_{\text{АКБ2}, \theta_m} \xrightarrow{i_{\text{ЗЛ}}^{(3)}(\theta_m)} G_{\text{БИ, БН}, \theta_m} \xrightarrow{i_{\text{ГС}}^{(4,-)}(\theta_m)}$, выполняющих следующие функции: $G_{\text{ШСР}, \theta_m}$ – поддержание текущей величины напряжения конденсатора $u_{\text{ШСР}}(\theta_m)$ (узла – шины сборки и распределения ШСР) путем выдачи оптимального управляющего воздействия в виде балансирующего тока $i_{\text{ЗЛ}}^{(1)}(\theta_m)$; $G_{\text{АКБ1}, \theta_m}$, $G_{\text{АКБ2}, \theta_m}$, $G_{\text{БИ, БН}, \theta_m}$ – оптимальные ситуационные алгоритмы для последовательной реализации балансирующего тока $i_{\text{ЗЛ}}^{(1)}(\theta_m)$ с использованием элементов системы НРПМ соответственно (АКБ1(1), АКБ1(2)), (АКБ2(1), АКБ2(2)), (БИ, БН) с целью поддержания перетока $i_{\text{ГС}}^{(-,-)}(\theta_m)$ между ГС и НРПМ в окрестности номинального $i_{\text{ГС}}^{\text{ном}}(\theta_m)$.

Алгоритм $G_{\text{АОСУ}, \theta_{\text{пл}}}$ обладает тем, что при подборе и изменении конфигурации системы НРПМ на этапе проектирования систем АРГЭК для различных регионов с

соответствующими им ВИЭ, его структура легко модифицируется, что важно при создании системы автоматизированного проектирования автоматизированных распределенных гибридных энергокомплексов АРГЭК.

Литература:

1. M.Asanov, S.Asanova, M.Safaraliev, I. Zicmane, S. Beryozkina, S. Suerkulov. Design methodology of intelligent autonomous distributed hybrid power complexes with renewable energy sources. International Journal of Hydrogen Energy. Volume 48, Issue 81, 22 September 2023. Pages 31468-31478.
2. Лукутин Б.В. Способы снижения расхода топлива дизельных электростанций / Лукутин Б.В., Шандарова Е.Б. // Современные проблемы науки и образования. – 2013. – №2. – С. 139.
3. Обухов С.Г. Двухконтурный накопитель энергии для гибридных энергетических систем с возобновляемыми источниками энергии / Обухов С.Г., Плотников И.А., Ибрагим А., Маслов В.Г. // Известия Томского университета. Инжиниринг георесурсов. –2020. – Т. 331. № 1. – С. 64–76.
4. Лукутин Б.В. Способы снижения расхода топлива дизельных электростанций / Лукутин Б.В., Шандарова Е.Б. // Электричество. – 2012. – №6. – С. 24–29.
5. Asanova S.M. Optimization of the structure of autonomous distributed hybrid power complexes and energy balance management in them / Asanova S.M., Kokin S.E., Dmitriev S.A., Safaraliev M., Arfan Kh., Zhabudaev T., Satarkulov T.K. // International Journal of Hydrogen Energy. – 2021. - Volume 46, Issue 70. – P. 34542-34549.
6. Asanova S.M., Ahyoev J.S, Askarbek N., Suerkulov S.M., Asanova D.U. Safaraliev M. Method for designing drop-of-wire recognition systems on sections of undistorted two-wire power transmission lines. IOP Conference Series: Materials Science and Engineering. 15. Sep. "15th International Conference on Industrial Manufacturing and Metallurgy" 2020. C. 012114.
7. Сатаркулов К.А., Асанова С.М. и др. Токопроводящая жила проводов и кабелей. – Патент KG № 1187. 2009 г.
8. Asanov M., Kokin S., Asanova S.M., Satarkulov K., Dmitriev S., Safaraliev M. The use of Petri computing networks for optimization of the structure of distribution networks to minimize power losses. Energy Reports. Vol. 6, Supplement 9, December 2020, 1337-1343
9. Asanova S., M.Safaraliev, I. Zicmane, S. Suerkulov, S. Kokin. Improving the reliability of the energy balance management process in hybrid power complexes with green hydrogen and energy storage. International Journal of Hydrogen Energy. 2024. T. 61. C. 1485-1494.
10. Asanov M., Asanova S., Semenenko S., Matrenin P., Safaraliev M., Rusina A. Optimal amount of information determination for power system steady state estimation. Energy Reports, Volume 8, Supplement 1, April 2022, Pages 1085-1092
11. Куо Б. Теория и проектирование цифровых систем управления/ Пер. с англ. – М.: Машиностроение, 1986. – 448 с.
12. Медич Дж. Статистически оптимальные линейные оценки и управление. / Пер. с англ.// Под ред. А.С. Шаталова. – М.: «Энергия», 1973. – С. 440.
13. М.С. Асанов, С.М. Асанова, К.А. Сатаркулов. Структурная модель вычислительных сетей Петри. Известия КГТУ. – Бишкек, 2008. – №13. – С. 78–85.
14. М.С. Асанов, С.М. Асанова, К.А. Сатаркулов. Вычислительные компоненты, язык описания и правила функционирования вычислительных сетей Петри. Известия КГТУ. – Бишкек, 2008. – №13. – С. 85–95.

15. Асанова С.М. Развитие сетей Петри для разработки самоорганизующихся многокомпонентных вычислительных алгоритмов решения задач электроэнергетики / Проблемы автоматизации и управления, НАН КР, июль 2022, № 2 (44). –С. 15–21.
16. Сафаралиев М.Х., Матренин П.В., Дмитриев С.А., Асанова С.М., Ахъев Дж.С. Разработка моделей среднесрочного прогнозирования электропотребления в изолированно работающих энергосистемах на основе ансамблевых методов машинного обучения / Известия НТЦ ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ. – 2021. – №1 (84)). –С.32–39.

К.М. Жумалиев, jkm56@mail.ru

НАН КР

Г.К. Алибаева, agkguli@gmail.com

КГТУ им. И. Раззакова

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ГЕОИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ

В работе рассмотрены инструменты анализа и визуализации пространственных данных геоинформационного моделирования, что делает его актуальным для решения задач по экосистеме, прогнозирования климатических изменений, оценки распределения ресурсов. Рассмотрены виды и методы геоинформационного моделирования, а также сделан сравнительный анализ современных программных платформ. Проанализированы современные программные платформы для решения задач в исследованиях температуры воды на поверхности внутренних водоемов, а также температуры поверхности и нормализованного разностного водного индекса (NDWI).

Ключевые слова: моделирование, геоинформационное моделирование, виды геоинформационного моделирования, средства ГИМ.

Введение

В настоящее время геоинформационное моделирование (ГИМ) применяется в исследованиях различных областей в нашей жизни для анализа и визуализации пространственных данных. Оно применяется для мониторинга состояния экосистем, анализа качества воздуха и воды, определения состояния источников ресурсов и прогнозирования последствий изменения климата. Помогает выявлять экологические риски и планировать природоохранные мероприятия. Также дает возможность оптимизировать использование земель, прогнозировать урожайность, учитывать плодородие почв, а также выявлять зональные риски (например, прогрессивные засухи или эрозии).

Геоинформационное моделирование решает такие прикладные задачи, как получение цифровых моделей и расчеты пространственных объектов [3]. Основной задачей такого моделирования являются следующие виды операций, как картометрические операции, проекционные преобразования, операции с пересечениями объектов (оверлейные операции), построение буферных зон, операции с объектами различных геометрических типов [2].

Виды геоинформационного моделирования

Геоинформационным моделированием называют технологию обработки пространственных данных в рамках геоинформационных систем (ГИС), связанную с преобразованиями графической и сопряженной с ней табличной информации [6]. ГИМ включает в себя различные подходы и методы, которые позволяют отображать, проецировать и расшифровать пространственные данные. Рассмотрим основные виды геоинформационного моделирования:

- моделирование с использованием цифровых моделей дает возможность создавать виртуальные аналоги реальных объектов или процессов, чтобы тестировать, анализировать и оптимизировать их характеристики и поведение. Для оценки эффективности, выявления потенциальных проблем и прогнозирования результатов в различных областях часто применяются такие модели;
- пространственное моделирование дает возможность создания моделей, которые представляют собой географические объекты и их атрибуты. Следует отметить, что основные методы включают векторное моделирование и растровое моделирование;
- картографическое моделирование предоставляет возможность процесса создания и анализа пространственных карт, который используется для представления, моделирования и

анализа географической информации. Где важна работа с пространственными данными в географии, экологии, урбанистике, логистике и др. областях, оно широко применяется;

- экологическое моделирование позволяет создавать математические или компьютерные модели для исследования и анализа природных экосистем, их компонентов и процессов. Оно позволяет прогнозировать поведение экосистем, оценивать воздействие человеческой деятельности на природу и помогает в разработке стратегий для сохранения и устойчивого использования природных ресурсов. Эти модели применяются в экологии, биологии, климатологии, агрономии и других науках о Земле;

- моделирование с использованием ГИС (ГИС-моделирование) предоставляет возможность использования геоинформационных систем в процессе построения моделей с пространственными данными, связанными с местоположением объектов. ГИС-моделирование применяется в различных областях: экологии, градостроительстве, логистике, сельском хозяйстве и других сферах;

- моделирование геоданных и визуальное моделирование предполагает создание структурированных представлений пространственной информации, где данные могут относиться к объектам местности, геологическим структурам, инфраструктуре и природным ресурсам. А визуальное моделирование создает графические представления данных, часто в формате 2D и 3D-визуализации, пространственной структуры и взаимосвязей. Оно позволяет более наглядно оценивать различные сценарии, взаимодействия и эффекты изменений;

- 3D-моделирование позволяет визуализировать и анализировать географические данные в трехмерном пространстве. Это может включать геометрические модели местности [4,10].

Общим для этих видов используют широкий набор данных (место, время, тема), который в других технологиях не используют.

Средства геоинформационного моделирования

Геоинформационное моделирование создает новые информационные модели и информационные ресурсы [1]. Чтобы получить новые информационные материалы, используются разные средства геоинформационного моделирования. Для создания карт, проведения анализа или разработки продуктов визуализации данных важно ознакомиться с различными программными платформами.

Рассмотрим основные программные платформы для геоинформационного моделирования.

ArcGIS (ArcGIS Online) — самая масштабируемая система программ для создания, формирования, регулирования, исследования и распространения географической информации. Данная система используется специалистами во всем мире [6]. Платформа ArcGIS позволяет выполнять следующие задачи: создавать, обмениваться и использовать интеллектуальные карты, создавать и управлять базами географических данных, решает задачи при помощи пространственного анализа и создания приложения на основе карт [7].

Следующая программная платформа QGIS – это открытое программное обеспечение для работы с ГИС. Платформа охватывает широкий спектр потребностей картографирования и пространственного анализа. QGIS предлагает полный набор инструментов, отвечающих потребностям различных областей, включая городское планирование, управление окружающей средой и научные исследования. Его открытый исходный код означает, что пользователи могут свободно загружать и использовать программное обеспечение, применяя широкий спектр плагинов и возможностей настройки. Это делает QGIS особенно ценным для проектов, требующих гибкости и адаптируемости [8]. Помимо вышеуказанных программных продуктов с такими же особенностями, существуют такие программные платформы, как SAGA GIS, TatukGIS, GRASS GIS, и т.д.

Далее рассмотрим программные платформы со специализированным инструментом, такие как Whitebox Software. Это платформа геопространственного анализа, известная своими мощными и универсальными инструментами, предназначенными для

профессионалов в области ГИС и дистанционного зондирования. Платформа предлагает множество инструментов для обработки растровых, векторных и LiDAR-данных, что придает ей особую ценность для специалистов в области геопространственных данных в различных отраслях. Программная платформа высоко ценится за скорость, гибкость и простоту интеграции с другими ГИС-платформами, такими как QGIS и ArcGIS.

Manifold GIS — это мощная геопространственная программная платформа, обеспечивающая высокопроизводительный пространственный анализ, визуализацию данных и возможности картографирования. Эта платформа, разработанная Manifold Software Ltd., известна своей эффективностью, особенно при обработке больших наборов данных. В Manifold GIS надежные и быстрые ГИС-инструменты, которые могут использоваться для современного вычислительного оборудования для обеспечения геопространственной обработки высшего уровня [8].

Рассмотрим далее мощное программное обеспечение MapInfo Professional. Оно предоставляет ряд инструментов и возможностей для визуализации данных, пространственного анализа и создания карт. MapInfo Professional поддерживает широкий спектр форматов данных, включая векторные данные (точки, линии, полигоны) и растровые данные. Также позволяет эффективно импортировать, экспортировать и управлять геопространственными данными. Оно предоставляет инструменты для символизации объектов на основе значений атрибутов, создания тематических карт и применения расширенных картографических методов. Дает возможность выполнять пространственные запросы, анализ наложения, анализ буфера, анализ близости, сетевой анализ и многое другое [9].

Сравнительный анализ некоторых средств геоинформационного моделирования

Технология работы в различных средствах геоинформационного моделирования отличается, чтобы понять преимущества и недостатки геоинформационного моделирования, необходимо провести сравнительный анализ между ними. Представлена таблица сравнения возможностей наиболее популярных средств геоинформационного моделирования.

Таблица 1 – Анализ средств геоинформационного моделирования

	ArcGIS	QGIS	GRASSGIS
Сфера применения	– городское и региональное планирование; – экология и природные ресурсы; – сельское хозяйство; – транспорт и логистика; – геология и горнодобывающая промышленность; – телекоммуникации и энергетика [11]	– городское и региональное планирование; – экология и управление природными ресурсами; – сельское хозяйство; – транспорт и логистика; – туризм и рекреация; – охрана окружающей среды и управление рисками; – гуманитарные проекты и некоммерческий сектор [11]	– экология и охрана окружающей среды; – гидрология и водные ресурсы; – геология и геоморфология; – климатология и метеорология; – археология и историческая география; – мониторинг природных ресурсов и управление заповедниками; – городское планирование и управление земельными ресурсами [14]
Поддержка ОС	– совместим с Windows	– совместим с Windows – Mac OS, Linux	– совместим с Windows – Mac OS, Linux

Гидрологические исследования	– Поддерживает гидрологическую информацию и ЦМР, а также применяются функции гидрологического анализа	– Поддерживает картометрические и морфометрические измерения, для мониторинга в гидрологии	– Поддерживает анализ временных данных, особенно полезно для мониторинга изменений гидрологии и других областях, где данные изменяются во времени
Достоинства	– поддерживает различные типы данных (растр, вектор, 3D); – позволяет работать с точными картографическими данными; – выполняет сложные геопространственные вычисления; – предоставляет мощные инструменты для анализа, визуализации, редактирования и управления пространственными данными; – ПО совместимо с множеством форматов данных и позволяет интегрироваться с другими платформами (например, AutoCAD, Excel и базами данных); – предоставляет пользователям возможность настраивать интерфейс и инструменты под конкретные задачи	– бесплатное и открытое ПО; – поддерживает широкий спектр инструментов для картографирования, анализа данных, работы с векторными и растровыми слоями, а также 3D-визуализации; – поддерживает стандартные ГИС-форматы (например, Shapefile, GeoTIFF, KML); – позволяет импортировать и экспортировать данные в различных форматах; – поддерживает скрипты на Python	– полностью бесплатная платформа с открытым исходным кодом; – включает более 350 встроенных модулей для анализа растровых и векторных данных; – предлагает высокую точность расчетов; – легко интегрируется с другими ГИС-программами; – поддерживает обмен данными с Python и R
Недостатки	– высокая стоимость; – программа требует мощного компьютера для корректной работы, особенно при работе с большими объемами данных или 3D-визуализацией [11-12].	– сложность для начинающих пользователей; – трудности при работе с большими наборами данных или при выполнении сложных пространственных анализов; – не предоставляет официальной технической поддержки; – предоставляет базовые возможности автоматизации, но для создания сложных рабочих процессов может потребоваться больше усилий и знаний в программировании [11-12]	– сложность для новых пользователей; – ограниченные возможности для создания визуально привлекательных карт; – модели могут быть ресурсо-затратными и требуют большого объема памяти и времени на выполнение. – особо не ориентирована на бизнес-аналитику, маркетинг или логистику [14]

Заключение

В ходе изучения можно отметить, что геоинформационное моделирование представляет собой инструмент наблюдения, способный значительно повысить эффективность исследований и управления в различных отраслях, где важна пространственная информация. Современные методы и ресурсы ГИМ, включая использование облачных вычислений и специализированных программных платформ (таких как ArcGIS, QGIS и других), обеспечивают точность.

Геоинформационное моделирование находит широкое применение в решении экологических, градостроительных и агропромышленных задач, а также в управлении климатическими изменениями. Оно позволяет моделировать сложные экологические процессы (например, климатические изменения, изменения водных ресурсов и т.д.), прогнозировать изменения состояния окружающей среды.

Как показывает анализ некоторых современных средств геоинформационного исследования, каждая платформа имеет свои сильные стороны: ArcGIS отличается высоким уровнем и совместимостью с различными форматами. QGIS доступностью и гибкостью обеспечивает широкий выбор инструментов для анализа и управления данными. GRASS GIS эффективностью в обработке больших объемов данных больше ориентирована на научные и исследовательские задачи.

Используя метод обработки аэрокосмических снимков со средствами геоинформационного моделирования QGIS и GRASS GIS, можно получить наиболее достоверные результаты температуры воды на поверхности внутренних водоемов, таких как оз. Иссык-Куль, а также температуру поверхности, нормализованную разностным водным индексом (NDWI), и другие пользовательские выходные данные, выполняя атмосферную и радиометрическую коррекцию.

Таким образом, геоинформационное моделирование остается перспективным направлением, поддерживающим междисциплинарные исследования и предоставляющим инновационные решения для задач развития, что делает его важным фундаментом современной науки и практики.

Литература

1. Markelov V. M. Geoinformation Modeling in Logistics // European Journal of Economic Studies, 2012., Vol.(1). №1. – P. 129–133.
2. Андреева О.А. Геоинформационное моделирование при проектировании линейных объектов // Информационные технологии в науке, образовании и управлении. ИТНОУ. – 2019. №1. – Стр. 30–38.
3. Булгаков С.В., Геоинформационное моделирование и информационное взаимодействие. Конструкторское бюро. 2018.2.
4. Шаннаа А. А., Кулик Е. Н. Современные средства пространственного моделирования территории в ГИС. //DOI: 10.33764/2618-981X-2019-6-2-208-214, 2019. Стр. 208–214.
5. Использование ГИС для мониторинга [Electronic resource]. – Mode of access:<http://kadastrua.ru/lektsii-po-gis/962-ispolzovanie-gis-dlya-monitoringa.html> (Дата обращения: 29.10.2024).
6. Геоинформационные технологии [Electronic resource]. – Mode of access: <http://www.geol.vsu.ru/history/direct.html#Geoinformatics> (дата обращения: 29.10.2024).
7. ArcGis Resources [Electronic resource]. – Mode of access: <https://resources.arcgis.com/ru/help/> (дата обращения: 01.11.2024).
8. Geospatial modeling software and artificial intelligence tools [Electronic resource]. – Mode of access: <https://flypix.ai/hi/blog/geospatial-modeling-software-tools-ai/> (Дата обращения: 01.11.2024).
9. Geographic Information Systems (GIS) Tools [Electronic resource]. – Mode of access: https://www.devopsschool.com/blog/top-30-geographic-information-systems-gis-tools/#4_MapInfo_Professional (Дата обращения: 05.11.2024).
10. Доступ и получение пространственных данных [Electronic resource]. – Mode of access:<http://www.gisa.ru/28018.html> (дата обращения: 05.11.2024).
11. QGIS vs ArcGIS [Electronic resource]. – Mode of access: <https://cartetika.ru/tpost/v9z7ti7jx1-qgis-vs-arcgis> (Дата обращения: 13.11.2024).
12. Сысоев А. В., Елшина Т.Е. Создание и обработка цифровых моделей рельефа в среде ГИС// Науки о Земле и смежные экологические науки. 2017. – Стр.72–77.

13. III Всероссийский конкурс разработок учебных занятий «Современный урок с РЕД ОС» [Electronic resource]. – Mode of access: https://redos.red-soft.ru/base/redos-7_3/7_3-education/7_3-qgis/?nocache=1731600340948 (Дата обращения: 13.11.2024).
14. GISTechnik- Все о ГИС и их применении [Electronic resource]. – Mode of access: <http://gistechnik.ru/programmy-gis/nastolnaya-gis/grass-gis> (Дата обращения: 12.11.2024).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.5

С.В. Корякин, srgkoryakin1@gmail.com

Институт информационных технологий КГТУ им. И.Раззакова

Институт машиноведения автоматизации и геомеханики НАН КР

В.В. Ким, vyacheslav.kim.2003@mail.ru

Институт информационных технологий КГТУ им. И. Раззакова

ОБЗОР МЕТОДОВ РАЗРАБОТКИ ПОДСИСТЕМ ЗАЩИТЫ ОТ ФИШИНГОВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ

Данная работа посвящена анализу методов разработки подсистемы SOC для защиты от фишинговых атак с использованием технологий искусственного интеллекта (ИИ) и машинного обучения (МО). Рассмотрены основные методы обнаружения фишинга, проведен обзор коммерческих систем защиты и их функциональных возможностей. Особое внимание уделено сравнению моделей ИИ для выявления фишинговых атак с оценкой их точности, скорости работы и адаптивности. Также приведены примеры применения ИИ в действующих системах безопасности и рассмотрены возможные сложности внедрения таких решений, включая настройку и риски ложных срабатываний. В заключение даны рекомендации по выбору подходящих технологий и инструментов для разработки подсистемы SOC, позволяющей эффективно выявлять и блокировать фишинговые атаки с применением ИИ.

Ключевые слова: фишинг, ИИ, машинное обучение, SOC, кибербезопасность, нейронные сети, анализ текста, автоматизация, деревья решений, случайные леса, ансамблевые методы, машины опорных векторов (SVM), логистическая регрессия, градиентный бустинг, K-means, BERT

Введение

Одной из наиболее распространенных киберугроз являются фишинговые атаки, нацеленные на компрометацию корпоративных данных. Более 80% кибератак в 2024 году начинались с фишинга. Традиционные методы защиты, такие как черные списки и фильтры ключевых слов, не противостоят новым, сложным угрозам. В этой статье рассматриваются преимущества использования технологий искусственного интеллекта (ИИ) и машинного обучения (МО) в защите от фишинговых атак, сравнение их с традиционными методами и перспективы развития. [1]

В 2024 году наблюдался значительный рост фишинговых атак на онлайн-магазины и финансовые компании. Согласно отчету «Лаборатории Касперского», количество попыток перехода по фишинговым ссылкам увеличилось на 26% по сравнению с предыдущим годом, достигнув 893 216 170 случаев. [1]

Согласно исследованию, среднее количество фишинговых угроз на каждый бренд выросло с 495 до 734. Ежедневно злоумышленники создают около четырех новых фишинговых ресурсов под каждый целевой бренд. Подавляющее большинство этих сайтов (94%) нацелено на кражу данных банковских карт, оставшиеся 6% предназначены для хищения учетных данных пользователей.

Исследователи выявили следующее распределение вредоносных ресурсов по типам:

- 70% — поддельные веб-сайты
- 13% — каналы и боты в мессенджерах
- 11% — группы в социальных сетях
- 4% — мобильные приложения
- 2% — объявления на торговых площадках.

Сфера электронной коммерции также находится под серьезным давлением киберпреступников. Количество фишинговых ресурсов в этом секторе увеличилось на 33,7%,

а среднее число угроз на один бренд достигло 405. Особую озабоченность вызывает рост числа скам-ресурсов на 20,7%, достигший показателя 1333 угрозы на бренд. [2]

В 2024 году в странах СНГ, включая Кыргызстан, наблюдался рост кибератак, в том числе фишинговых. Злоумышленники активно использовали методы социальной инженерии и вредоносное программное обеспечение для компрометации учетных записей сотрудников различных организаций. Особенно уязвимыми были сотрудники, работающие с конфиденциальной информацией, такие как специалисты IT, HR и топ-менеджмент. [3]

Фишинг остается одной из самых распространенных киберугроз, и, согласно статистике, количество таких атак продолжает расти. Современные фишинговые атаки становятся все сложнее, активно применяются технологии искусственного интеллекта (ИИ), что делает традиционные методы защиты менее эффективными.

В связи с этим возрастает необходимость использования ИИ и машинного обучения для защиты от фишинга. Такие технологии позволяют быстрее выявлять новые угрозы, снижать количество ложных срабатываний, автоматизировать обработку инцидентов и сокращать нагрузку на специалистов SOC. Это повышает эффективность защиты и снижает затраты на ее поддержку.

Методы обнаружения фишинга

С развитием технологий фишинговые атаки становятся все более сложными, требуя усовершенствованных методов их обнаружения. Наиболее перспективным направлением в борьбе с фишингом является использование искусственного интеллекта (ИИ), который позволяет анализировать атаки на более глубоком уровне и адаптироваться к новым угрозам. Однако традиционные методы также находят применение, особенно в комбинации с ИИ-алгоритмами.

Традиционные методы обнаружения фишинга. Исторически фишинг выявляли с помощью правил и сигнатур:

- Методы на основе правил используют заранее заданные эвристики, например, проверку подозрительных URL или подозрительных заголовков писем. [4]
- Сигнатурный анализ опирается на базы данных известных фишинговых шаблонов.

Преимущества традиционных методов:

- Простота реализации.
- Высокая скорость обнаружения известных угроз.

Недостатки:

- Неэффективность против новых, неизвестных атак.
- Требуется постоянное обновление баз данных.
- Высокая вероятность ложных срабатываний [4].

В современных условиях эти методы слабо защищают от фишинга, но могут дополнять другие подходы, например, ИИ-аналитику. Общие способы обнаружения описаны на рисунке 1 [5]

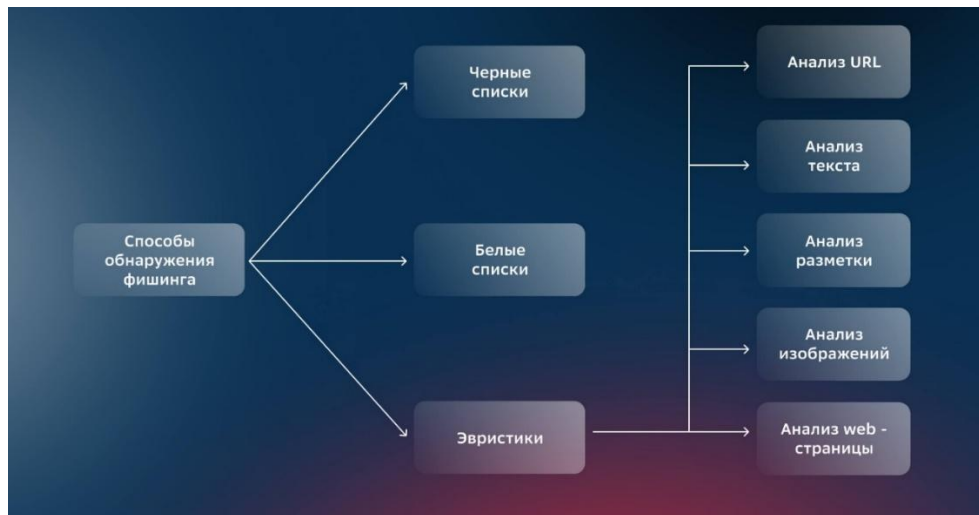


Рисунок 1 – Традиционные методы обнаружения фишинга

Методы машинного обучения

Алгоритмы машинного обучения (МО) анализируют массивы данных, выявляя фишинг без необходимости предварительно заданных правил. [4]

Контролируемое обучение (Supervised Learning)

Требуется размеченный набор данных с примерами фишинговых и безопасных писем. [5]

Популярные алгоритмы:

- Деревья решений – легко интерпретируемые модели, анализирующие признаки писем.
- Случайный лес – повышает точность за счет комбинации нескольких деревьев решений.
- SVM (метод опорных векторов) – эффективно классифицирует сложные случаи. [5]

Неконтролируемое обучение (Unsupervised Learning)

Используется, когда нет размеченных данных. Позволяет находить новые виды атак:

- Кластеризация (k-means, DBSCAN) – группирует похожие письма и выделяет аномалии.
- Обнаружение аномалий (Isolation Forests) – находит отклонения от нормального поведения. [4]

Преимущества МО:

- Высокая точность при достаточном количестве данных.
- Способность выявлять ранее неизвестные атаки.
- Автоматическая адаптация к новым угрозам [4].

Недостатки:

- Требуется больших объемов данных для обучения.
- Возможны ложные срабатывания [5].

Обработка естественного языка (NLP) для обнаружения фишинга

ИИ активно используется для анализа текстов писем с помощью методов обработки естественного языка (NLP). Это позволяет выявлять фишинговые атаки на основе содержания. [4]

Методы NLP включают:

- Классификацию текста (определяет, является ли письмо фишингом).
- Анализ тональности (подозрительные обращения, срочность, запугивание).
- Семантический анализ (поиск лексических признаков фишинга).

Современные модели NLP (например, BERT, GPT) анализируют текст глубже, чем простые эвристики.

Преимущества NLP:

- Учитывает смысл текста, а не только формальные признаки.
- Выявляет сложные фишинговые атаки [4].

Недостатки:

- Требует значительных вычислительных ресурсов.
- Сложность интерпретации [5].

Глубокое обучение в обнаружении фишинга

Глубокое обучение позволяет обнаруживать фишинг на более сложном уровне, автоматически выявляя закономерности в данных. [5]

Основные модели:

- CNN (сверточные нейронные сети) – анализируют URL и структуру письма.
- RNN и LSTM (рекуррентные сети) – обрабатывают текстовые последовательности, выявляя подозрительные фразы.
- Трансформеры (BERT, GPT) – отлично анализируют контекст, выявляя даже замаскированные атаки.

Преимущества:

- Высокая точность при анализе сложных атак.
- Способность учитывать контекст сообщений [5].

Недостатки:

- Высокие вычислительные затраты.
- Необходимость в больших объемах обучающих данных.

Общие различия машинного обучения и глубокого обучения изображены на рисунке

2.

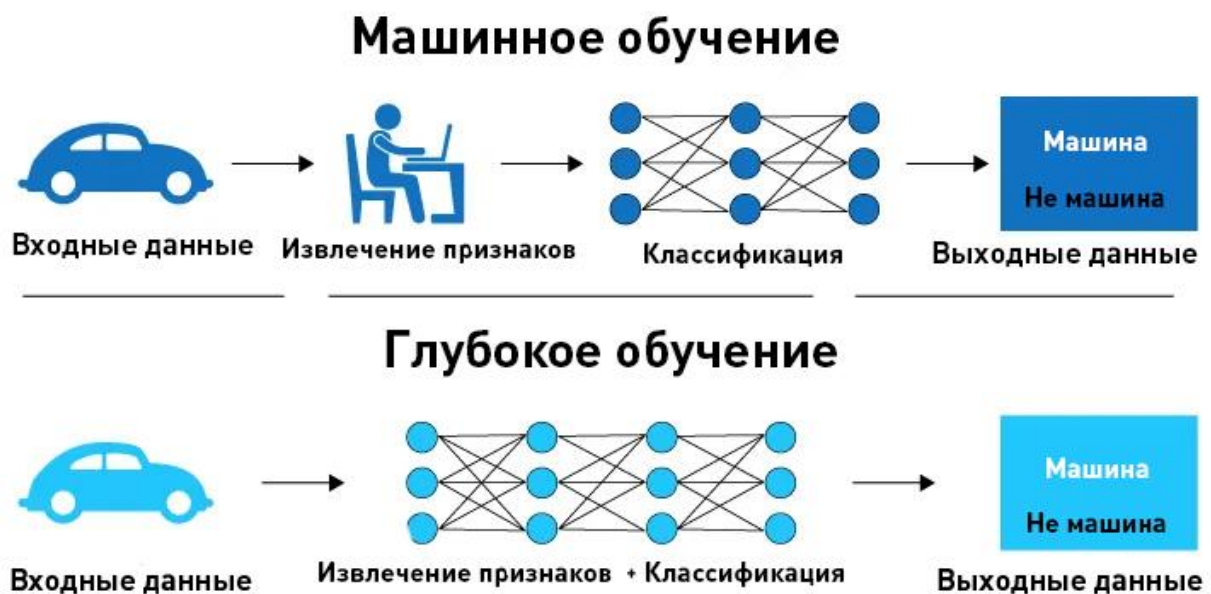


Рисунок 2 –Машинное и глубокое обучение

В таблице 1 описано сравнение различных методов защиты от фишинга по принципу работы, их преимущества, недостатки и актуальность.

Таблица 1 – Сравнение методов защиты от фишинга

Метод	Принцип работы	Преимущества	Недостатки	Актуальность
-------	----------------	--------------	------------	--------------

Методы на основе правил	Проверка заголовков, URL, ключевых слов по заданным эвристикам	Простота и скорость работы. Не требует сложных вычислений	Уязвим для новых атак. Высокая доля ложных срабатываний	Устарел, может использоваться в сочетании с ИИ
Сигнатурный анализ	Сравнение с базами известных фишинговых шаблонов	Быстродействие. Высокая точность для известных атак	Не выявляет новые угрозы. Требуется постоянное обновления баз	Эффективен только в комбинации с другими методами
Машинное обучение (ML)	Обучение модели на размеченных данных	Высокая точность. Адаптация к новым угрозам	Требуется обучающего набора данных. Возможны ложные срабатывания	Эффективен, но требует качественных данных
Обработка естественного языка (NLP)	Анализ текста, структуры писем, тональности	Учитывает контекст. Выявляет сложные атаки	Высокая нагрузка на вычислительные мощности	Перспективный метод, особенно с трансформерами (BERT, GPT)
Глубокое обучение (DL)	Автоматический анализ признаков с помощью нейросетей (CNN, RNN, трансформеры)	Высокая точность. Выявляет сложные фишинговые схемы	Требуется больших данных и ресурсов. Сложен в интерпретации	Один из наиболее эффективных подходов, но требует значительных вычислительных мощностей

ИИ-методы, особенно ML, NLP и DL, обеспечивают высокую точность и адаптацию к новым фишинговым атакам, превосходя традиционные подходы. Хотя они требуют качественных данных и вычислительных ресурсов, их применение является наиболее перспективным для эффективного обнаружения и предотвращения фишинга.

Анализ коммерческих систем обнаружения фишинга.

PhishLabs. PhishLabs предлагает комплексное решение для защиты от фишинговых атак. Система использует машинное обучение, анализ ссылок и URL-адресов, а также предоставляет детектирование фишинговых сайтов и фишинговых писем.

Преимущества:

- Полный анализ угроз в реальном времени.
- Поддержка различных типов фишинга, включая фишинг через социальные сети.
- Оповещения и отчеты для управления инцидентами.

Недостатки:

- Высокая стоимость, особенно для малого и среднего бизнеса.
- Требуется интеграция с другими системами безопасности.

Цена: от \$3,000 в год, в зависимости от масштаба и потребностей организации. [6]

Cofense (ранее PhishMe)

Cofense предлагает решения для обнаружения фишинга и обучения сотрудников, чтобы предотвратить атаки через фишинговые письма. Система использует как ручные, так и автоматические методы для обнаружения фишинговых угроз.

Преимущества:

- Высокая точность в классификации фишинговых писем.
- Инструменты для обучения сотрудников на основе реальных атак.
- Обширная база данных фишинговых сообщений.

Недостатки:

- Требуется постоянное обновление данных об угрозах.
- Дорогое решение для небольших компаний.

Цена: Цены варьируются от \$2,000 до \$10,000 в год, в зависимости от функционала и количества пользователей. [7]

Barracuda PhishLine

Barracuda PhishLine предлагает комплексное решение для обучения сотрудников и обнаружения фишинговых атак. Система использует как обучение через имитацию фишинга, так и активную защиту от фишинговых писем и ссылок.

Преимущества:

- Инструменты для создания тестов фишинговых атак и обучения сотрудников.
- Поддержка различных каналов (электронная почта, социальные сети).
- Интеграция с другими продуктами Barracuda для комплексной защиты.

Недостатки:

- Ограниченные возможности для обнаружения фишинга на уровне веб-сайтов.
- Не всегда эффективно работает против продвинутых фишинговых техник.

Цена: от \$1,200 до \$10,000 в год в зависимости от выбранных опций. [8]

Proofpoint. Proofpoint — это система, предназначенная для защиты от фишинговых атак через электронную почту и веб-сайты. Использует технологии ИИ для анализа письма и обнаружения подозрительных ссылок и вложений.

Преимущества:

- Высокая точность в фильтрации фишинговых писем.
- Обширный анализ угроз на основе ИИ и машинного обучения.
- Хорошая интеграция с другими корпоративными инструментами безопасности.

Недостатки:

- Высокая стоимость для малых и средних предприятий.
- Не всегда подходит для защиты от фишинга через каналы, отличные от электронной почты.

Цена: Цены начинаются от \$15,000 в год для малого бизнеса и могут достигать \$100,000+ для крупных организаций. [9]

KnowBe4

KnowBe4 предлагает систему для обучения сотрудников и обнаружения фишинговых атак. Включает в себя инструменты для имитации фишинга, обучение персонала и защиты от фишинговых угроз.

Преимущества:

- Мощный инструмент для тестирования сотрудников на фишинг.
- Постоянные обновления базы данных фишинговых угроз.
- Хорошая интеграция с системами безопасности.

Недостатки:

- Ограниченная способность в обнаружении фишинга на уровне веб-сайтов.
- Некоторые пользователи сообщают о сложности в интерфейсе и настройках.

Цена: от \$1,000 до \$15,000 в год в зависимости от пакета и количества пользователей. [10]

Mimecast

Mimecast предоставляет облачную защиту от фишинговых атак, включая фильтрацию электронной почты, защиту от вредоносных ссылок и обучение пользователей.

Преимущества:

- Простой интерфейс и хорошая настройка под организацию.
- Высокая точность в обнаружении фишинговых писем и вложений.
- Интеграция с другими решениями для безопасности в облаке.

Недостатки:

- Высокая цена на более высокие уровни защиты.
- Ограниченные возможности защиты от фишинга через социальные сети.

Цена: от \$5,000 в год для малого бизнеса до \$50,000+ для крупных организаций. [11]

В таблице 2 описано сравнение вышеупомянутых коммерческих систем обнаружения фишинга, а также разработка своей системы.

Таблица 2 – Сравнение систем

Система	Описание	Преимущества	Недостатки	Цена
PhishLabs	Комплексное решение для защиты от фишинга с анализом ссылок и URL	Полный анализ угроз в реальном времени; поддержка разных типов фишинга; Оповещения	Высокая стоимость; требуется интеграция с другими системами	От \$3,000 в год
Cofense (PhishMe)	Обнаружение фишинговых писем и обучение сотрудников	Высокая точность классификации; Инструменты обучения	Требует постоянного обновления данных; дорогое для небольших компаний	От \$2,000 до \$10,000 в год
Barracuda PhishLine	Имитация фишинга и обучение сотрудников	Создание тестов фишинговых атак; поддержка разных каналов	Ограниченные возможности обнаружения фишинга на веб-сайтах	От \$1,200 до \$10,000 в год
Proofpoint	Защита от фишинга через email и веб-сайты, ИИ-анализ	Высокая точность фильтрации; обширный анализ угроз	Высокая стоимость; ограниченная защита вне email	От \$15,000 до \$100,000+ в год
KnowBe4	Обучение сотрудников, имитация фишинга	Мощные инструменты тестирования; частые обновления базы угроз	Ограниченная защита веб-сайтов; сложный интерфейс	От \$1,000 до \$15,000 в год
Mimecast	Облачная защита email, фильтрация вредоносных ссылок	Простой интерфейс; интеграция с облачными сервисами	Высокая цена; ограниченная защита соцсетей	От \$5,000 до \$50,000+ в год
Разработка собственной системы	Использование модели ИИ для анализа текстов на фишинг	Гибкость настройки под бизнес; более низкая стоимость эксплуатации	Требует начальных затрат на разработку и обучение	Разовые затраты на разработку, дальнейшее обслуживание дешевле

Разработка собственной ИИ-системы требует начальных вложений, но в долгосрочной перспективе снижает затраты и позволяет гибко адаптировать защиту под бизнес-процессы. Коммерческие решения точны, но дороги и ограничены, тогда как своя система дает независимость и расширяемость.

Сравнение моделей ИИ для создания системы обнаружения фишинга

Для создания собственной системы необходимо выбрать модель ИИ, которая будет удовлетворять всем требованиям системы. Для этого нужно сравнить известные модели ИИ.

В таблице 3 приведено сравнение различных моделей ИИ для создания своей системы обнаружения фишинга.

Таблица 3 – Сравнение моделей ИИ

Модель	Описание	Плюсы	Минусы
BERT[12]	Трансформер с двусторонним контекстом	Высокая точность, отличная работа с контекстом	Высокие вычислительные требования, много данных
RoBERTa[13]	Улучшенная версия BERT	Повышенная точность, лучше для длинных текстов	Высокие затраты, сложная интерпретация
DistilBERT[14]	Облегченная версия BERT	Почти такая же точность, меньше ресурсов	Чуть хуже на сложных паттернах
FastText[19]	Быстрая модель для коротких текстов	Высокая скорость, низкие требования	Не учитывает контекст, неэффективен против сложных атак
XLNet[15]	Улучшенная версия трансформера	Высокая точность, лучше для сложных текстов	Высокие затраты, сложность настройки
GPT-4[17]	Генеративная модель	Отлично анализирует сложные схемы	Требует много ресурсов, трудно объяснить решения
InstructGPT[18]	GPT-3 для инструкций	Точные предсказания, анализ контекста	Требует подстройки, высокие затраты
T5	Модель для текстовых задач	Гибкость, адаптивность	Высокие ресурсы, долгое обучение
ERNIE[20]	Китайская версия BERT	Улучшенное понимание текста	Ограниченные ресурсы и документация
LightGBM[21]	Градиентный бустинг для структурированных данных	Быстро обучается, хорошо для табличных данных	Плохо с необработанным текстом
Hybrid Model (BERT + LightGBM)	BERT анализирует текст, LightGBM предсказывает	Сочетание точности и скорости	Сложность настройки, большие ресурсы

Графики сравнения моделей

Также при выборе модели ИИ необходимо обращать внимание на процент ложных срабатываний, чтобы он был не сильно высоким.

Уровень ложных срабатываний (%) для разных моделей описан в таблице 4.

Таблица 4 – Уровень ложных срабатываний

Модель	Ложные положительные (FP), %	Ложные отрицательные (FN), %	Общий процент
BERT	3.5%	4.2%	7.2%
RoBERTa	2.8%	3.5%	6.3%
DistilBERT	4.0%	5.1%	9.1%
FastText	7.5%	9.2%	16.6%
XLNet	2.7%	3.3%	6%
GPT-4	2.1%	3.0%	5.1%
InstructGPT	2.3%	3.5%	5.8%
T5	3.1%	4.0%	7.1%
ERNIE	2.9%	3.7%	6.6%
LightGBM	6.5%	8.0%	14.5%
Hybrid (BERT + LightGBM)	2.9%	3.5%	6.4%

На рисунке 3 изображен график, демонстрирующий процент ложных срабатываний у различных моделей ИИ.

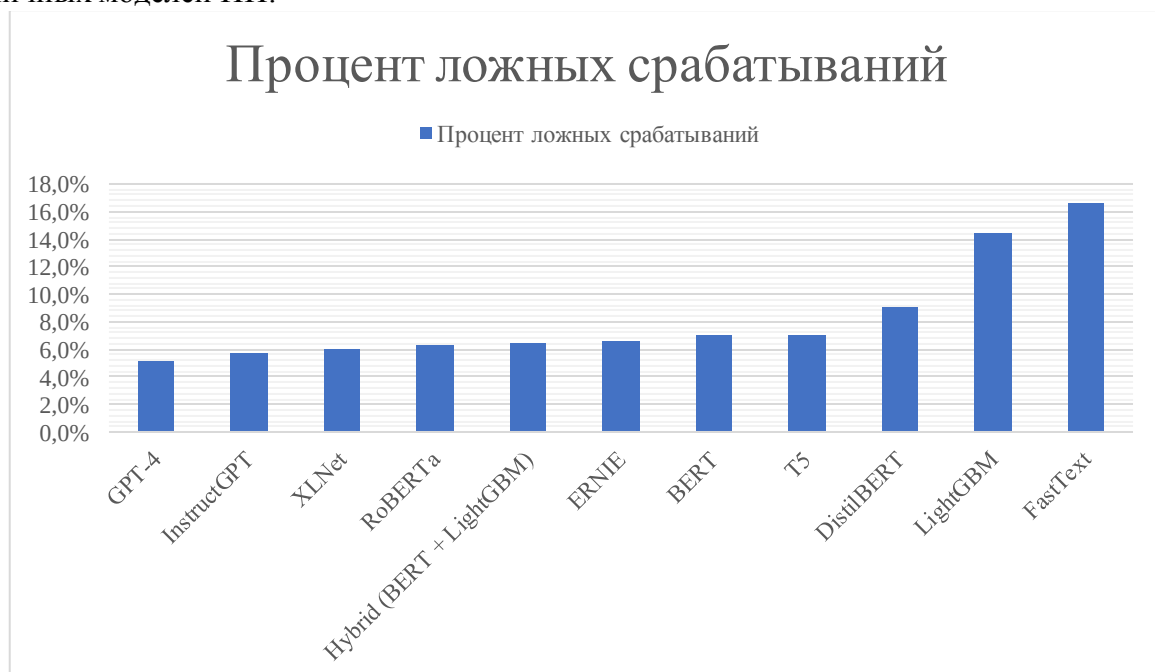


Рисунок 3 – График, демонстрирующий процент ложных срабатываний

Среднее время обработки одного запроса (мс) – еще один параметр, который влияет на скорость работы подсистемы – время обработки запросов. Чем быстрее идет обработка, тем больше писем подсистема сможет анализировать и обрабатывать.

В таблице 5 приведено среднее время обработки запроса для каждой модели ИИ.

Таблица 5 – Среднее время обработки одного запроса

Модель	Среднее время обработки (мс)
BERT	280
RoBERTa	320
DistilBERT	150
FastText	10
XLNet	350
GPT-4	450
InstructGPT	420
T5	380
ERNIE	300
LightGBM	15
Hybrid (BERT + LightGBM)	140

На графике сопоставлено среднее время обработки запроса различных моделей ИИ в порядке увеличения времени.



Рисунок 4 – График, демонстрирующий среднее время обработки одного запроса

Для максимальной точности: лучше использовать RoBERTa, GPT-4 или XLNet.

Для баланса скорости и точности: подойдут BERT, DistilBERT, ERNIE или гибридные модели.

Для быстрого, но менее точного анализа: можно использовать FastText или LightGBM.

Оптимальный вариант: гибридный BERT + LightGBM, так как он сочетает хорошую точность и приемлемую скорость.

Реальные примеры применения ИИ в борьбе с фишингом. Google Safe Browsing

Google использует искусственный интеллект для анализа веб-сайтов и выявления фишинговых страниц. Система анализирует сайты на наличие подозрительных ссылок, а также проверяет их репутацию, применяя различные алгоритмы машинного обучения. По данным Google, использование таких технологий помогло значительно снизить количество успешных фишинговых атак. [27] Anti-Phishing Working Group (APWG). APWG использует ИИ для сбора и анализа данных о фишинговых сайтах и письмах, делая их доступными для

общественности. Системы на основе ИИ автоматизируют процесс идентификации фишинговых атак, что помогает быстрее реагировать на угрозы. [27]

Проведение исследования Kaspersky

Kaspersky проводил исследование, насколько хорошо ChatGPT может обнаруживать фишинг. По итогам нескольких проверок, если дать ChatGPT только URL-ссылку на веб-сайт, то результат после всех ошибок и отказов будет следующий: «Мы остались с набором данных из 2322 фишинговых и 2943 легитимных URL-адресов. Итоговые показатели:

- Доля обнаруженного фишинга (detection rate, DR): **87,2%**.
- Доля ложных срабатываний (false positive rate, FPR): **23,2%**».

Также есть статья «URLNet: изучение представления URL с помощью глубокого обучения для обнаружения вредоносных URL». В данной статье предоставляется ROC-кривая, иллюстрирующая достигаемые доли истинных обнаружений (уровень обнаружения) и ложных.

При этом ChatGPT хорошо извлекает название компаний из ссылок, указывает данные на сервис WhoIs, на контент веб-сайта, на срок действия сертификата SSL и т.п.

На рисунке 6 изображена ROC-кривая, иллюстрирующая достигаемые доли истинных обнаружений (уровень обнаружения) и ложных.

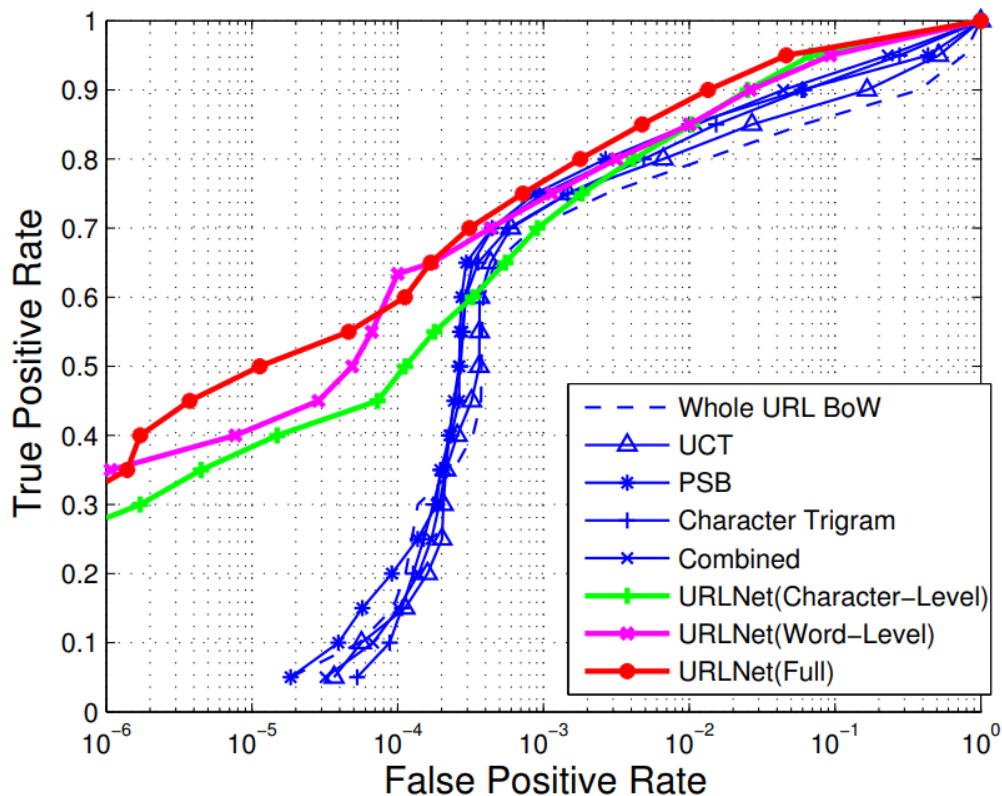


Рисунок 6 – ROC-кривая из статьи Лэ и других авторов за 2018 год

Учитывая, что ChatGPT в этих экспериментах работала в режиме zero-shot, то есть без обучения на примерах, результаты поразительны. Это использование ИИ эффективно для обнаружения фишинга, если модель хорошо натренировать. [28]

Выбор модели ИИ

Для эффективного обнаружения фишинговых атак используются различные модели искусственного интеллекта (ИИ), каждая из которых имеет свои преимущества в зависимости от задачи. Среди популярных моделей выделяются трансформеры, такие как BERT, и модели на основе градиентного бустинга, например, LightGBM.

Модель BERT (Bidirectional Encoder Representations from Transformers), разработанная Google, зарекомендовала себя как мощный инструмент для анализа текстов благодаря своей способности учитывать контекст слов в обе стороны. Модификации BERT, такие как RoBERTa и DistilBERT, обеспечивают еще более высокую точность. В задаче обнаружения фишинга такие модели могут эффективно распознавать сложные паттерны фишинговых сообщений и сайтов, но требуют значительных вычислительных ресурсов. Применение **BERT** в реальных системах, таких как у Яндекса для определения фишинговых сайтов, позволяет достигать точности до 99,9%.

С другой стороны, модели на основе градиентного бустинга, такие как LightGBM, тоже показывают хорошие результаты, особенно при работе с табличными данными, такими как URL или метаданные. Эти модели быстро обучаются и могут обрабатывать запросы за несколько миллисекунд, однако их точность ниже по сравнению с трансформерами, и они менее эффективны при работе с неструктурированными текстовыми данными.

Большие языковые модели, такие как GPT-4, также нашли свое применение в детектировании фишинговых атак. В исследованиях, таких как «ChatSpamDetector: Leveraging Large Language Models for Effective Phishing Email Detection», показано, что GPT-4 может достичь точности 99,7% при обнаружении фишинговых писем, но требует значительных вычислительных мощностей и более длительного времени обработки.

Таким образом, для создания системы обнаружения фишинга оптимальным выбором будет модель, которая сочетает высокую точность и достаточную скорость обработки. Модели на основе трансформеров, такие как BERT и RoBERTa, предпочтительны для задач, требующих глубокого понимания текста и контекста. В то время как LightGBM может быть хорошим выбором для быстрых решений с меньшими вычислительными затратами, но с компромиссами по точности.

BERT и трансформеры

Трансформеры – это архитектура нейросетей, применяемая в обработке естественного языка (NLP). Они работают на основе механизма *self-attention* (самовнимания), позволяющего анализировать контекст слова с учетом всех остальных слов в предложении. В отличие от рекуррентных сетей (RNN) трансформеры обрабатывают весь текст одновременно, что делает их более эффективными.

Основные компоненты трансформера:

- Self-attention – вычисляет вес слов относительно друг друга.
- Feed-forward слои – обрабатывают информацию после механизма внимания.
- Embeddings – представляют слова в числовом формате.
- Многоголовое внимание (multi-head attention) – анализирует разные контексты одновременно.
- Нормализация и пропускные соединения – помогают стабилизировать обучение.

BERT – это модель на основе трансформеров, разработанная Google. Ее ключевая особенность – двунаправленное обучение: модель анализирует текст как слева направо, так и справа налево, что улучшает понимание контекста.

Как работает BERT:

1. Входные данные: текст преобразуется в токены (единицы текста).
2. Embeddings: токены конвертируются в векторы.
3. Трансформер-энкодеры: несколько слоев обрабатывают информацию через механизмы самовнимания.
4. Выходные данные: полученные представления используются для различных NLP-задач (анализ тональности, машинный перевод, чат-боты).

BERT обучается с помощью двух задач:

- Masked Language Model (MLM) – часть слов в предложении заменяется на [MASK], и модель учится предсказывать их.

- Next Sentence Prediction (NSP) – модель определяет, связаны ли два предложения друг с другом.

На рисунке 7 изображен принцип работы BERT, где есть входные данные – два предложения, в которых по слову замаскировано, и BERT должен предсказать их. Также он должен определить, связаны ли между собой два предложения. Для работы слова, начало и разделения (точки) преобразуются в векторное представление токенов, а также пишется разделение предложений на А (первое) и В (второе). И также проставляется порядок слов. [33]

		[MASK]				[MASK]			
Входные значения	[CLS]	моя	собака	милая	[SEP]	она	любит	играть	[SEP]
Векторные представления токенов	$E_{[CLS]}$	$E_{\text{моя}}$	E_{mask}	$E_{\text{милая}}$	$E_{[SEP]}$	$E_{\text{она}}$	$E_{\text{[MASK]}}$	$E_{\text{играть}}$	$E_{[SEP]}$
	+	+	+	+	+	+	+	+	+
Векторное представление предложения	E_A	E_A	E_A	E_A	E_A	E_B	E_B	E_B	E_B
	+	+	+	+	+	+	+	+	+
Позиционное кодирование в трансформере	E_0	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8

Рисунок 7 — Принцип работы BERT

Заключение

Подводя итоги проведенного аналитического обзора, можно говорить о том, что процесс разработки подсистемы SOC для защиты от фишинговых атак с применением технологий искусственного интеллекта и машинного обучения является актуальным и востребованным направлением в кибербезопасности. В ходе исследования были рассмотрены традиционные методы обнаружения фишинга, выявлены их ограничения и проведен анализ современных подходов на основе ИИ. Проведенное сравнение коммерческих решений показало, что готовые системы обладают высокой эффективностью, но требуют значительных финансовых вложений и адаптации под конкретные бизнес-процессы.

В ходе анализа моделей ИИ было установлено, что наиболее перспективным решением являются трансформерные архитектуры, в частности BERT и его модификации, которые демонстрируют высокую точность в выявлении фишинговых атак. Использование современных алгоритмов обработки естественного языка и методов машинного обучения позволяет адаптировать системы обнаружения фишинга к новым угрозам, повышая их эффективность в реальных условиях.

Следует отметить, что предложенный в работе подход к разработке собственной подсистемы SOC на основе ИИ представляется перспективным направлением, обеспечивающим эффективную защиту от фишинговых угроз, адаптивность к новым видам атак и снижение нагрузки на специалистов по кибербезопасности. Несмотря на необходимость первоначальных затрат на разработку и обучение моделей, в долгосрочной перспективе такие решения способны повысить уровень защиты информационных систем и оптимизировать процессы реагирования на инциденты.

Литература

1. Спам и фишинг в 2024 году – https://securelist.ru/spam-and-phishing-report-2024/111743/?utm_source=chatgpt.com (дата обращения 10.01.2025г.)
2. Число фишинговых сайтов, имитирующих финансовые бренды, выросло почти на 50% – <https://cybersecurefox.com/ru/rost-fishinga-finansoviy-sektor-2024/> (дата обращения 12.01.2025г.)

3. Актуальные киберугрозы в странах СНГ 2023—2024 – https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/?utm_source=chatgpt.com (дата обращения 15.01.2025г.).
4. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ АЛГОРИТМОВ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ЗАЩИТЫ ОТ ФИШИНГОВЫХ АТАК – https://cyberleninka.ru/article/n/issledovanie-vozmozhnostey-algoritmov-glubokogo-obucheniya-dlya-zaschity-ot-fishingovykh-atak?utm_source=chatgpt.com (дата обращения 20.01.2025г.).
5. PhishLabs – <https://www.phishlabs.com/> (дата обращения 25.01.2025г.).
6. Cofense – <https://cofense.com/> (дата обращения 27.01.2025г.).
7. Barracuda – <https://www.barracuda.com/products/email-protection/plans> (дата обращения 30.01.2025г.).
8. Proofpoint – <https://www.proofpoint.com/us> (дата обращения 10.02.2025г.).
9. KnowBe4 – <https://www.knowbe4.com/> (дата обращения 12.02.2025г.).
10. Mimecast – <https://www.mimecast.com/products/email-security/> (дата обращения 15.02.2025г.).
11. Barracuda vs KnowBe4 – https://www.gartner.com/reviews/market/security-awareness-computer-based-training/compare/barracuda-vs-knowbe4?utm_source=chatgpt.com (дата обращения 20.02.2025г.).
12. Barracuda Security Awareness Training Alternatives – <https://www.gartner.com/reviews/market/security-awareness-computer-based-training/vendor/barracuda/product/barracuda-security-awareness-training/alternatives> (дата обращения 25.02.2025г.).
13. Attention Is All You Need - <https://arxiv.org/abs/1706.03762> (дата обращения 28.02.2025г.).
14. RoBERTa: A Robustly Optimized BERT Pretraining Approach - <https://arxiv.org/abs/1907.11692> (дата обращения 30.02.2025г.).
15. DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter – <https://arxiv.org/abs/1910.01108> (дата обращения 05.03.2025г.).
16. XLNet: Generalized Autoregressive Pretraining for Language Understanding – <https://arxiv.org/abs/1906.08237> (дата обращения 07.03.2025г.).
17. Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer – <https://arxiv.org/abs/1910.10683> (дата обращения 10.03.2025г.).
18. GPT-4 - <https://openai.com/index/gpt-4-research/> (дата обращения 12.03.2025г.).
19. Language Models are Few-Shot Learners - <https://arxiv.org/abs/2005.14165> (дата обращения 15.03.2025г.).
20. Enriching Word Vectors with Subword Information – <https://arxiv.org/abs/1607.04606> (дата обращения 18.03.2025г.).
21. ERNIE: Enhanced Representation through Knowledge Integration – <https://arxiv.org/abs/1904.09223> (дата обращения 20.03.2025г.).
22. LightGBM: A Highly Efficient Gradient Boosting Decision Tree – https://proceedings.neurips.cc/paper_files/paper/2017/file/6449f44a102fde848669bdd9eb6b76fa-Paper.pdf (дата обращения 20.03.2025г.).
23. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding - <https://arxiv.org/abs/1810.04805> (дата обращения 21.03.2025г.).
24. Глубокое обучение в борьбе с фишингом: как ИИ распознает угрозы – https://cisoclub.ru/glubokoe-obuchenie-v-borbe-s-fishingom-kak-ii-raspoznayet-ugrozy/?utm_source=chatgpt.com (дата обращения 22.03.2025г.).
25. Исследование возможностей алгоритмов глубокого обучения для защиты от фишинговых атак - <https://www.sberbank.ru/ru/person/kibrary/experts/issledovanie-vozmozhnostej-algoritmov-glubokogo-obucheniya-dlya-zashchity-ot-fishingovykh-atak> (дата обращения 23.03.2025г.).

26. AI-Driven Phishing Detection Systems – https://www.researchgate.net/publication/382917933_AI-Driven_Phishing_Detection_Systems (дата обращения 24.03.2025г.).
27. Защита от фишинга с ИИ (искусственного интеллекта) – <https://domznaniya.ru/page/zashchita-ot-fishinga-s-ii-iskusstvennogo-intellekta-4972291607/> (дата обращения 26.03.2025г.).
28. Что ChatGPT знает о фишинге? – <https://securelist.ru/chatgpt-anti-phishing/107389/> (дата обращения 05.03.2025г.). (дата обращения 26.03.2025г.).
29. Зоопарк трансформеров: большой обзор моделей от BERT до Alpaca – https://habr.com/ru/companies/just_ai/articles/733110/ (дата обращения 27.03.2025г.).
30. Роль ИИ в обеспечении ИБ: Яндекс.Толока и модель BERT для выявления фишинговых атак - <https://baskobrin.ru/blog/rol-ii-v-obespechenii-ib-yandeks-toloka-i-model-bert-dlya-vyyavleniya-fishingovyh-atak> (дата обращения 27.03.2025г.).
31. PhishNet: A Phishing Website Detection Tool using XGBoost – <https://arxiv.org/abs/2407.04732> (дата обращения 28.03.2025г.).
32. ChatSpamDetector: Leveraging Large Language Models for Effective Phishing Email Detection – <https://arxiv.org/abs/2402.18093> (дата обращения 28.03.2025г.).
33. BERT в двух словах: Инновационная языковая модель для NLP – <https://habr.com/ru/companies/otus/articles/702838/> (дата обращения 29.03.2025г.).

Ю.С. Корякина, jk169@list.ru

Институт машиноведения автоматизации и геомеханики НАН КР

М.Э. Эсенбекова, meerimaesenbekova@gmail.com

Институт информационных технологий КГТУ им. И. Раззакова

ОБЗОР ПОДХОДОВ РЕАЛИЗАЦИИ ПОДСИСТЕМ ЗАЩИТЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В СОСТАВЕ SOC

Современные корпоративные сети сталкиваются с растущими угрозами кибератак, что требует применения передовых технологий защиты. В данной работе проведен аналитический обзор методов реализации подсистем обнаружения и предотвращения вторжений (IDS/IPS) в составе центров мониторинга безопасности (SOC). Рассмотрены теоретические аспекты работы сетевых и хостовых решений (NIDS, HIDS, NIPS, HIPS), а также методы анализа поведения сети (NBA). Проанализированы современные подходы к интеграции технологий Suricata, Zeek и Security Onion, их функциональные возможности, принципы работы и сравнительная эффективность. Особое внимание уделено вопросам корреляции событий, минимизации ложных срабатываний, взаимодействия с SIEM-системами и автоматизации реагирования на инциденты. В работе рассмотрены преимущества и недостатки различных технологий, а также предложена схема комплексного подхода к обеспечению безопасности корпоративных сетей. В заключение сформулированы рекомендации по выбору оптимальных решений для построения устойчивой системы защиты, способной эффективно противодействовать современным угрозам.

Ключевые слова: SOC, IDS, IPS, информационная безопасность, NIDS, HIDS, NIPS, HIPS, NBA, корреляция событий, сигнатурный анализ, поведенческий анализ, автоматическое предотвращение атак, SIEM, SOAR.

Введение

В условиях стремительной цифровой трансформации и роста угроз ИБ актуальность разработки современных методов реализации подсистем защиты обнаружения и предотвращения вторжений для центров мониторинга безопасности (SOC) приобретает особое значение. Современные организации сталкиваются с динамично меняющейся средой, где злоумышленники постоянно совершенствуют свои методики, используя автоматизированные инструменты и эксплуатируя уязвимости в критически важных программных решениях. Объектом исследования являются методы и технологии обеспечения безопасности корпоративных сетей в рамках SOC. Предметом исследования являются методы обнаружения и предотвращения сетевых атак с использованием систем IDS/IPS в составе SOC. В работе особое внимание уделяется разработке и интеграции подсистемы IDS/IPS, анализу методов детектирования угроз ИБ, а также механизму автоматического предотвращения атак. Рассматриваются вопросы корреляции событий, минимизации ложных срабатываний, взаимодействия IDS/IPS с SIEM-системами и влияние предложенного решения на эффективность защиты.

По данным Лаборатории Касперского, в первом полугодии 2024 года зафиксирован кратный рост атак на сферы телекоммуникаций и строительства, что свидетельствует о том, что ключевые отрасли инфраструктуры становятся приоритетными целями для киберпреступников. Такой рост атак отражает не только увеличение количества инцидентов, но и их возрастающую сложность, поскольку злоумышленники применяют новые методы обхода традиционных систем защиты. [1]

Отчет ICS CERT за второй квартал 2024 года демонстрирует, что в промышленном секторе происходят регулярные инциденты, направленные на вывод из строя производственных систем или кражу технологической информации, что может привести к

значительным экономическим потерям и подрыву доверия к инфраструктурной безопасности предприятий. [2]

Особенно тревожной является информация о том, что каждая четвертая компания в мире столкнулась с АРТ-угрозами в 2024 году. АРТ-атаки, отличающиеся многоступенчатостью и длительностью, представляют особую сложность для традиционных систем защиты, так как требуют комплексного анализа и корреляции данных. Атаки такого типа направлены на кражу конфиденциальной информации, включая персональные данные, коммерческие тайны и финансовые сведения, что подрывает не только репутацию, но и конкурентоспособность организаций. Наряду с этим возрастает число DDoS-атак, направленных на перегрузку сетевых ресурсов, что приводит к временному нарушению работы сервисов и снижению доступности корпоративных систем. Такие атаки существенно влияют на оперативную деятельность организаций и требуют эффективного обнаружения и реагирования в режиме реального времени. [3]

По данным глобальной сети центров очистки трафика, всего системы StormWall в 2024 году предотвратили 6,6 млн DDoS-атак по всему миру. Средняя продолжительность атаки составила 23 минуты. Количество инцидентов с продолжительностью больше 1 часа увеличилось на 120%. При этом средняя мощность атак выросла на 53%. Самая мощная DDoS-атака, предотвращенная StormWall в 2024 году, достигала 1,6 Тбит/с. Из всего количества DDoS-атак, предотвращенных StormWall, 59% были направлены на прикладной уровень модели OSI, а точнее — на протокол HTTP. [4] На рисунке 1 представлена статистика DDoS-атак StormWall.

Квартал	Количество предотвращённых DDoS-атак	Рост за квартал
1 кв. 2024	1,2 млн	-
2 кв. 2024	1,4 млн	16,7 %
3 кв. 2024	1,7 млн	21,4 %
4 кв. 2024	2,3 млн	35,3 %

Рисунок 1 — Статистика DDoS-атак StormWall

Считается, что традиционные решения IPS/IDS, развернутые на различных платформах, обладают рядом недостатков, существенно влияющих на их эффективность, а именно:

1. Большое количество аппаратных ресурсов.
2. Большое количество программных ресурсов.
3. Существенных финансовых затрат.
4. Отсутствие одного интерфейса, что приводит к фрагментации процессов мониторинга и анализа угроз, что усложняет оперативное реагирование на инциденты.
5. Ограничения в функциональных возможностях.
6. Не имеют автономности и зависят от других компонентов SOC, а именно от SIEM и SOAR систем.

Поэтому для обеспечения надежной защиты корпоративных сетей необходим комплексный подход, объединяющий возможности различных систем мониторинга и анализа угроз в единую интегрированную платформу.

Основа IPS/IDS, принцип работы

IDS (Intrusion Detection System) — это система обнаружения вторжений, а IPS (Intrusion Prevention System) — система предотвращения вторжений. Они настолько близки и похожи, что обычно упоминаются в связке друг с другом. Кроме того, ранее IDS было отдельным инструментом, но позднее вошло в состав IPS. Если сравнивать их с традиционными решениями информационной безопасности, то IDS/IPS способны добиться более высокого уровня сетевой защиты. [5] IDS представляет собой пассивную систему, которая сканирует трафик и сообщает об угрозах. IDS никоим образом не изменяет сетевые пакеты, тогда как IPS предотвращает доставку пакета в зависимости от содержимого пакета, подобно тому, как межсетевой экран предотвращает трафик по IP-адресу. IPS – это средство безопасности для предотвращения сетевых угроз. Система исследует сетевой трафик, потоки для предотвращения эксплойтов, злонамеренных действий с целевым приложением или службой. Все для того, чтобы злоумышленники не смогли прервать работу компании и получить контроль над приложением или конечной точкой. [6]

IDS функционируют в режиме мониторинга и анализа сетевого трафика или активности хостов. Они сравнивают поступающие данные с известными шаблонами атак (сигнатурами) или выявляют аномальное поведение, после чего уведомляют администраторов о подозрительной активности. Однако IDS не могут блокировать атаки самостоятельно. IPS работают аналогично IDS, но с ключевым отличием – они не только обнаруживают угрозы, но и принимают активные меры по их блокировке. IPS могут автоматически фильтровать вредоносный трафик, разрывать соединения и предотвращать выполнение вредоносного кода, действуя в режиме реального времени.

Принцип работы IPS/IDS можно описать следующим образом:

1. Мониторинг трафика: Система получает копии сетевых пакетов или анализирует журналы событий, чтобы отслеживать деятельность в сети или на хостах.
2. Анализ данных:
 - Сигнатурный анализ: сравнивает данные с базой известных шаблонов атак (например, SQL-инъекций, DDoS-атак).
 - Анализ аномалий: оценивает, соответствует ли поведение сети или хоста нормальным параметрам. Аномалии могут быть вызваны необычными пиками трафика или подозрительными действиями.
3. Обнаружение угроз: если найдена угроза, IDS создает уведомление (алерт), а IPS немедленно принимает меры.
4. Реакция на угрозу:
 - Для IDS: Система записывает событие и уведомляет администратора.
 - Для IPS: Система автоматически блокирует вредоносный трафик или действия (например, завершает соединение или запрещает доступ к ресурсу).

IPS/IDS часто интегрируются в межсетевые экраны (firewalls) и работают на уровне сетевого трафика или хостов для обеспечения максимальной безопасности.

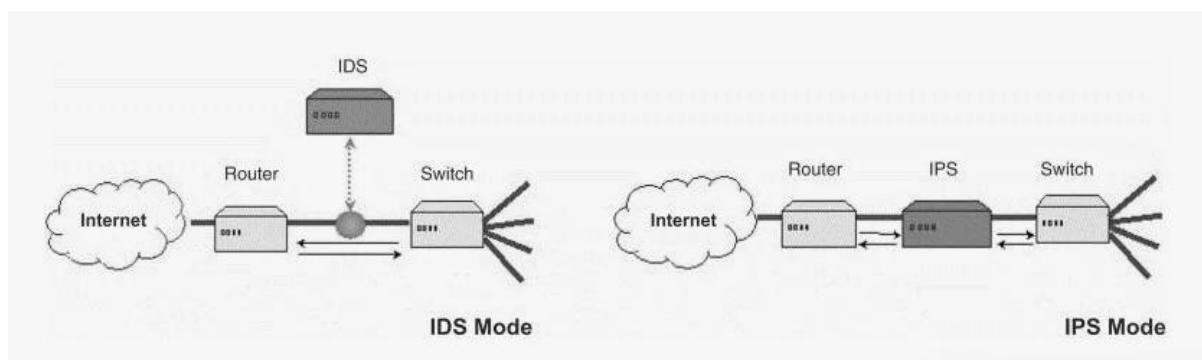


Рисунок 2 — Схема работы IPS/IDS

На рисунке 2 представлены две схемы, иллюстрирующие работу систем IDS и IPS в сетевой инфраструктуре:

1. IDS Mode (слева):
 - В этой конфигурации система IDS расположена параллельно сетевому трафику.
 - Роутер передает трафик к коммутатору, и система IDS получает копию трафика через механизм зеркалирования портов (Port Mirroring или SPAN).
 - IDS анализирует трафик, но не вмешивается в процесс его передачи.
 - Если обнаружена угроза, IDS генерирует уведомление для администратора, но не блокирует угрозу самостоятельно.
2. IPS Mode (справа):
 - Здесь система IPS расположена непосредственно в пути сетевого трафика между роутером и коммутатором.
 - IPS анализирует трафик в режиме реального времени.
 - При обнаружении угрозы IPS может заблокировать вредоносные пакеты, прервать соединение или применить другие защитные меры.
 - Таким образом, IPS активно участвует в защите сети, предотвращая потенциальные атаки.

Ключевое различие между двумя режимами заключается в том, что IDS работает в режиме мониторинга (пассивно), тогда как IPS действует в режиме вмешательства (активно).

Аналитический обзор существующих мер для реализации поставленных задач

На сегодняшний день существует широкий спектр методов и технологий для создания подсистем обнаружения и предотвращения вторжений (IDS/IPS), которые интегрируются в инфраструктуру SOC (Security Operations Center) для обеспечения комплексной информационной безопасности. Эти меры направлены на эффективное выявление угроз, минимизацию ложных срабатываний и автоматизацию реагирования.

На рисунке 3 представлены основные методы обнаружения вторжений, которые классифицируются по их функциональным возможностям.

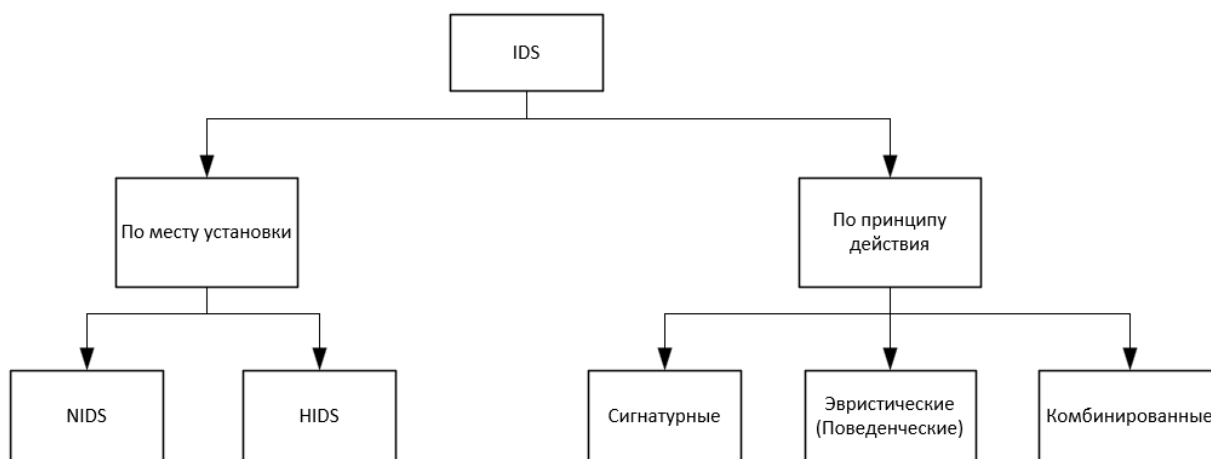


Рисунок 3 — Систематизация методов обнаружения вторжений (IDS)

Системы IDS различаются по месту установки и по принципу действия. В зависимости от места расположения IDS делятся на *сетевые* (network-based IDS, NIDS) и *хостовые* (host-based, HIDS). [7] IDS уровня сети (NIDS) используют сенсоры, являющиеся отдельными компьютерами с установленным на них специальным программным обеспечением либо специальными выделенными устройствами (appliance). Каждый сенсор имеет сетевую карту (NIC – network interface card), работающую в режиме прослушивания сети (promiscuous mode). Обычные сетевые карты получают только сетевые пакеты, адресованные этой сетевой карте, широковещательные (broadcast) и много адресные (multicast) пакеты. Драйвер сетевой карты копирует данные из передающей среды и отправляет его стеку сетевых протоколов для обработки. Если сетевая карта находится в режиме прослушивания, драйвер сетевой карты захватывает весь трафик, делает копии всех пакетов, а затем передает одну копию в стек TCP, а вторую копию – анализатору для поиска определенных шаблонов (сигнатур). NIDS контролирует сетевой трафик и не может увидеть действия, происходящие внутри отдельного компьютера. Для отслеживания таких действий следует использовать IDS уровня хоста. [8] IDS уровня хоста (HIDS) может быть установлена на отдельные рабочие станции и/или серверы для выявления нежелательных или аномальных действий. HIDS обычно используются для обеспечения уверенности, что пользователи не удаляют системные файлы, не изменяют важные настройки или подвергают систему риску иными способами. Так, если NIDS понимает и контролирует сетевой трафик, средства HIDS ограничиваются только самим компьютером. HIDS не понимает и не отслеживает сетевой трафик, а NIDS не контролирует действия внутри системы. Каждое из этих средств имеет свои задачи и выполняет их своими способами. В большинстве сред системы HIDS устанавливаются только на критичные серверы, а не на каждый компьютер в сети, поскольку это могло бы вызвать существенное повышение нагрузки на компьютеры и на администраторов. [8]

HIDS и NIDS могут быть одного из следующих типов:

- Сигнатурные (signature based).
- Поведенческие или эвристические (heuristic-based).
- Комбинированные.

1) **Сигнатурные методы.** Сигнатурные методы обнаружения вторжений – на основе сигнатур обычно используются в системах обнаружения вторжений, в которых содержатся сигнатуры (шаблоны) типовых атак, созданные на основе заголовков или содержимого сетевых пакетов. Большое количество сигнатур делает этот метод более затратным с точки зрения стоимости вычисления. Для решения этого ограничения был предложен метод, сочетающий новый метод анализа данных с традиционным сопоставлением с сигнатурами. Главным преимуществом этого подхода является увеличение

производительности сигнатурного метода и уменьшение ложных срабатываний [9], поскольку поиск идет только в определенных частях пакетов. [9] При сигнатурном методе система анализирует сетевые пакеты или логи. Далее полученные данные проверяются на соответствие известным шаблонам атак. Если обнаружена совпадающая сигнатура, IDS фиксирует инцидент и отправляет администратору или в SOC. На рисунке 4 представлен сигнатурный метод обнаружения вторжений.

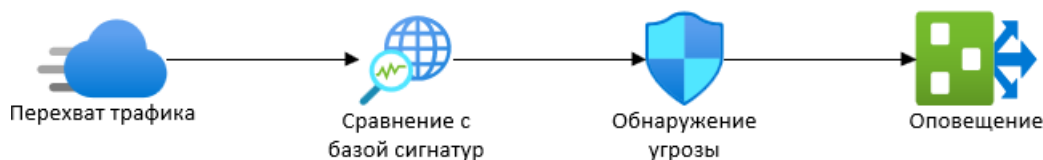


Рисунок 4 — Сигнатурный метод обнаружения вторжений

Преимущества сигнатурного метода: эффективное определение атак на ИС, отсутствие большого числа ложных срабатываний [9], надежное определение использования конкретного инструментального средства или метода атаки, возможность наиболее точно задать параметры сигнатуры.

Недостатки сигнатурного метода: необходимость обновлять базы сигнатур для обнаружения новых атак; невозможность выявления атак, не описанных в экспертной системе; невозможность выявить атаки, отличающиеся от сигнатурного описания, либо без описания.

2) Поведенческие методы. Поведенческие методы основаны не на моделях информационных атак, а на моделях «нормального» функционирования ИС. Принцип работы любого из этих методов состоит в обнаружении расхождении [9] между текущим режимом работы информационной системы и режима работы, который является эталонным для этой ИС. Любое несоответствие рассматривается как вторжение или аномалия. Сложностью данного принципа является создание точной эталонной модели «нормального» режима информационной системы. [9]



Рисунок 5 — Поведенческий метод обнаружения вторжений

На рисунке 5 представлен поведенческий метод обнаружения вторжений, который сопровождается этапами, описанными далее. Система мониторинга сетевого трафика и действий пользователей собирает данные. Далее строится нормальная модель поведения (на основе машинного обучения или эвристики) и выявляются отклонения от норм (высокая активность, необычные запросы, новые соединения). Если зафиксировано подозрительное поведение, система помечает его как возможную атаку. В конце отправка уведомлений, регистрация или передача данных в IPS для блокировки.

Преимущества поведенческого метода: определение атаки без знания конкретных деталей (сигнатуры); детекторы аномалий [9] могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур атак. высокая чувствительность к изменениям состоянии [9] ИС.

Недостатки поведенческого метода: ложные сигналы при непредсказуемом поведении пользователей; ложные срабатывания при непредсказуемой сетевой активности; временные затраты на этапе обучения системы.

У каждого принципа есть свои методы, построенные на основе этих принципов. **Сигнатурные методы:** Метод контекстного поиска состоит в обнаружении в исходной информации определенного набора символов. Например, для обнаружения атак на веб-сервера под Unix подобные ОС, направленной на получение несанкционированного доступа к файлу паролей, производится поиск последовательности символов "*/e c/ra" в заголовке запроса HTTP.

Методы анализа состояния основаны на формировании сигнатур атак в виде последовательности переходов информационной системы из одного состояния в другое. **наборы таких событий** — задается параметрами сигнатур атак.

Поведенческие методы (методы обнаружения аномалий): Методы, основанные на статистических моделях, определяют статистические показатели, характеризующиеся параметрами регулярного поведения системы. Если с течением времени есть некоторое отклонение этих параметров от заданных значений, то фиксируется обнаружение атаки. [9]

3) Комбинированные методы: Метод продукционных правил позволяют описать модели для атак на естественном языке с высоким уровнем абстракции. Экспертные системы, использующие эти методы, состоят из двух баз данных: факты и правила. Факты являются входными данными из информационной системы, а правила алгоритмы для логических решений — о факте нападения на основе входящего набора фактов. Полученная система правил должна описывать характеристики атак, которые должна обнаружить система обнаружения вторжения. [9]

База правил. С помощью экспертной системы можно точно определить взаимодействие между узлами ИС, которое всегда осуществляется в соответствии с определенными протоколами. Если в процессе обмена информацией между узлами появляется неизвестная команда или нестандартное значение одного из параметров, можно считать это признаком атаки.

Метод имитации поведения биологических систем не использует алгоритмы моделей, основанных на биологических объектах, таких как генетические алгоритмы и искусственные нейронные сети (ИНС). Методы, основанные на биологических моделях, считаются наиболее перспективным в первую очередь из-за их адаптации и саморазвития.

На этапе вторжения можно обнаруживать атаку как сигнатурным, так и поведенческим методом. Любое вторжение характеризуется определенными особенностями, которые, с одной стороны, могут быть представлены в виде сигнатур, а с другой, как своего рода отклонение от эталонного поведения информационной системы. Наиболее эффективное сочетание обоих методов одновременно, при этом для получения необходимых входных данных применить любые (сетевые либо узловые) датчики. [9]



Рисунок 6 — Комбинированный метод обнаружения вторжения

На рисунке 6 представлен комбинированный метод обнаружения вторжений, который сопровождается этапами: сбор данных — анализ сетевого трафика, журналов, активности пользователей; проверка по сигнатурам — сравнение с базой известных атак (SQLi, XSS, DDoS и др.); анализ поведения — выявление аномалий (нестандартные запросы, подозрительные соединения); корреляция данных — объединение результатов методов для точного обнаружения; обнаружение внешней угрозы — фильтрация ложных устройств и проявление слабого воздействия; оповещение — передача в IPS для блокировки.

В таблице 1 представлены преимущества и недостатки методов обнаружения вторжений.

Таблица 1 — Сравнительный анализ

Методы обнаружения вторжений (IDS)	Преимущества	Недостатки
NIDS (Network-based IDS)	- Отслеживает трафик всей сети, позволяя выявлять широкомасштабные атаки - Менее нагружает конечные устройства, так как анализ ведется на сетевом уровне - Централизованное управление и настройка правил - Может анализировать несколько сегментов сети одновременно	- Не видит зашифрованный трафик (например, HTTPS) или трафик внутри зашифрованных VPN-туннелей - При высоких скоростях сети может возникать проблема с производительностью - Сложность корректной настройки фильтров и правил обнаружения
HIDS (Host-based IDS)	- Глубокий анализ активности на конкретном устройстве (системные вызовы, логи, изменения файлов) - Точная диагностика инцидентов (можно определить, какие именно процессы были скомпрометированы) - Возможность обнаружения атак, не видимых на сетевом уровне	- Нагрузка на систему, так как анализ ведется локально на хосте - Не защищает всю сеть в целом, а только конкретный узел - Сложнее централизованно управлять большим количеством хостов - Требуется регулярное обновление политик и правил
Сигнатурные (Signature-based)	- Высокая точность при обнаружении известных угроз - Быстрое срабатывание при совпадении с сигнатурами - Относительно простая реализация и настройка (использование готовых баз правил)	- Не выявляет новые, ранее неизвестные атаки (0-day) - Требуется регулярное обновление сигнатур - Может генерировать ложные срабатывания при неверных или слишком общих правилах
Эвристические (Поведенческие)	- Способны обнаруживать новые и неизвестные атаки (0-day), анализируя аномалии и поведение - Менее зависят от базы сигнатур, применяют статистические и поведенческие методы - Позволяют выявлять	- Возможны ложные срабатывания из-за неправильной или недостаточной настройки базовой модели поведения - Требуют значительных вычислительных ресурсов - Более сложная реализация и поддержка,

	сложные, многовекторные атаки	чем у сигнатурных систем
Комбинированные (Signature + Heuristic)	- Сочетают преимущества сигнатурного и поведенческого подходов - Высокая точность при обнаружении известных угроз + способность выявлять новые атаки - Гибкость настройки и адаптации к разным сценариям	- Более высокая сложность конфигурации и сопровождения - Повышенная нагрузка на ресурсы (анализ ведется сразу несколькими методами) - При неправильной настройке возрастает риск ложных срабатываний

Таким образом, IDS у нас может предупреждать о вредоносной активности, но зачастую задача стоит предотвратить вредоносную активность на ранней стадии. В этом может помочь IPS. Методы ее работы относятся к своевременным (превентивным) и проактивным, в отличие от IDS, выполняющей детективные функции. [2] Подобно сетевым IDS (network IDS, NIDS) и IDS на хосте (host IDS, HIDS) существуют сетевые IPS (NIPS) и IPS на хосте (HIPS). Решения NIPS анализируют трафик, прежде чем пропустить его в сеть или подсеть. Решения HIPS анализируют пакеты перед тем, как они поступают в компьютер. [9] Возможность предотвращения атак реализована за счет того, что сетевая IPS, как правило, встраивается «в разрыв» сети и пропускает через себя весь трафик, а также имеет внешний интерфейс, на который приходит трафик и внутренний интерфейс, который пропускает трафик далее, если он признается безопасным. Существует также возможность работы с копией трафика в режиме мониторинга, но тогда мы теряем основной функционал данной системы. [9]

На рисунке 7 представлены основные методы обнаружения вторжений, которые классифицируются по их функциональным возможностям.

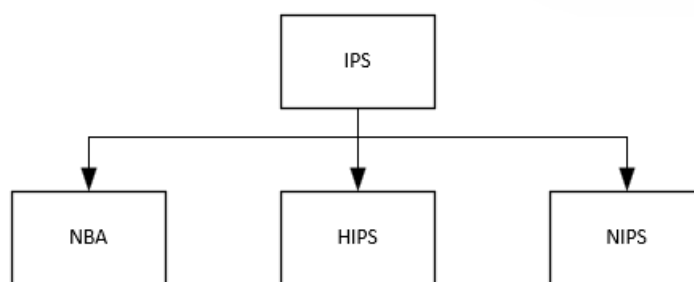


Рисунок 7 — Классификация методов предотвращения вторжений (IPS)

На сегодняшний день существуют два класса IPS - NIPS (Network based Intrusion Prevention System — сетевые системы противодействия вторжениям) и HIPS (Host based Intrusion Prevention System — системы противодействия вторжениям для защиты хост-компьютеров). [10] Глобально IPS можно разделить на те, которые анализируют трафик и сравнивают с известными сигнатурами, и те, которые на основе анализа протоколов ищут нелегитимный трафик, основываясь на базе знаний о найденных ранее уязвимостях. За счет второго класса обеспечивается защита от неизвестного типа атак. Что касается методов реагирования на атаки, то их накопилось большое количество, но из основных можно выделить следующие: блокирование соединения с помощью TCP-пакета с RST-флагом или посредством межсетевого экрана, перенастройка коммуникационного оборудования, а также

блокирование записей пользователей или конкретного хоста в инфраструктуре. [7] Но, кроме двух известных методов, имеется и 3 подход — анализатор поведения сети (Network Behavior Analysis, NBA): анализирует сетевой трафик, идентифицирует нетипичные потоки, например DoS и DDoS- атаки.

- Сетевые IPS (Network-based Intrusion Prevention, NIPS): отслеживают трафик компьютерной сети и блокируют подозрительные потоки данных. NIPS работает, будучи установленным в сетевой трафик или через зеркальные порты. Он выполняет глубокую проверку пакетов (DPI) для анализа данных в реальном времени. Система включает в себя ключевые компоненты, такие как захват пакетов, декодеры протоколов, механизмы сопоставления сигнатур, эвристики, алгоритмы обнаружения аномалий и проверку состояния. Первым шагом является захват пакетов, где он получает необработанные пакеты из сетевого интерфейса. Далее я продолжу описывать, как каждый компонент вносит свой вклад в процесс обнаружения и предотвращения. NIPS перехватывает и анализирует сетевой трафик на лету, захватывая пакеты и выполняя глубокую проверку пакетов (DPI). Она собирает фрагментированные пакеты, проверяет полезную нагрузку и декодирует протоколы, такие как TCP, UDP и SSL/TLS. Обнаружение на основе сигнатур сравнивает пакеты с известными шаблонами атак, в то время как обнаружение аномалий ищет отклонения трафика. Проверка с отслеживанием состояния обеспечивает целостность протокола. NIPS использует аппаратное ускорение для повышения эффективности и интегрируется с SIEM для централизованного ведения журнала событий. Она может блокировать угрозы в режиме реального времени и использует машинное обучение для адаптации и улучшения обнаружения с течением времени.

На рисунке 8 представлена сетевая система предотвращения вторжений.



Рисунок 8 — Сетевая система предотвращения вторжений

NIPS применяет многослойный подход для обнаружения атак на разных уровнях сетевого трафика. Это включает в себя анализ трафика приложений, таких как SQL-инъекции и XSS, а также сетевые атаки, такие как DoS и аномалии протоколов. Система использует правила для обнаружения атак с регулярными обновлениями. В режиме встроенной системы процесс включает захват, обработку, анализ и принятие решений о действиях.

- Хостовые IPS (Host-based Intrusion Prevention, HIPS): резидентные программы, обнаруживающие подозрительную активность на компьютере. HIPS работает, будучи установленным непосредственно на конечном устройстве, и интегрируется с операционной системой для мониторинга всех системных событий. Он выполняет глубокий анализ событий (Deep Inspection of Events) для анализа действий в реальном времени. [11] Система включает в себя ключевые компоненты, такие как захват событий, декодеры системных вызовов, механизмы сопоставления сигнатур, эвристический анализ, алгоритмы обнаружения аномалий и проверку целостности системы. Первым шагом является захват событий, где HIPS регистрирует все обращения к системным ресурсам, файловой системе, реестру и сетевым интерфейсам. Далее рассмотрим, как каждый компонент вносит свой вклад в процесс обнаружения и предотвращения угроз.

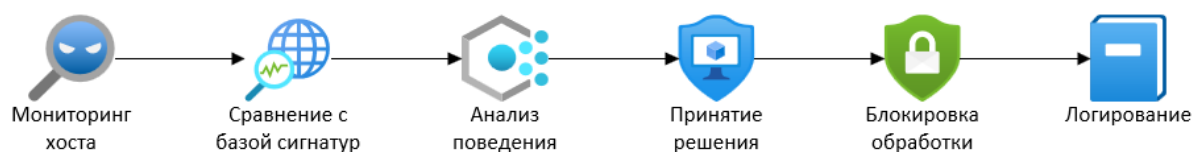


Рисунок 9 — Хостовая система предотвращения вторжений

HIPS перехватывает и анализирует системные события в реальном времени, фиксируя действия процессов, изменения файлов, обращения к критически важным компонентам системы и системные вызовы. Система собирает информацию о действиях приложений и операционной системы, декодирует вызовы и преобразует их в понятный формат для дальнейшего анализа. Обнаружение на основе сигнатур сравнивает эти события с известными шаблонами атак, тогда как эвристический анализ выявляет отклонения в поведении приложений, которые могут указывать на новые, ранее не зарегистрированные угрозы. Контроль целостности и отслеживание состояния помогают убедиться, что системные файлы и настройки не были изменены злоумышленниками.

HIPS использует следующие ключевые компоненты:

- **Захват событий:** Получение необработанных системных вызовов, изменений файлов, действий приложений и сетевых операций.
- **Декодеры системных вызовов:** Преобразование низкоуровневых данных операционной системы в структурированную информацию.
- **Механизмы сопоставления сигнатур:** Сравнение событий с базой данных известных угроз и шаблонов атак.
- **Эвристический анализ:** Применение алгоритмов для обнаружения аномального поведения, даже если конкретная угроза еще не зарегистрирована.
- **Алгоритмы обнаружения аномалий:** Поиск отклонений от нормального поведения системы, что может свидетельствовать о попытках компрометации.
- **Проверка целостности и состояния:** Контроль изменений в критически важных системных файлах и настройках для выявления несанкционированных изменений.

HIPS интегрируется с централизованными системами логирования (например, SIEM) для ведения подробного журнала событий, что позволяет администраторам оперативно получать уведомления и анализировать инциденты. Система может блокировать или ограничивать подозрительные процессы в режиме реального времени, применять методы машинного обучения для адаптации к новым угрозам и постоянно обновлять свои базы сигнатур и эвристические модели.

Применяя многослойный подход, HIPS анализирует события на различных уровнях операционной системы – от действий отдельных приложений до низкоуровневых системных вызовов. Это позволяет обнаруживать как попытки изменения системных файлов и вмешательства в работу служб, так и атаки на уровне приложений, такие как эксплойты или несанкционированное изменение конфигурации. В активном режиме HIPS может немедленно блокировать вредоносные процессы, а в режиме мониторинга – лишь регистрировать события для последующего анализа, что позволяет снизить риск ложных срабатываний.

Таким образом, HIPS представляет собой комплексное решение для защиты конечного устройства, где каждая составляющая, от захвата событий до анализа и принятия решения, играет свою роль в своевременном обнаружении и предотвращении угроз.

• **Анализатор поведения сети (Network Behavior Analysis, NBA):** анализирует сетевой трафик, идентифицирует нетипичные потоки, например DoS и DDoS- атаки. NBA работает, установленный через зеркальные порты или inline, для анализа сетевого трафика в реальном времени. Он осуществляет глубокий анализ пакетов (DPI) и обнаруживает аномалии, сравнивая поведение текущего трафика с установленными базовыми моделями. Система включает следующие ключевые компоненты:

- Захват пакетов – получение необработанных пакетов с сетевого интерфейса, включая сбор фрагментированных данных.
- Декодеры протоколов – распознавание и восстановление протоколов (TCP, UDP, ICMP, HTTP, SSL/TLS и др.).
- Нормализация трафика – приведение данных к единому формату для корректного анализа.
- Механизмы сопоставления сигнатур – сравнение пакетов с известными шаблонами атак.
- Эвристический анализ и алгоритмы обнаружения аномалий – выявление отклонений от нормы с помощью машинного обучения и статистических методов.
- Проверка с отслеживанием состояния – контроль целостности сессий и протоколов.

На рисунке 10 представлен анализатор поведения сети. Первым шагом происходит захват пакетов с сетевого интерфейса, после чего трафик агрегируется, декодируется и нормализуется. Далее система применяет алгоритмы для выявления аномальных паттернов, что позволяет обнаруживать атаки типа DDoS, сканирование портов, ботнет-активность, SQL-инъекции и XSS. Интеграция с SIEM обеспечивает централизованное ведение журнала событий и корреляцию инцидентов. В inline-режиме NBA может блокировать подозрительный трафик, а в пассивном режиме – только мониторить сетевую активность.



Рисунок 10 — Анализатор поведения сети

В таблице 2 представлены преимущества и недостатки методов предотвращения обнаружения.

Таблица 2 — Сравнительный анализ

Методы предотвращения вторжений (IPS)	Преимущества	Недостатки
NIPS (Сетевые IPS)	- Анализ трафика в реальном времени с помощью DPI- Inline -блокировка угроз - Декодирование протоколов (TCP, UDP, SSL/TLS и др.) - Интеграция с SIEM для централизованного ведения журнала	- Высокая ресурсоемкость - Возможны ложные срабатывания - Сложность настройки - Потенциальное увеличение задержек в сети
HIPS (Хостовые IPS)	- Локальная защита конечного устройства - Многоуровневый анализ (сигнатурный, поведенческий, эвристический) - Детальное логирование событий - Гибкая настройка политик безопасности	- Высокая нагрузка на систему - Риск ложных тревог - Сложность конфигурации - Необходимость регулярных обновлений баз данных

NBA (Анализатор поведения сети)	- Глубокий анализ поведения сети в реальном времени - Обнаружение аномалий и неизвестных угроз - DPI и декодирование протоколов - Централизованное логирование через SIEM - Гибкая настройка порогов аномалий	- Возможны ложные срабатывания при неправильной настройке - Требуется обучения базовым моделям трафика - Высокая вычислительная нагрузка при обработке больших объемов данных - Сложность интеграции в инфраструктуру
---------------------------------	---	--

Проведенный анализ различных методов обнаружения и предотвращения вторжений показал, что каждая система имеет свои технические особенности и ограничения. Из этого следует, что:

IDS (система обнаружения вторжений):

- oNIDS (Network-based IDS) – анализирует весь сетевой трафик и обнаруживает атаки до их проникновения в систему.
- oHIDS (Host-based IDS) – мониторит активность на уровне операционной системы и файловой структуры серверов и рабочих станций.
- oКомбинированный метод (сигнатурный + поведенческий анализ) – позволяет обнаруживать как известные, так и новые угрозы.

IPS (система предотвращения вторжений):

- oNIPS (Network-based IPS) – предотвращает вторжения, блокируя вредоносные пакеты на сетевом уровне.
- oHIPS (Host-based IPS) – защищает серверы и рабочие станции от эксплойтов и вредоносных процессов.
- oNBA (Network Behavior Analysis) – анализирует аномальное поведение в сети и выявляет сложные угрозы (ботнеты, APT, скрытые атаки).

Таким образом, после рассмотрения всех факторов, следует выделить платформы, использующие данные методы:

- Cisco Firepower – включает NIPS, NBA и HIPS.
- Darktrace – мощная NBA-система на основе ИИ.
- Suricata – IDS/IPS, анализ пакетов и сетевых атак (NIDS/NIPS).
- Snort – IDS/IPS, мониторинг трафика и предотвращение атак (NIDS/NIPS).
- OSSEC – HIDS, мониторинг целостности файлов и журналов, предотвращение атак.
- Zeek – NIDS, анализ сетевого трафика и обнаружение инцидентов.

Каждая из этих платформ так или иначе решает поставленные задачи, но при этом затрачивает дополнительно: аппаратные, программные и денежные ресурсы; не имеет одного интерфейса, что доставляет неудобство при использовании; не имеет автономности и зависит от других компонентов SOC, а именно от SIEM и SOAR систем. Но чтобы решить эти проблемы, предлагается использовать комплексный подход.

Таблица 3 — Решение поставленных задач

Поставленные задачи:	Решение:
Предотвращение несанкционированного изменения данных о событиях и атаках	Логи и события сохраняются в защищенном хранилище с применением методов хеширования и цифровых подписей для подтверждения их целостности
Защита алгоритмов детекции от	Настройки и алгоритмы детекции в

внешнего вмешательства	Suricata и Zeek защищены через строгие механизмы контроля доступа (например, RBAC) и мониторинг всех изменений
Обеспечение безопасности передачи и хранения данных	Все данные о событиях шифруются, а доступ к ним строго контролируется. Логи могут быть защищены через хранение в зашифрованных базах данных или на защищенных серверах.
Конфиденциальность и целостность данных при интеграции с другими системами	Взаимодействие с другими системами безопасности, такими как SIEM или SOAR, осуществляется через защищенные каналы связи (например, VPN или HTTPS), чтобы исключить утечку или компрометацию данных
Реагирование на угрозы в реальном времени	Система на базе Suricata и Zeek позволяет выявлять угрозы в реальном времени с минимальной задержкой. Это обеспечивается быстрым анализом пакетов и аномалий, а также возможностью автоматического реагирования (например, блокировка трафика)

Комплексный подход решает поставленные задачи, которые представлены в таблице 3. Благодаря такому подходу решаются не только поставленные задачи, но и перекрываются все недостатки, упомянутые ранее при использовании всех компонентов по отдельности, а именно:

- Автономная система, позволяющая работать без поддержки SIEM/SOAR;
- Использование IPS/IDS;
- Использование меньшего количества аппаратных ресурсов;
- Использование меньшего количества программных ресурсов;
- Оптимизация;
- Гибкость в интеграции с SOC;
- Платформы имеют бесплатные решения.

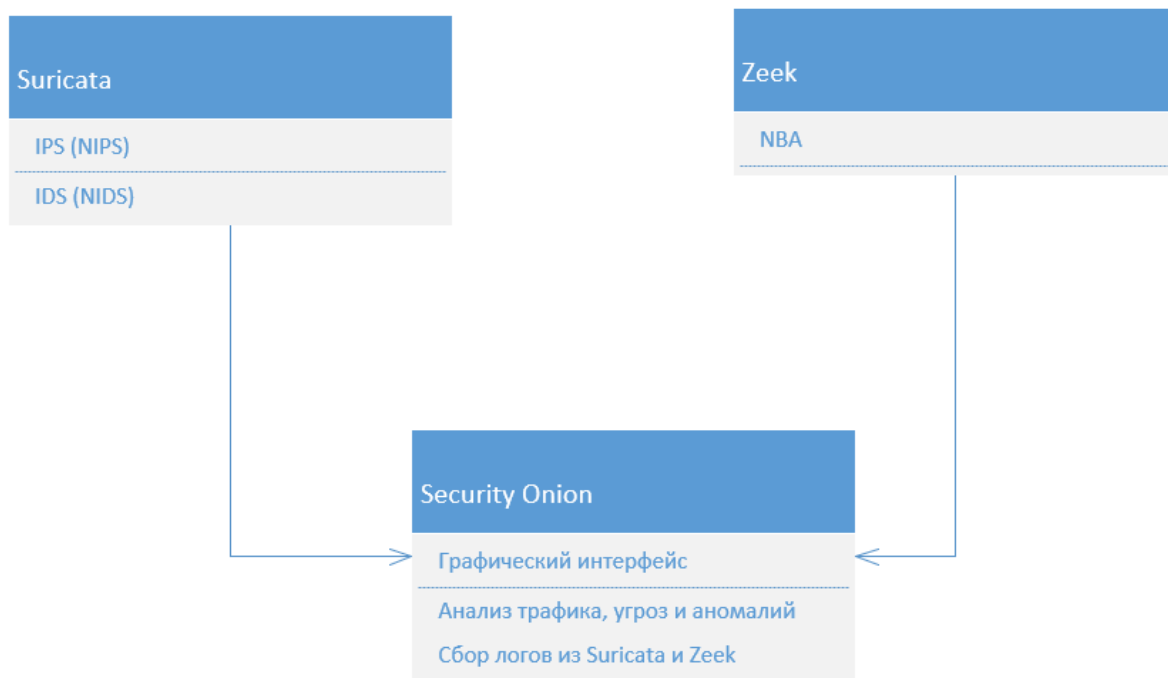


Рисунок 11 — Комплексный подход IPS/IDS

На рисунке 11 представлен комплексный подход IPS/IDS. Система на базе Security Onion, Suricata и Zeek является комплексным решением для мониторинга и защиты сети в реальном времени. Она сочетает в себе возможности IDS/IPS, анализа поведения и сетевого трафика для обнаружения угроз и атак. Эти компоненты работают совместно для того, чтобы обеспечить всестороннюю защиту.

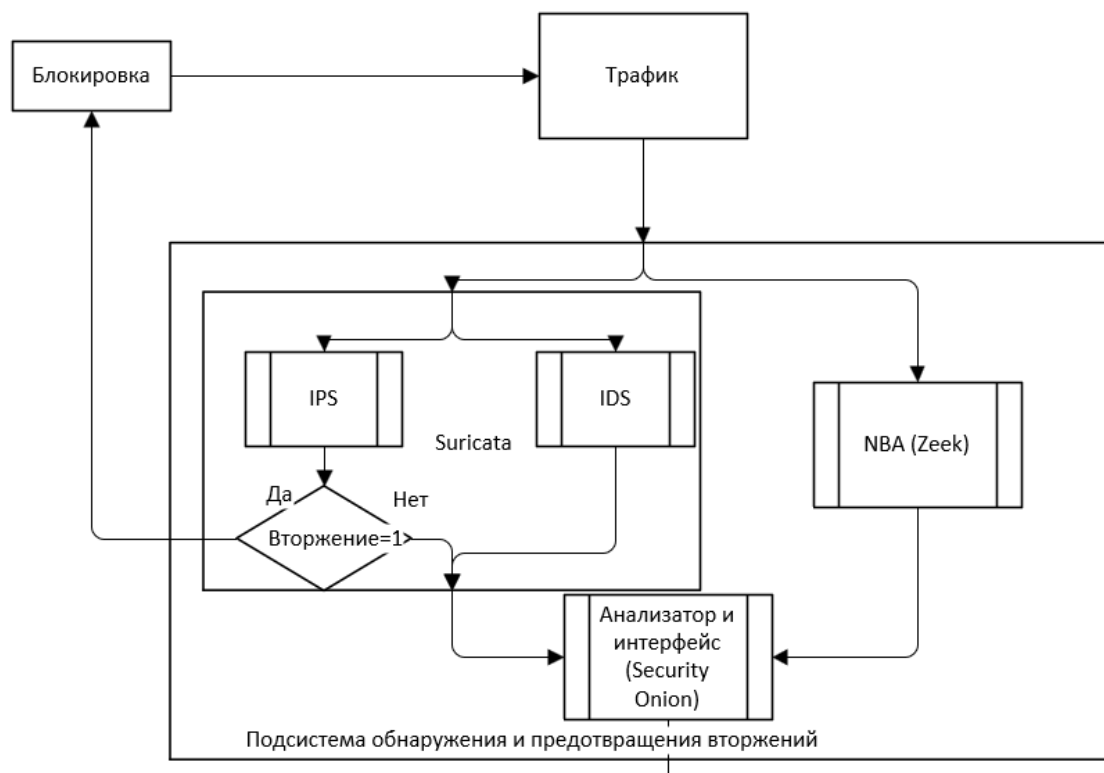


Рисунок 12 — Архитектура комплексного подхода IPS/IDS

На рисунке 12 представлена архитектура комплексного подхода IPS/IDS. На **первом этапе** идет сбор данных о трафике: Suricata просматривает пакеты данных и использует сигнатуры угроз, чтобы идентифицировать известные атаки. Она также может работать в режиме IPS, чтобы блокировать трафик, если обнаружены угрозы. Zeek анализирует трафик на более высоком уровне, чем Suricata. Вместо того чтобы только искать сигнатуры атак, он пытается выявить аномалии в поведении сети. Например: если в сети появляются необычные запросы на разрешение DNS или аномально много попыток подключения к внутренним серверам, Zeek будет генерировать события для дальнейшего анализа. На **втором этапе** идет обработка и хранение логов. Все данные о сетевых событиях, которые собираются Suricata и Zeek, сохраняются в Security Onion. На **третьем этапе** реакция на угрозы: в случае обнаружения угроз, система может сгенерировать уведомления для администраторов безопасности или автоматически предпринять шаги по устранению угрозы: Suricata может заблокировать вредоносный трафик в режиме IPS. Zeek может отслеживать аномальные события и, если настроено, передавать эти события в другие системы для реакции. В случае обнаружения угроз в реальном времени, например, в результате DDoS-атаки или подозрительного поведения на DNS, система может изолировать атакующие устройства или применить политику ограничения доступа. На **четвертом этапе** идет защита и безопасность данных. Важно также защитить сами данные о сетевых событиях. Шифрование логов и трафика на уровне передачи данных (например, через SSL/TLS) помогает предотвратить утечку данных. Целостность данных контролируется через хеширование. Логи и события могут подписываться цифровыми подписями, чтобы гарантировать, что они не были изменены. Защищенные каналы передачи используются для передачи данных между компонентами системы, что исключает их компрометацию.

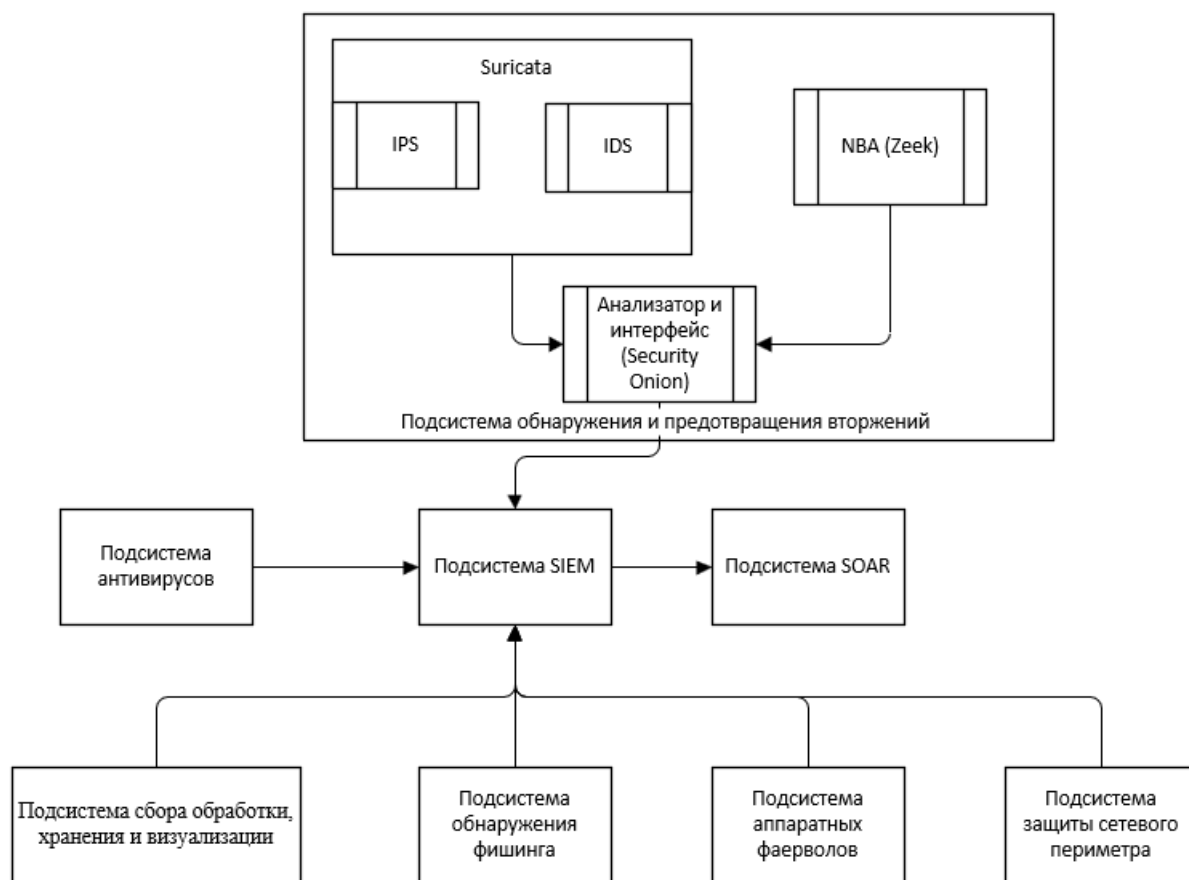


Рисунок 13 — Взаимодействие подсистемы IPS/IDS с SOC

На рисунке 13 представлено взаимодействие подсистемы IPS/IDS с SOC. А именно NBA анализирует поведение трафика (странные запросы, необычные порты, аномальные DNS-запросы). Если находит аномалию, отправляет ее в Security Onion → SIEM → SOAR. Не блокирует трафик, а просто сообщает о подозрительном. Suricata проверяет пакеты по сигнатурам атак (например, SQL-инъекции, DDoS, сканирование портов). Если обнаружена угроза, отправляет событие в Security Onion → SIEM → SOAR. Если атака подтверждена, IPS блокирует ее сразу. Параллельно передает данные в Security Onion → SIEM → SOAR для расследования. Если Zeek нашел аномалию, то это не значит, что атака подтверждена. Дальше анализ идет через SIEM → SOAR. Но если Suricata (IDS) нашла атаку, то в режиме IPS она сразу заблокирует ее.

Защита клиентских сетей с помощью комплексного подхода IPS/IDS:

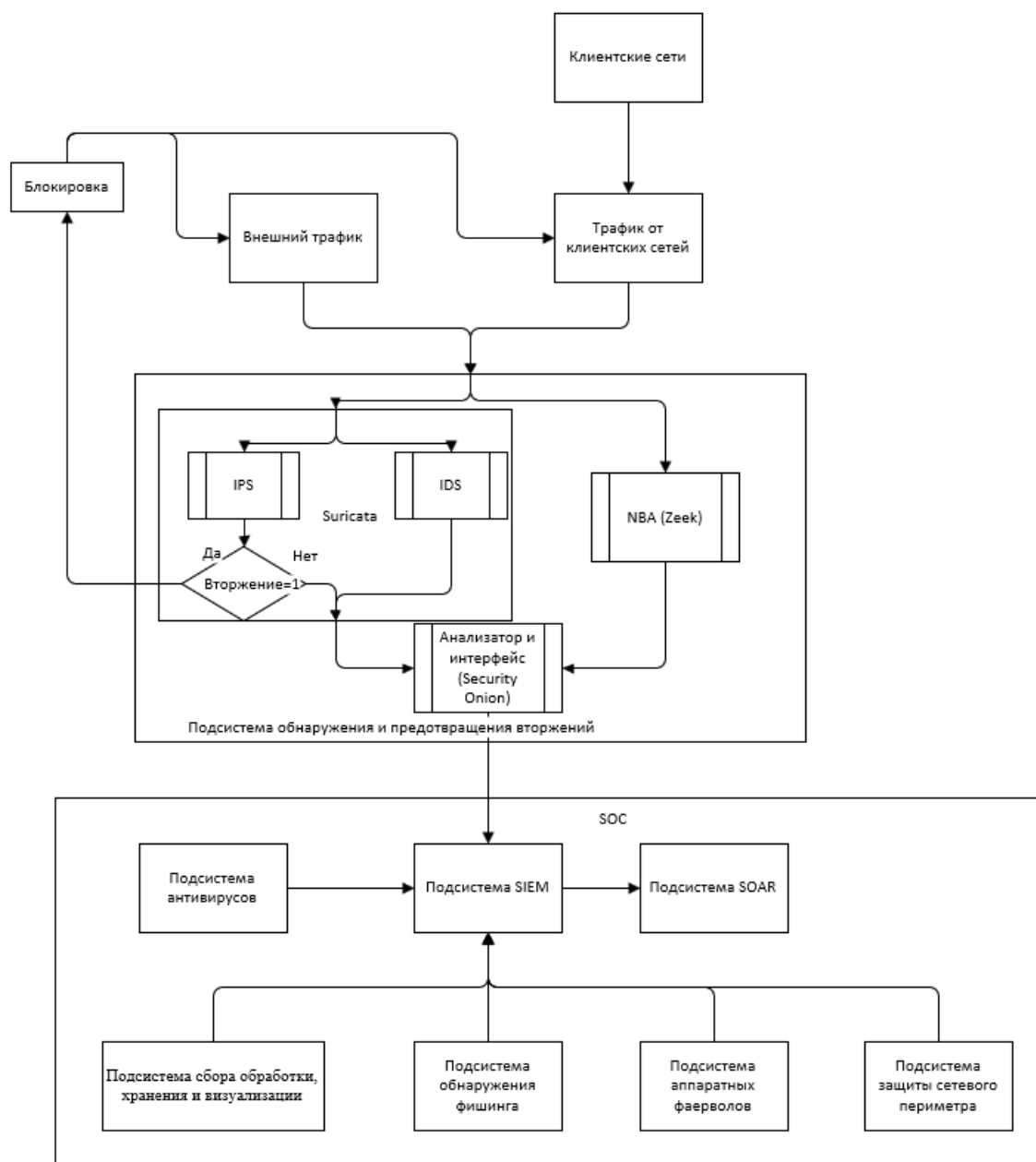


Рисунок 14 — Защита клиентских сетей

На рисунке 14 представлена защита клиентских сетей в рамках **SOC (Security Operations Center)**. Она включает в себя несколько подсистем, совместно работающих, отслеживающих и предотвращающих вторжения.

1. Клиентские сети — источник трафика, который поступает в систему SOC. Трафик от клиентских сетей направляется в SOC для анализа и фильтрации.

2. Клиентский трафик проходит через систему обнаружения и предотвращения вторжений. Она включает: IDS и IPS — реализованы на основе Suricata. IDS анализирует трафик и выявляет потенциальные угрозы. IPS может блокировать лицензионные пакеты. NBA анализирует сетевой трафик и выявляет аномальное поведение. В случае обнаружения угрозы информация направляется в Security Onion, который обеспечивает интерфейс для анализа инцидентов.

3. Вредоносный трафик может быть заблокирован системой IPS. Внешний трафик также анализируется на предмет угрозы.

4. SOC получает данные от систем обнаружения вторжений и передает их в другие подсистемы для обработки: SIEM (Информация о безопасности и управление событиями) – собирает и анализирует события безопасности и SOAR (Security Orchestration, Automation and Response) – автоматизирует реагирование на угрозу.

Дополнительные преимущества SOC:

- Антивирусная защита.
- Систему обнаружения рыбалки.
- Аппаратные фаерволлы.
- Защита периметра сети.

Эти компоненты работают совместно, обеспечивая всестороннюю защиту клиентских сетей. В этом контексте предлагаемая в данной работе подсистема IPS/IDS, основанная на интеграции технологий Suricata, Zeek и Security Onion, эффективно решает поставленные задачи. Объединяя возможности обнаружения, анализа и предотвращения угроз, данное решение не только оптимизирует затраты на инфраструктуру, но и обеспечивает единый интерфейс для мониторинга, что значительно повышает уровень защиты корпоративных сетей. Комплексный подход, включающий анализ аномалий, корреляцию событий и оперативное реагирование, позволяет минимизировать потенциальный ущерб и повысить устойчивость информационных систем перед современными угрозами ИБ.

Таким образом, учитывая масштаб и разнообразие современных угроз ИБ, а также ограничения традиционных систем IPS/IDS, актуальность разработки и внедрения интегрированной подсистемы обнаружения и предотвращения вторжений является бесспорной. Комплексный подход к защите, позволяющий объединить все необходимые инструменты в единую платформу, является ключом к обеспечению безопасности корпоративных сетей в условиях постоянно эволюционирующей среды.

Заключение

В заключение можно обозначить, что для эффективного выявления и предотвращения сетевых атак используются различные системы сетевой безопасности, каждая из которых обладает своими преимуществами в зависимости от задачи. Среди наиболее мощных решений выделяются IDS/IPS-системы, такие как Suricata, и системы анализа сетевого поведения (NBA), например, Zeek, объединенные в единую платформу Security Onion.

Suricata, работая в режиме IDS и IPS, обеспечивает детектирование атак на основе сигнатурного анализа и предотвращение угроз в реальном времени. В то же время Zeek фокусируется на поведенческом анализе трафика, выявляя аномалии и подозрительные шаблоны взаимодействий, которые могут указывать на скрытые атаки. Такое сочетание позволяет обнаруживать как известные угрозы, так и новые атаки, ранее не включенные в базы сигнатур.

Security Onion интегрирует эти инструменты, обеспечивая централизованный сбор, хранение и анализ событий безопасности. Использование Elasticsearch, Logstash и Kibana позволяет визуализировать угрозы, выявлять закономерности и оперативно реагировать на инциденты. Благодаря встроенным механизмам шифрования и защиты логов система предотвращает несанкционированное изменение данных, обеспечивая их целостность и конфиденциальность.

Таким образом, комбинация Security Onion, Suricata и Zeek создает эффективное и экономичное решение для защиты сетей, не требующее дополнительных SIEM- и SOAR-систем. Этот подход обеспечивает оперативное реагирование на угрозы, минимальные задержки при анализе атак и надежную защиту данных, что делает его оптимальным выбором для построения современной системы кибербезопасности.

Литература

1. <https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-v-pervom-polugodii-2024-goda-zafiksirovan-kratnyj-rost-atak-na-sfery-telekoma-i-stroitelstva> (дата обращения 01.15.2025).
2. <https://ics-cert.kaspersky.ru/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/> (дата обращения 01.20.2025).
3. <https://www.kaspersky.ru/about/press-releases/v-nachale-2024-goda-v-apt-atakah-po-vsemu-miru-chashe-vsego-ispolzovalis-uyazvimosti-v-instrumentah-udalyonnogo-dostupa-i-winrar> (дата обращения 01.25.2025).
4. <https://stormwall.pro/resources/blog/ddos-2024-godovoj-otchet#:~:text=%D0%92%D1%81%D0%B5%D0%B3%D0%BE%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B%20StormWall%20%D0%B2%202024,%D0%BC%D0%BE%D1%89%D0%BD%D0%BE%D1%81%D1%82%D1%8C%20%D0%B0%D1%82%D0%B0%D0%BA%20%D0%B2%D1%8B%D1%80%D0%BE%D1%81%D0%BB%D0%B0%20%D0%BD%D0%B0%2053%25.> (дата обращения 01.30.2025).
5. <https://www.cloud4u.ru/blog/ips-and-ids-what-is-it/> (дата обращения 02.05.2025).
6. [https://cloudnetworks.ru/inf-bezopasnost/ids-ips#:~:text=%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D0%BE%D0%B1%D0%BD%D0%B0%D1%80%D1%83%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%B2%D1%82%D0%BE%D1%80%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9%20\(IDS\)%20%D0%BF%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D1%8F%D0%B5%D1%82,%D0%BF%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B0%D0%B5%D1%82%20%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%20%D0%BF%D0%BE%20IP%2D%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D1%83.](https://cloudnetworks.ru/inf-bezopasnost/ids-ips#:~:text=%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D0%BE%D0%B1%D0%BD%D0%B0%D1%80%D1%83%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%B2%D1%82%D0%BE%D1%80%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9%20(IDS)%20%D0%BF%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D1%8F%D0%B5%D1%82,%D0%BF%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B0%D0%B5%D1%82%20%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%20%D0%BF%D0%BE%20IP%2D%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D1%83.) (дата обращения 02.10.2025).
7. <https://habr.com/ru/companies/otus/articles/479584/> (дата обращения 02.15.2025).
8. <https://studfile.net/preview/6211055/page:19/#46> (дата обращения 02.20.2025).
9. <https://cyberleninka.ru/article/n/metody-obnaruzheniya-anomaliy-i-vtorzheniy/viewer> (дата обращения 02.25.2025).
10. <https://lib.itsec.ru/articles2/Oborandteh/tehnologii-hips> (дата обращения 02.30.2025).
11. <https://www.osp.ru/winitpro/2006/04/2578870#:~:text=%D0%A0%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D1%8F%20NIPS%20%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B8%D1%80%D1%83%D1%8E%D1%82%20%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%2C%20%D0%BF%D1%80%D0%B5%D0%B6%D0%B4%D0%B5,%D0%BC%D0%BE%D0%B3%D1%83%D1%82%20%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D1%87%D0%B0%D1%82%D1%8C%D1%81%D1%8F%20%D0%BF%D0%BE%20%D1%82%D0%B8%D0%BF%D1%83%20%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82%D0%B0.> (дата обращения 03.15.2025).

Ю.С. Корякина, jk169@list.ru

Институт машиноведения автоматизации и геомеханики НАН КР

А. А. Каныбекова, kanybekovaa21@gmail.com

Институт информационных технологий КГТУ им. И. Раззакова

ОБЗОР МЕТОДОВ ДЛЯ РЕАЛИЗАЦИИ ПОДСИСТЕМ АНТИВИРУСНОЙ ЗАЩИТЫ В СИСТЕМАХ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Данная работа посвящена разработке подсистем антивирусной защиты в составе Центра мониторинга информационной безопасности (SOC). Основное внимание уделено теоретическим основам антивирусных технологий, а также детальному анализу современных инструментов для защиты от вредоносного программного обеспечения (ПО). В статье проведен обзор функциональных возможностей различных антивирусных решений, их принципов работы и эффективности в условиях современных угроз информационной безопасности (ИБ).

Ключевые слова: SOC; антивирусная защита; информационная безопасность; вредоносное ПО; обнаружение угроз; мониторинг; корпоративная сеть; защита данных; управление инцидентами; интеграция систем; производительность; ложные срабатывания; обновление баз данных; реагирование на угрозы; киберугрозы.

Введение

В современном мире киберугрозы становятся все более изощренными, что требует от Центров мониторинга безопасности (Security Operations Centers, SOC) внедрения эффективных подсистем антивирусной защиты. Актуальность разработки и совершенствования таких подсистем подтверждается рядом реальных инцидентов, продемонстрировавших уязвимость критически важных инфраструктур к вредоносным программам.

Одним из наиболее показательных примеров является атака червя Stuxnet в 2010 году. Этот вредоносный код был специально разработан для саботажа иранской ядерной программы, поражая промышленные системы управления (SCADA) и выводя из строя центрифуги для обогащения урана. Stuxnet использовал несколько уязвимостей нулевого дня и действительные цифровые подписи, что позволяло ему обходить традиционные антивирусные средства и оставаться незамеченным длительное время. Этот инцидент продемонстрировал необходимость разработки специализированных антивирусных решений, способных защищать не только офисные системы, но и промышленные объекты. С тех пор количество обнаруженных уязвимостей нулевого дня продолжает расти. В первой половине 2024 года было выявлено более 1,2 тысячи таких уязвимостей, что на 25% больше по сравнению с аналогичным периодом предыдущего года. Это свидетельствует о сохраняющейся угрозе для промышленных объектов и необходимости постоянного совершенствования мер безопасности.[9]

Еще один значимый случай — распространение программы-вымогателя WannaCry в мае 2017 года. Вирус порастил более 200 000 компьютеров в 150 странах, шифруя данные пользователей и требуя выкуп за их восстановление. Многие организации, включая медицинские учреждения и крупные корпорации, столкнулись с серьезными перебоями в работе из-за недостаточной защиты своих систем. Этот инцидент подчеркнул важность своевременного обновления антивирусных баз и операционных систем, а также необходимости интеграции антивирусных подсистем в общую стратегию кибербезопасности SOC. Несмотря на повышение осведомленности и улучшение мер защиты, программы-вымогатели продолжают представлять серьезную угрозу. Организации по-прежнему сталкиваются с атаками, приводящими к утечкам данных и финансовым потерям.

Эти примеры демонстрируют, что современные кибератаки могут иметь разрушительные последствия для различных сфер деятельности. Поэтому разработка и внедрение эффективных методов реализации подсистем антивирусной защиты в SOC является критически важной задачей для обеспечения информационной безопасности. [1]

В отчете State of Threat Hunting от компании Intrusion определили 5 основных проблем, с которыми сталкиваются центры управления безопасностью (Security Operations Centers, SOC). По мнению участников опроса, самыми серьезными проблемами являются следующие:

- Обнаружение современных угроз
- Нехватка специалистов по безопасности для устранения угроз
- Слишком много времени тратится на ложные срабатывания
- Недостаточная уверенность в том, что средства автоматизации способны выявить все угрозы
- Медленное время реагирования на современные угрозы.



Рисунок 1 — Основные проблемы SOC

1. Недостаточная способность обнаруживать современные угрозы.

Продвинутые угрозы, использующие методы уклонения, способны поразить многие средства обнаружения угроз, имеющиеся в арсенале SOC. В прошлом высокотехнологичные кибератаки были делом рук исключительно организованных киберпреступных групп. Однако сегодня современные кибератаки могут исходить и от более зловещих противников. Появление угроз со стороны иностранных государств радикально изменило ландшафт киберугроз в худшую сторону.

Обладая огромным человеческим, технологическим и финансовым капиталом, эти субъекты способны разворачивать современные постоянные угрозы (APT), в основном для шпионажа и диверсионных кампаний. APT — это глубоко законспирированные группы угроз, которые могут проникать в хорошо защищенные инфраструктуры и сохраняться в них столько, сколько им нужно. Поскольку в отчете Microsoft Digital Defense Report за 2022 год говорится о том, что кибератаки со стороны угрожающих групп иностранных государств стали более изощренными, необходимость обнаружения современных угроз стала еще более важной.

Для того чтобы SOC мог обнаруживать эти высокотехнологичные угрозы, необходимы мощные, но обычно дорогостоящие инструменты обнаружения угроз. Для их использования

также необходим опыт. Без необходимых знаний и опыта ваши средства безопасности не смогут быть оптимизированы для обнаружения АPT и других современных угроз.

2. Нехватка специалистов по безопасности для устранения угроз.

В настоящее время организации сталкиваются с проблемой нехватки специалистов по кибербезопасности, из-за которой в прошлом году не было заполнено 3,5 миллиона вакансий в сфере кибербезопасности. Даже если бы вы хотели нанять сотрудников по кибербезопасности для своего SOC и могли бы себе это позволить, то все равно никого бы не нашлось.

Этот недостаток усугубляется все более широким внедрением таких методов работы, как удаленная работа и использование собственных устройств (BYOD), а также таких технологий, как облачные вычисления, которые не только расширяют поверхность атаки, но и повышают сложность всей ИТ-среды.

Нехватку специалистов по кибербезопасности можно компенсировать автоматизацией. А именно средствами или продуктами безопасности, способными функционировать без постоянного наблюдения сотрудников.

3. Слишком много времени тратится на предупреждения о ложных срабатываниях.

Растущая сложность и разнообразие угроз в сочетании с постоянным шквалом маркетинговых кампаний от поставщиков средств защиты подтолкнули организации к накоплению арсенала инструментов безопасности. Сейчас у организаций в среднем 76 инструментов, многие из которых генерируют массу предупреждений, и значительная часть из них является ложными срабатываниями.

Одна только сортировка, обогащение, обработка и анализ легитимных оповещений уже может оказаться непосильной задачей. Куда больше, если вам приходится иметь дело еще и с ложными срабатываниями? Ложноположительные оповещения могут помешать вам проанализировать и выявить текущую кибератаку. Они могут ввести аналитиков в заблуждение, заставив их пуститься в бесполезную, отнимающую много ресурсов погоню.

Кроме того, слишком большое количество ложных срабатываний может сделать аналитиков SOC более восприимчивыми к усталости от оповещений. Когда наступает усталость от оповещений, сотрудники службы безопасности начинают испытывать разочарование, стресс и склонность к выгоранию. Это, в свою очередь, может заставить сотрудников отключить оповещения (что позволит большему количеству угроз избежать обнаружения) или, что еще хуже, покинуть вашу организацию в поисках более благоприятных условий работы.

4. Отсутствие уверенности в том, что средства автоматизации способны отразить все угрозы.

Автоматизация имеет решающее значение для операций безопасности. Автоматизируя рабочие процессы, аналитики SOC могут сократить время, затрачиваемое на выполнение определенных функций, таких как анализ угроз, мониторинг угроз, обнаружение угроз, анализ угроз, реагирование на инциденты и так далее. Это помогает повысить скорость и эффективность выполнения задач. Таким образом, автоматизация в какой-то мере помогает решить проблему нехватки кадров в сфере кибербезопасности.

Но есть одна загвоздка. Автоматизация сильно зависит от надежности отдельных компонентов. Например, если данные, используемые для обнаружения угроз, состоят в основном из ложных срабатываний, это только введет в заблуждение и запутает аналитиков угроз. Аналогичным образом, если вы слишком полагаетесь на автоматизированный процесс, а он генерирует множество ложноотрицательных результатов, вы просто приобретете ложное чувство безопасности.

5. Медленное время реагирования на современные угрозы.

Ложные срабатывания и отсутствие надежных автоматизированных средств обнаружения угроз не позволяют сотрудникам службы безопасности оперативно реагировать на современные угрозы. Но чем дольше киберугроза остается незамеченной, тем больше у нее возможностей нанести значительный ущерб вашей организации.

К сожалению, в прошлогоднем отчете Cost of a Data Breach среднее время обнаружения и локализации утечки данных составило 277 дней. Это слишком долго. В том же отчете говорится, что средняя экономия, которую вы получаете при локализации утечки за 200 дней или менее, составляет 1,12 млн долларов. Очевидно, что если вы сможете сократить время на обнаружение угрозы и реагирование на нее, то получите значительную экономию средств. И наоборот, более длительное время обнаружения и реагирования приводит к увеличению затрат.

В рамках проекта «Разработки подсистемы антивирусной защиты SOC» можно выделить следующие возможные решения проблем, упомянутые выше.[2]

- 1) Обнаружение современных угроз.
 - Внедрение поведенческого анализа (Behavior-Based Detection) для выявления аномальной активности.
 - Интеграция с Threat Intelligence платформами для получения актуальных индикаторов компрометации (IoC).
- 2) Нехватка специалистов по безопасности для устранения угроз.
 - Интеграция антивирусной системы с SOC SIEM для централизованного анализа событий.
 - Использование автоматических патчей и обновлений антивирусных баз данных без участия специалистов.
- 3) Слишком много времени тратится на ложные срабатывания.
 - Использование интеллектуальных фильтров для уменьшения false positives.
 - Настройка поведенческого анализа с учетом специфики организации, чтобы сократить количество ложных тревог.
- 4) Недостаточная уверенность в автоматизированных средствах обнаружения.
 - Разработка гибридной модели обнаружения, объединяющей сигнатурный, эвристический и поведенческий анализ.
 - Интеграция с Threat Intelligence для обогащения данных о новых атаках.
- 5) Медленное время реагирования на современные угрозы.
 - Автоматическая изоляция зараженных узлов и устранение вредоносного ПО без вмешательства оператора.
 - Настройка реактивных политик для автоматической блокировки вредоносных процессов и подключения зараженных систем к карантинной сети.

Для поэтапного решения вышеперечисленных проблематик необходимо ознакомиться с методами антивирусной защиты SOC. Методы делятся на несколько этапов:

Классические сигнатурные методы

Обнаружение на основе сигнатур остается основополагающим подходом к антивирусной защите в Центрах управления безопасностью (SOC). Этот метод основан на сравнении файлов, кода и процессов с заранее определенной базой данных известных сигнатур вредоносного ПО, что обеспечивает быстрое выявление и устранение ранее распознанных угроз. Благодаря своей эффективности и низким вычислительным затратам сигнатурное обнаружение остается важным компонентом современных стратегий кибербезопасности.

Однако его основное ограничение заключается в неспособности обнаружить угрозы «нулевого дня» и полиморфные вредоносные программы, которые часто изменяют свой код, чтобы обойти распознавание по сигнатурам. Для решения этих проблем современные SOC используют эвристический анализ, поведенческий мониторинг и модели машинного

обучения в дополнение к традиционным методам, основанным на сигнатурах. Кроме того, платформы Threat Intelligence позволяют в режиме реального времени обновлять и коррелировать возникающие индикаторы угроз, повышая точность и адаптивность механизмов обнаружения.

На рисунке 2 поэтапно описан традиционный антивирусный процесс, основанный на сигнатурном методе:

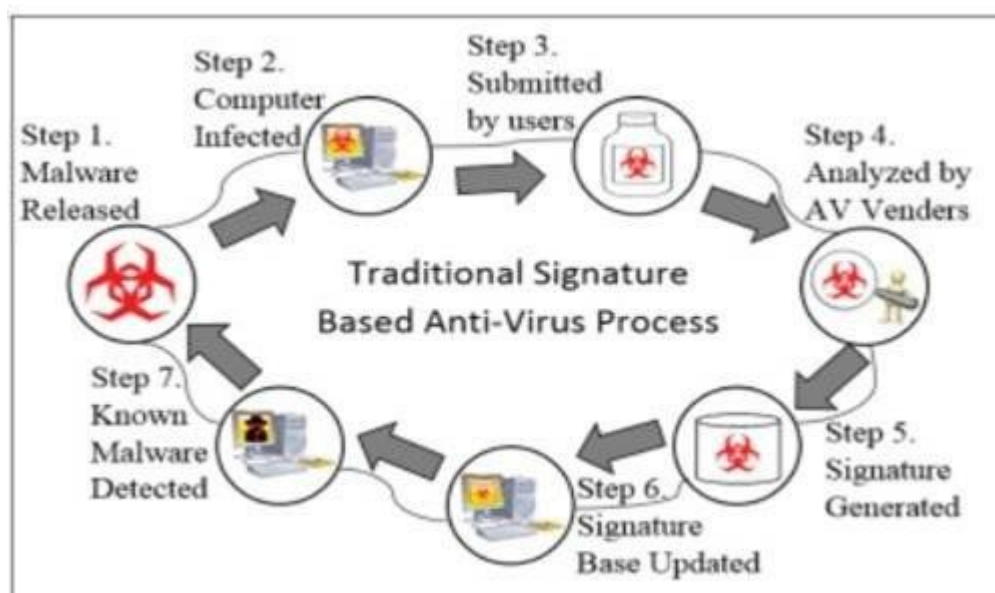


Рисунок 2 — Традиционный антивирусный процесс, основанный на сигнатурах

1. Выпуск вредоносного ПО.
2. Заражение компьютера.
3. Отправка пользователями.
4. Анализ антивирусными вендорами.
5. Генерация сигнатуры.
6. Обновление базы сигнатур.
7. Обнаружение известного вредоносного ПО.

Эвристические методы

Эвристические методы антивирусной защиты представляют собой проактивный подход к выявлению потенциальных угроз путем анализа поведения, структуры и атрибутов файлов, а не только на основе известных сигнатур. В Центрах управления безопасностью (SOC) эти методы необходимы для обнаружения новых, неизвестных или модифицированных вредоносных программ, которые системы на основе сигнатур могут пропустить. Эвристика предполагает оценку файлов на наличие подозрительных шаблонов, таких как необычное выполнение кода или аномальное поведение системы, что может указывать на наличие вредоносной активности.

В отличие от традиционного обнаружения на основе сигнатур, которое требует предварительного знания об угрозе, эвристические методы позволяют выявлять атаки «нулевого дня» и полиморфные вредоносные программы, которые эволюционируют, чтобы обойти статические средства защиты. Эвристика поведения расширяет эти возможности, динамически анализируя действия программ в режиме реального времени, что позволяет выявлять подозрительное поведение, например попытки несанкционированного доступа или изменения файловой системы до того, как будет нанесен значительный ущерб.

Хотя эвристические методы позволяют повысить эффективность обнаружения, они могут генерировать ложные срабатывания, поскольку основаны на распознавании образов, что может привести к тому, что вполне безопасное ПО будет считаться вредоносным. Чтобы смягчить эту проблему, SOC объединяют эвристический анализ с машинным обучением, анализом угроз и контекстным анализом, повышая точность и снижая нагрузку на аналитиков безопасности. Такой многоуровневый подход позволяет SOC оперативно реагировать на возникающие угрозы, повышая общий уровень защиты от сложных кибератак.

Далее представлена схема на рисунке 3 – поэтапный принцип работы эвристического метода антивирусной защиты:

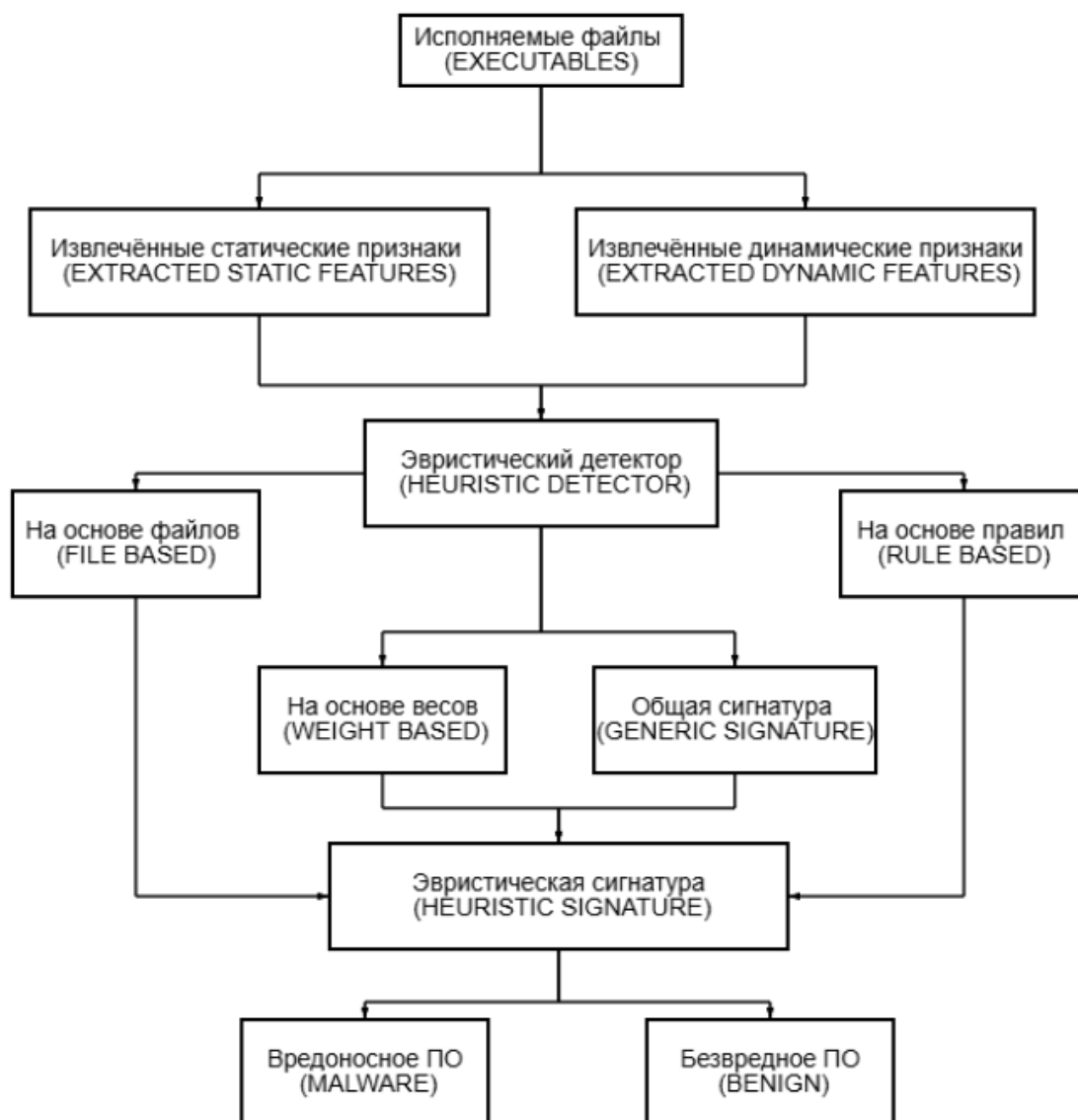


Рисунок 3 — Принцип работы эвристического метода

Поведенческий анализ и мониторинг активности

Поведенческий анализ и мониторинг играют важную роль в антивирусной защите в Центрах управления безопасностью (SOC), позволяя обнаруживать угрозы, которые традиционные методы, основанные на сигнатурах, могут пропустить. В отличие от статических методов обнаружения поведенческий анализ фокусируется на действиях и шаблонах, демонстрируемых программами во время выполнения. Этот метод позволяет антивирусным системам в режиме реального времени выявлять «вредоносное поведение», например, несанкционированные модификации файлов, сетевую активность или попытки

использования уязвимостей системы, даже в ранее неизвестных вариантах вредоносного ПО.

Наблюдая и анализируя такое поведение, SOC могут обнаруживать «атаки нулевого дня», полиморфные вредоносные программы и передовые постоянные угрозы (APT), которые постоянно совершенствуются, чтобы обойти обычные средства защиты. Поведенческий мониторинг обычно осуществляется с помощью инструментов Endpoint Detection and Response (EDR), которые непрерывно отслеживают конечные точки и выдают предупреждения о подозрительных действиях, способствуя тем самым быстрому обнаружению угроз и реагированию на них.

Несмотря на высокую эффективность, поведенческий анализ может давать ложные срабатывания из-за сложности различения легитимных и вредоносных действий. Чтобы смягчить эту проблему, SOC часто объединяют поведенческий мониторинг с контекстным анализом, машинным обучением и анализом угроз для повышения точности обнаружения. Такой подход повышает способность SOC реагировать на сложные кибератаки, обеспечивая критически важный уровень защиты от возникающих и развивающихся угроз.

Далее на рисунке 4 представлен поэтапный принцип работы поведенческого анализа и мониторинга активности:



Рисунок 4 — Принцип работы метода

Комплексный подход: сочетание различных методов

Комплексный подход к антивирусной защите в Центрах управления безопасностью (SOC) предполагает интеграцию нескольких механизмов обнаружения и защиты для обеспечения многоуровневой защиты от широкого спектра киберугроз. Эта стратегия сочетает традиционное обнаружение на основе сигнатур, эвристический анализ, поведенческий мониторинг и анализ сетевого трафика, создавая многогранную систему защиты, которая повышает способность выявлять и устранять как известные, так и неизвестные угрозы.

Обнаружение на основе сигнатур обеспечивает высокую точность обнаружения ранее идентифицированных вредоносных программ, в то время как эвристические методы позволяют выявлять новые или модифицированные угрозы на основе подозрительных шаблонов кода. Поведенческий анализ, в свою очередь, отслеживает активность в реальном времени, чтобы обнаружить аномальные действия, указывающие на потенциальную угрозу, например несанкционированный доступ или манипуляции с системой. Анализ сетевого трафика направлен на выявление аномальных схем обмена данными, которые могут свидетельствовать об утечке данных, деятельности ботнетов или боковом перемещении злоумышленников.

Комбинируя эти методы, SOC могут эффективно устранить недостатки каждого из них в отдельности. Системы, основанные на сигнатурах, усиливаются эвристикой и поведенческим анализом, которые позволяют обнаружить ранее неизвестные или полиморфные вредоносные программы. Аналогичным образом анализ сетевого трафика обеспечивает дополнительный уровень видимости для обнаружения угроз, пытающихся обойти защиту конечных точек.

Далее представлена таблица 1 – роли и взаимодействия различных методов в комплексном подходе.

Таблица 1 – Комплексный подход

Комплексный метод				
Сигнатурный метод	Эвристический метод	Поведенческий анализ	Мониторинг и анализ логов	Взаимодействие всех методов
Проверка файлов по базе известных вирусов	Анализирует структуру и код файлов	Мониторинг активности программ и процессов	Собирает события с разных систем (EDR, Firewall, IDS)	Сигнатуры → быстрый отклик на известные угрозы
Быстрое обнаружение известных угроз	Определяет подозрительные команды и поведение	Выявляет аномалии (подозрительные изменения в ОС, сети, файлах)	Коррелирует данные и выявляет комплексные атаки	Эвристика → находит скрытые угрозы
Не выявляет новые и мутирующие угрозы	Возможны ложные срабатывания	Требует мощных ресурсов и глубокой аналитики	Сложно настроить и требует SOC-аналитиков	Поведение → выявляет атаки нулевого дня

Технологии и инструменты для реализации подсистемы антивирусной защиты

Инструменты для данной цели рассматриваются open-source и коммерческие решения. Необходимо проанализировать эти категории и выявить наиболее подходящий.

Open-source решения или решения с открытым исходным кодом. В качестве рассматриваемого примера берутся такие инструменты, как ClamAV и Zeek. Эти решения широко применяются в условиях, когда первоочередное внимание уделяется экономической эффективности, гибкости и общинному развитию.

Основное преимущество открытых решений — их бесплатная доступность, устранение лицензионных сборов для частных лиц или организаций с ограниченным бюджетом. Этот аспект экономии средств особенно привлекателен для небольших предприятий или научно-исследовательских учреждений.

Открытые решения, такие как ClamAV и Zeek, предоставляют обширные возможности для настройки, позволяя пользователям изменять программное обеспечение в соответствии с конкретными потребностями безопасности. Организации могут изменять конфигурации, интегрировать с другими инструментами и даже разрабатывать пользовательские сценарии обнаружения, предлагая уровень гибкости, не всегда доступный при коммерческих решениях. [4]

Далее в виде таблицы представлены основные преимущества и недостатки обоих решений. [5]

Таблица 2 — Преимущества и недостатки ClamAV

Преимущества	Недостатки
Кросс-платформенность: Поддерживает различные операционные системы, включая Unix-подобные системы, OpenVMS, Microsoft Windows и macOS	Ограниченная эффективность обнаружения: в тестах 2008 года ClamAV показал низкие результаты в обнаружении вредоносных программ и rootkit-ов. В исследовании 2022 года его эффективность составила 59,94% при обнаружении распространенных типов вредоносного ПО
Открытый исходный код: распространяется под лицензией GNU General Public License, что позволяет пользователям и разработчикам вносить изменения и улучшения	Отсутствие официального графического интерфейса: ClamAV не предоставляет собственного графического интерфейса, что может затруднить использование для некоторых пользователей. Однако существуют сторонние GUI, такие как KlamAv для KDE и ClamTk для GNOME
Интеграция с почтовыми серверами: предоставляет интерфейс Milter для Sendmail и поддерживает большинство форматов почтовых файлов, что делает его полезным для сканирования электронной почты на наличие вирусов	Ограниченная защита в реальном времени: хотя ClamAV предоставляет возможности сканирования "на лету", его защита в реальном времени может быть не такой эффективной, как у некоторых коммерческих антивирусных решений
Поддержка различных форматов файлов: может анализировать сжатые файлы (RAR, ZIP, Gzip, Bzip2), форматы OLE2, Cabinet, CHM и другие, а также файлы форматов HTML, RTF и PDF	Зависимость от обновлений базы данных: эффективность ClamAV зависит от регулярного обновления вирусных баз данных. В некоторых регионах доступ к обновлениям может быть ограничен, что снижает эффективность защиты

Таблица 3 — Преимущества и недостатки Zeek

Преимущества	Недостатки
Глубокий анализ сетевого трафика: Zeek осуществляет детальный анализ различных протоколов и взаимодействий, что позволяет выявлять подозрительные или вредоносные действия в сети	Сложность настройки и использования: для эффективного использования Zeek требуются определенные знания и навыки в области сетевой безопасности и администрирования, что может быть сложным для неопытных пользователей

Гибкость и расширяемость: Zeek предоставляет возможности для написания пользовательских скриптов, что позволяет адаптировать его под конкретные нужды и сценарии использования	Ответственность за обслуживание: пользователь несет ответственность за обслуживание и обновление сервера с установленным Zeek, а также за резервное копирование данных
Интеграция с другими инструментами: Zeek может интегрироваться с различными системами управления событиями информационной безопасности (SIEM), такими как Splunk или Elastic, для дополнительного анализа данных	Потребление ресурсов: при высоких нагрузках или в больших сетях Zeek может потреблять значительные системные ресурсы, что требует соответствующей инфраструктуры для обеспечения производительности
Открытый исходный код: Zeek является бесплатным проектом с открытым исходным кодом, что позволяет сообществу вносить вклад в его развитие и адаптировать под специфические требования	Отсутствие графического интерфейса: Zeek не предоставляет собственного графического интерфейса, что может затруднить его использование для некоторых пользователей. Однако существуют сторонние решения для визуализации данных.

В целом данные инструменты не представляют собой антивирусной системы по отдельности, но при объединении и комплексном использовании получается эффективное решение [6]. Однако даже вместе они не смогут полностью закрыть основные проблемы, которые рассматриваются в данной статье. Поэтому необходимо разобрать и коммерческие решения. В качестве примера будут рассмотрены антивирусные системы ESET и Kaspersky.

ESET и Kaspersky — два известных коммерческих антивирусных решения, обеспечивающих комплексную защиту от широкого спектра киберугроз. Оба решения обладают уникальными возможностями.

И ESET, и Kaspersky используют передовые многоуровневые механизмы защиты, включая сигнатурное обнаружение, эвристику, поведенческий анализ и облачную аналитику угроз, обеспечивая надежную защиту от известных и возникающих угроз, таких как вредоносное ПО, программы-вымогатели и атаки «нулевого дня». Далее также, в виде таблицы, будут представлены их преимущества и недостатки.

Таблица 4 —Преимущества и недостатки антивирусной системы ESET

Преимущества	Недостатки
Минимальное влияние на системные ресурсы: ESET известен своей эффективностью и низким потреблением ресурсов, что обеспечивает быструю работу системы	Ограниченный функционал в базовой версии: базовая версия ESET NOD32 предоставляет только основные функции защиты без дополнительных возможностей
Высокая скорость сканирования: быстрое обнаружение и удаление угроз благодаря оптимизированному механизму сканирования	Отсутствие некоторых дополнительных функций: в сравнении с конкурентами ESET может не предоставлять такие функции, как VPN

	или менеджер паролей
Регулярные обновления: частые обновления вирусных баз данных обеспечивают защиту от новых угроз	Ограниченная защита от фишинга: защита от фишинговых сайтов может быть менее эффективной по сравнению с другими антивирусами
Кросс-платформенность: поддержка различных операционных систем, включая Windows, macOS и Linux	Интерфейс пользователя: интерфейс может показаться сложным для неопытных пользователей [7]

Таблица 5 —Преимущества и недостатки Kaspersky

Преимущества	Недостатки
Высокий уровень обнаружения угроз: Kaspersky регулярно получает высокие оценки в независимых тестах за эффективность обнаружения и блокировки вредоносных программ	Высокое потребление системных ресурсов: некоторые пользователи отмечают, что Kaspersky может замедлять работу системы из-за значительного потребления ресурсов
Широкий набор функций: кроме базовой антивирусной защиты, Kaspersky предлагает дополнительные функции, такие как родительский контроль, защита онлайн-платежей и VPN	Потенциальные конфликты с другим ПО: Kaspersky может быть несовместим с некоторыми другими антивирусными и антишпионскими программами, что может вызвать конфликты при совместном использовании
Регулярные обновления и поддержка: частые обновления вирусных баз и оперативная техническая поддержка обеспечивают актуальность защиты	Ограниченная совместимость с некоторыми системами: Kaspersky может быть несовместим с определенными операционными системами или устаревшим оборудованием, что ограничивает его использование на некоторых устройствах
Интуитивно понятный интерфейс: пользовательский интерфейс Kaspersky разработан для удобства и простоты использования, что облегчает настройку и управление защитой	Потенциальные риски безопасности: в некоторых странах возникали опасения по поводу безопасности использования продуктов Kaspersky из-за предполагаемых связей с российскими государственными структурами, что привело к ограничениям на использование их ПО в государственных учреждениях
Интеграция с другими системами безопасности: Kaspersky предоставляет возможности для интеграции с другими решениями безопасности, что позволяет создавать комплексные системы защиты	Стоимость лицензии: полная версия Kaspersky с расширенным функционалом может быть дороже по сравнению с некоторыми конкурентами, что может быть существенным фактором для домашних пользователей и небольших предприятий.[8]

Ведущие антивирусные решения, такие как ESET и Kaspersky, используют гибридные модели обнаружения, сочетающие сканирование на основе сигнатур с поведенческим анализом и облачными системами репутации. Такой многоуровневый подход обеспечивает надежную защиту как от известных, так и от развивающихся киберугроз, укрепляя позиции организаций по защите от сложных векторов атак. Но при выборе антивирусного решения для защиты **Security Operations Center (SOC)** необходимо учитывать множество факторов. Основываясь на сравнении коммерческих решений, можно составить следующую таблицу:

Таблица 6 — Сравнение и анализ коммерческих решений

Проблема в SOC	Решение ESET	Решение Kaspersky
Обнаружение современных угроз	ESET обеспечивает обнаружение современных угроз благодаря регулярным обновлениям и проактивной защите	Kaspersky предоставляет расширенные функции для обнаружения сложных угроз, включая APT, с помощью команды GReAT.
Нехватка специалистов по безопасности для устранения угроз	ESET предлагает автоматизацию некоторых процессов, но может потребоваться дополнительная настройка и мониторинг	Kaspersky предоставляет комплексные решения с автоматизацией и аналитикой, что снижает нагрузку на специалистов SOC
Слишком много времени тратится на ложные срабатывания	ESET стремится минимизировать ложные срабатывания, но в некоторых случаях может потребоваться ручная проверка	Kaspersky известен низким уровнем ложных срабатываний благодаря точным алгоритмам обнаружения и регулярным обновлениям
Недостаточная уверенность в том, что средства автоматизации способны выявить все угрозы	ESET предоставляет базовые средства автоматизации, но для полной уверенности может потребоваться дополнительная настройка	Kaspersky предлагает расширенные средства автоматизации и аналитики, повышающие уверенность в обнаружении всех угроз
Медленное время реагирования на современные угрозы	ESET обеспечивает быстрое реагирование на известные угрозы, но сложные атаки могут требовать дополнительного вмешательства	Kaspersky предоставляет оперативное реагирование на современные угрозы благодаря постоянному мониторингу и обновлениям

Вследствие всего можно отметить, что данные решения подходят для минимизации основных проблем SOC, однако все же имеют свои нюансы. Таким образом, для эффективного функционирования Центра мониторинга информационной безопасности (SOC) рекомендуется использовать комбинацию решений от ESET и Kaspersky. ESET обеспечивает минимальное влияние на системные ресурсы и высокую скорость сканирования, что полезно для поддержания производительности системы. Kaspersky, в

свою очередь, предоставляет расширенные функции обнаружения сложных угроз и автоматизации, что снижает нагрузку на специалистов по безопасности и повышает эффективность реагирования на инциденты. Совместное использование этих антивирусных систем позволит компенсировать недостатки каждой из них.

Для ясности приведена схема взаимодействия подсистемы с SOC.

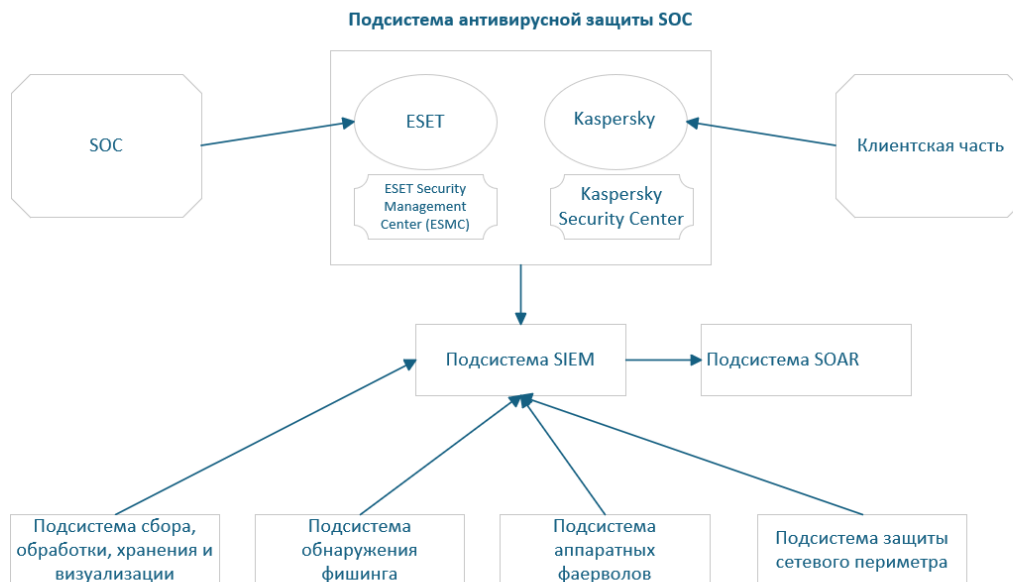


Рисунок 5—Структурная схема подсистемы антивирусной защиты

Принцип работы антивирусной защиты.

Все антивирусные решения (ESET и Kaspersky) управляются через свои серверы (ESMC и Kaspersky Security Center). Серверы управления интегрированы с SIEM для централизованного мониторинга. Антивирусные клиенты на рабочих станциях и серверах передают данные о состоянии системы и инцидентах на соответствующие серверы управления. Далее серверы управления передают сводные данные в SIEM-систему SOC. После чего все события поступают в SIEM, где выполняется корреляция и анализ, и интегрируются с SOAR для автоматического реагирования (блокировка, создание тикетов).

На следующей схеме более детально обрисован принцип защиты клиентской части и SOC (рис. 6):

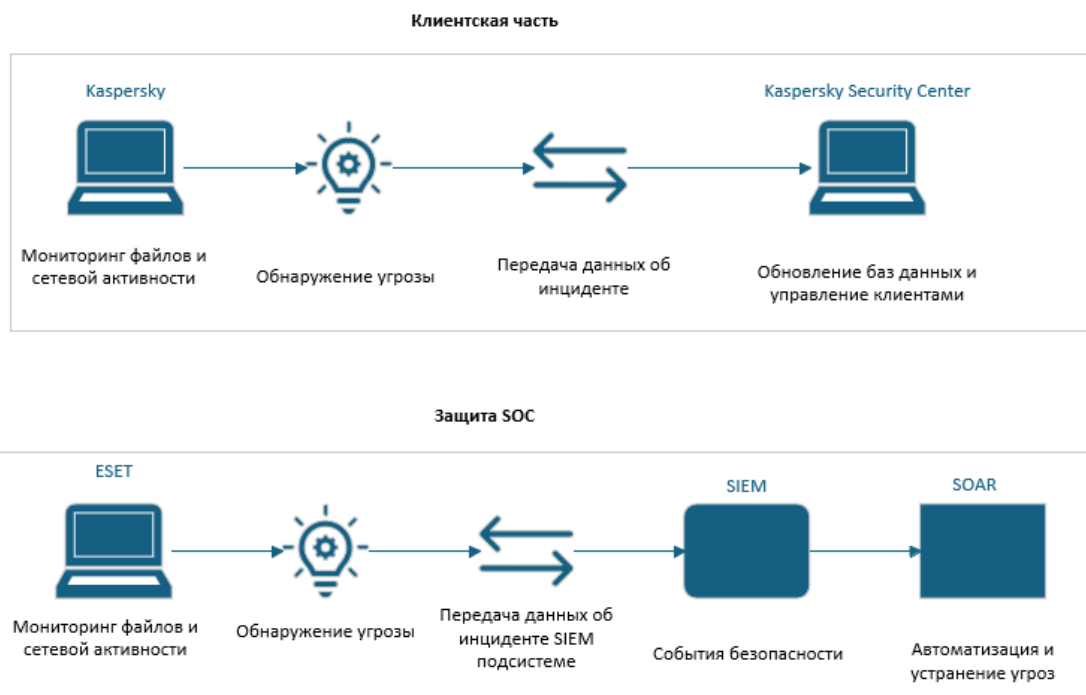


Рисунок 6—Логическая схема защиты клиентских устройств

Клиентская часть: агенты проводят мониторинг файловой системы, сетевой активности и процессов на наличие вредоносного ПО. При обнаружении угрозы агент передает данные на сервер управления (Kaspersky Security Center). После чего сервер управления обновляет базы данных угроз и отправляет данные в SIEM-систему для централизованного мониторинга.

Защита SOC: SIEM анализирует события, выполняет корреляцию с другими источниками данных и создает предупреждения о потенциальных угрозах. При подтверждении угрозы данные передаются в SOAR-систему для автоматического реагирования (например, изоляция зараженного устройства или блокировка вредоносного процесса).

Резервный вариант

В добавок ко всему прочему в разработке подсистемы антивирусной защиты учитывается фактор непредвиденных ситуаций, т.е. существует резервный вариант. Если основные инструменты (ESET, Kaspersky) перестанут функционировать, на замену им будет использоваться комплекс из решений с открытым исходным кодом (к примеру, ClamAV и Zeek) (рис. 7):



Рисунок 7— Структурная схема подсистемы антивирусной защиты с использованием резервной подсистемы

В ходе проведенного исследования были рассмотрены основные проблемы, влияющие на эффективность работы подсистем антивирусной защиты в SOC: недостаточная способность обнаружения современных угроз, нехватка специалистов по кибербезопасности, высокая частота ложных срабатываний, ограниченные возможности автоматизации и медленное время реагирования на инциденты. Для решения этих проблем были изучены различные методы антивирусной защиты, включая сигнатурные и эвристические подходы, поведенческий анализ и комплексные гибридные модели.

Проведенное сравнение бесплатных и коммерческих решений показало, что наиболее оптимальной стратегией является использование комплекса антивирусных систем на основе сочетания продуктов ESET и Kaspersky. Эти решения обеспечивают высокую точность обнаружения и автоматизацию реагирования, минимизируя ложные срабатывания и снижая нагрузку на специалистов. В качестве резервного варианта предложено использовать бесплатные решения с открытым исходным кодом, такие как ClamAV и Zeek, которые могут обеспечить базовый уровень защиты при отказе коммерческих продуктов.

Таким образом, комплексный подход к антивирусной защите SOC с использованием как коммерческих, так и бесплатных решений позволяет значительно повысить устойчивость к киберугрозам, сократить время реагирования на инциденты и обеспечить надежное функционирование инфраструктуры информационной безопасности.

Литература

1. <https://itta.info/ru/10-samyx-vpechatlyayushhix-kiberatak-v-istorii/> (дата обращения 05.01.2025 г.).
2. <https://www.intrusion.com/blog/the-biggest-challenges-for-socs/> (дата обращения 15.01.2025 г.).
3. https://www.anti-malware.ru/proactive_test_2010 (дата обращения 20.01.2025 г.).
4. <https://www.clamav.net/> <https://zeek.org/> (дата обращения 30.01.2025 г.).
5. <https://en.wikipedia.org/wiki/ClamAV> (дата обращения 05.02.2025 г.).
6. <https://itshaman.ru/it-programmy-dlya-linux/4866/zeek-analiz-setevogo-trafika-s-otkrytym-iskhodnym-kodom-dlya-monitoringa-bezopasnosti> (дата обращения 10.02.2025 г.).
7. <https://www.eset.com> (дата обращения 15.02.2025 г.).

8. <https://www.kaspersky.com> (дата обращения 20.02.2025 г.).
9. <https://securitymedia.org/news/kolichestvo-uyazvimostey-nulevogo-dnya-vozroslo-na-chetvert-v-pervoy-pолоvine-2024> (дата обращения 05.03.2025 г.).

УДК 004.056.5

С.В. Корякин, srgkoryakin1@gmail.com

Институт информационных технологий КГТУ им. И.Раззакова

Институт машиноведения автоматизации и геомеханики НАН КР

С.У. Сураналиева, suranalieva.salta18@gmail.com

Институт информационных технологий КГТУ им. И. Раззакова

ОБЗОР МЕТОДОВ РЕАЛИЗАЦИИ ПОДСИСТЕМ РАССЛЕДОВАНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SOAR (SECURITY ORCHESTRATION AUTOMATION AND RESPONSE) В СОСТАВЕ СИСТЕМ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В данной работе рассмотрены ключевые проблемы, с которыми сталкиваются центры мониторинга информационной безопасности (SOC), включая высокую нагрузку на персонал, длительное время реагирования на инциденты и разрозненность используемых инструментов и систем. Для решения этих проблем были проанализированы различные подходы и методы, направленные на повышение эффективности работы SOC. В результате исследования было установлено, что наиболее оптимальным решением является внедрение платформы SOAR (Security Orchestration, Automation, and Response), так как она позволяет устранить все выявленные недостатки.

Исследования, проведенные Palo Alto Networks и Rapid7, подтверждают эффективность SOAR: по их данным, применение данной технологии может сократить время реагирования на инциденты до 70% и повысить производительность аналитиков на 35%. SOAR повышает эффективность SOC за счет автоматизации рутинных задач, что позволяет аналитикам сосредоточиться на поиске угроз и расследовании инцидентов. Кроме того, SOAR оптимизирует рабочие процессы, предоставляя централизованную панель управления операциями по обеспечению безопасности, что сокращает время на поиск информации и принятие решений.

Помимо повышения оперативности реагирования, SOAR способствует сокращению затрат за счет автоматизации процессов, уменьшения необходимости в сверхурочной работе и предотвращения утечек данных, приводящих к крупным финансовым потерям. Дополнительным преимуществом является улучшение общей безопасности за счет глубокой интеграции аналитики угроз и автоматизированного реагирования. Таким образом, SOAR является стратегически важным инструментом для современных SOC, обеспечивая их эффективную и бесперебойную работу.

Ключевые слова: оркестровка безопасности, автоматизация, реагирование, центр управления безопасностью, кибербезопасность, реагирование на инциденты, управление угрозами.

Введение

В условиях стремительного роста числа кибератак и их усложнения центры операций безопасности (SOC) сталкиваются с рядом серьезных вызовов. Киберпреступники разрабатывают все более сложные методы атак, а компании вынуждены инвестировать значительные ресурсы в защиту своей цифровой инфраструктуры. Однако традиционные подходы к управлению инцидентами оказываются недостаточно эффективными, в связи с чем организации сталкиваются с такими большими проблемами как: 1) высокая нагрузка на персонал; 2) длительное время реагирования на инциденты; 3) разрозненность инструментов и систем. Эти проблемы необходимо решить самым оптимальным методом, так как при таких условиях ухудшается эффективность и увеличивается перегруженность самого SOC и персонала.

Высокая нагрузка на персонал

Современные SOC ежедневно обрабатывают огромное количество оповещений и событий безопасности. Специалисты вынуждены вручную анализировать и классифицировать множество инцидентов, значительная часть которых оказывается ложными срабатываниями. Это приводит к усталости, когнитивной перегрузке и выгоранию сотрудников. В результате критически важные угрозы могут оставаться без внимания, а общая эффективность работы SOC снижается. Нехватка квалифицированных специалистов еще больше усугубляет ситуацию, так как SOC испытывают кадровый дефицит, а существующие сотрудники вынуждены работать в условиях постоянного стресса.

Длительное время реагирования на инциденты

При отсутствии автоматизированных процессов расследование и устранение инцидентов требует значительных временных затрат. Вручную анализировать инциденты, собирать дополнительную информацию, сопоставлять данные из различных источников и разрабатывать стратегию реагирования — все это занимает слишком много времени. В условиях постоянных кибератак и растущего числа угроз такая задержка может привести к серьезным финансовым и репутационным потерям для организации. Время, затраченное на реагирование, напрямую влияет на эффективность SOC: чем быстрее инцидент выявляется и устраняется, тем меньше ущерб от атаки.

Разрозненность инструментов и систем

SOC используют широкий спектр решений для мониторинга, анализа и реагирования на угрозы, включая SIEM, EDR, NDR, TIP и множество других инструментов. Однако отсутствие интеграции между ними приводит к разрозненности данных, необходимости ручного анализа информации из разных источников и, как следствие, к снижению скорости и точности реагирования. Без централизованного управления инцидентами SOC теряют возможность эффективно координировать свои действия и оптимально использовать ресурсы.

Из этих проблем наиболее критичной является высокая нагрузка на персонал, так как именно она становится причиной замедления всех процессов в SOC, увеличивает риск ошибок и снижает общую эффективность работы специалистов.

Принято считать, что для решения таких ключевых проблем, как высокая нагрузка на персонал, длительное время реагирования и разрозненность инструментов, используются следующие методы, направленные на повышение эффективности работы SOC: 1) улучшение процессов и оптимизация рабочих процедур; 2) автоматизированное управление угрозами без SOAR; 3) автоматизация с использованием скриптов и RPA; 4) искусственный интеллект и машинное обучение; 5) интеграция Threat Intelligence (TI); 6) интеграция SOAR системы (Security Orchestration, Automation and Response).

Улучшение процессов и оптимизация рабочих процедур

Один из способов оптимизации работы SOC заключается в улучшении процессов и рабочих процедур. Внедрение стандартов реагирования на инциденты, таких как Incident Response Playbooks, позволяет создать четко регламентированные процедуры обработки инцидентов. Использование международных стандартов, таких как NIST CSF, MITRE ATT&CK и SANS Incident Response, помогает унифицировать работу SOC, а также улучшает процессы эскалации инцидентов для более быстрого реагирования. Кроме того, подход Fusion SOC, который предполагает интеграцию SOC с другими подразделениями безопасности, такими как IT, DevOps, Risk Management и Threat Intelligence, способствует лучшей координации действий и повышению качества расследований за счет обмена данными между различными отделами. Однако этот метод требует значительных временных и кадровых ресурсов для внедрения и постоянного контроля. Кроме того, сложность регламентации может привести к затруднениям в адаптации сотрудников к новым процессам.

Автоматизированное управление угрозами без SOAR

Другой подход – автоматизированное управление угрозами без использования SOAR. Оптимизация правил корреляции в SIEM за счет настройки более точных алгоритмов снижает количество ложных срабатываний. Применение поведенческой аналитики позволяет выявлять аномалии в данных, а использование технологий XDR (Extended Detection and Response) объединяет данные из различных источников, таких как EDR, NDR и облачные решения, что повышает точность обнаружения угроз. Также автоматизируется выявление сложных атак, которые не фиксируются отдельными инструментами. Однако этот метод имеет свои ограничения: он требует значительных усилий на настройку и сопровождение, а

также оставляет необходимость в ручном реагировании. Без полноценной автоматизации многие угрозы по-прежнему будут требовать вмешательства аналитиков, что увеличивает нагрузку на персонал и может замедлять реакцию на инциденты.

Автоматизация с использованием скриптов и RPA

Автоматизация с использованием скриптов и RPA (Robotic Process Automation) представляет собой еще один способ оптимизации работы SOC. Использование скриптов на Python, PowerShell и Bash позволяет автоматизировать рутинные задачи, такие как блокировка IP-адресов, выгрузка логов и изоляция хостов. Внедрение RPA для SOC помогает автоматизировать обработку типовых инцидентов, генерацию отчетов и сбор данных. Однако скрипты требуют ручного обслуживания, сложно масштабируются и не обеспечивают централизованного управления процессами. Кроме того, при изменении инфраструктуры SOC может потребоваться постоянное обновление скриптов, что создает дополнительную нагрузку на команду.

Искусственный интеллект и машинное обучение

Еще одним современным решением является применение искусственного интеллекта и машинного обучения. Использование моделей машинного обучения позволяет предсказывать угрозы, анализируя прошлые инциденты и выявляя характерные паттерны атак. Это также способствует автоматическому снижению уровня ложных срабатываний. Технология User and Entity Behavior Analytics (UEBA) помогает обнаруживать аномальное поведение пользователей и устройств внутри сети, что позволяет выявлять сложные атаки, такие как компрометация учетных записей. Однако для эффективного функционирования подобных моделей требуются большие объемы данных и длительное обучение, а также настройка алгоритмов. Возможны ложные срабатывания, что требует дополнительного контроля со стороны аналитиков и увеличивает нагрузку на персонал.

Интеграция Threat Intelligence (TI)

Интеграция Threat Intelligence (TI) также играет важную роль в повышении эффективности SOC. Использование платформ Threat Intelligence позволяет автоматически обновлять индикаторы компрометации (IoC) и проводить корреляцию с SIEM. Это значительно ускоряет выявление атак на основе глобальных данных о киберугрозах. Однако данный метод требует ручного анализа полученной информации и ее применения в защитных механизмах SOC. Автоматическое обновление данных TI может привести к перегрузке системы большим количеством ложных индикаторов, что может затруднить эффективное реагирование на реальные угрозы.

Интеграция SOAR системы (Security Orchestration, Automation and Response)

SOAR объединяет преимущества всех вышеперечисленных методов, обеспечивая автоматизацию реагирования на инциденты, интеграцию различных систем и сокращение нагрузки на персонал. Он позволяет автоматизировать анализ инцидентов, исключая рутинные задачи для аналитиков, и использовать плейбуки для быстрого реагирования без участия человека. Глубокая интеграция с SIEM, XDR, EDR, NDR и TIP создает централизованное управление инцидентами, а автоматическая корреляция данных снижает время анализа угроз. Дополнительным преимуществом SOAR является фильтрация ложных срабатываний, автоматизированная эскалация только важных инцидентов и уменьшение риска человеческих ошибок. Хотя SOAR требует первоначальной настройки и разработки сценариев реагирования, его преимущества в значительном снижении нагрузки на персонал и ускорении процесса реагирования делают его оптимальным выбором для современных SOC. Инвестиции в SOAR окупаются за счет повышения эффективности работы аналитиков, минимизации времени реагирования и улучшения общего уровня безопасности организации.

Несмотря на многообразие методов, используемых для решения указанных задач, наиболее эффективным подходом считается внедрение системы SOAR, которая

обеспечивает автоматизацию рутинных процессов, снижение числа ложных срабатываний и оперативную, координированную реакцию на инциденты.

Основы SOAR

SOAR (Security Orchestration Automation and Response) — это класс решений, предназначенный для оркестрации, координации и централизованного управления СЗИ, а также системами безопасности. SOAR обогащает данными инциденты ИБ, получаемые из SIEM системы или иных источников, обрабатывает инциденты ИБ и автоматизирует механизм реагирования, т.е. предлагает готовые инструкции реагирования на инциденты [1].

Что напрямую относится к работе SOAR [1]:

- Оркестровка (Orchestration) — интеграция технологий и инструментов для принятия решений на основе информации об уровне риска и состоянии системы.

- Автоматизация (Automation) — для замещения задач, которые ранее выполняли «вручную», автоматическими действиями со стороны системы по заготовленным сценариям (playbooks).

- Управление киберинцидентами и совместная деятельность (Incident management and collaboration) — сквозной подход по работе с «назначением приоритета», «протоколированием действий» и «принятием решений на основе политик компании».

- Формирование отчетов (Dashboards and reporting) — визуализация информации по ключевым метрикам и составление сводок для трех типов сотрудников — аналитиков, руководителей SOC и директоров по ИБ (Chief Information Security Officer, CISO).

На рисунке 1 представлена функциональная структурная схема SOAR системы.



Рисунок 1 — Основные функции SOAR-систем

SOAR обладают функциональностью, позволяющей сократить время расследования значимых инцидентов в сфере ИБ [2]. Это, в частности:

- интеграция технологий / инструментов, необходимых для принятия решений на основе отчетов о состоянии системы безопасности и оценки возможного уровня риска;
- автоматизация процессов;
- управление инцидентами с использованием сквозного подхода (определение приоритетов, регистрация всех действий по реагированию на инциденты, принятие решений в соответствии с политикой компании);
- визуализация данных, связанных с ключевыми показателями, отчетами сотрудников и документацией.

Огромным преимуществом использования SOAR является то, что они позволяют автоматизировать процессы управления инцидентами, начиная с назначения приоритетов и заканчивая, собственно, реагированием. Благодаря заранее созданным планам действий («плейбукам») система способна самостоятельно среагировать на то или иное происшествие, тем самым повысив точность и скорость выполнения операций. При этом следует обратить внимание на то, что автоматизация процессов реагирования при всей своей сложности и витиеватости должна быть гибкой и предусматривать включение человека в рабочий процесс, а иногда и вообще останавливаться, ожидая решения аналитика.

За счет оркестровки SOAR обеспечивает скоординированный автоматический ответ на выявленную несанкционированную активность. Конечно, полностью решить проблему в автоматическом режиме не всегда представляется возможным, но SOAR должна быть способна переводить средства защиты в более строгие режимы работы, своевременно начинать сбор подробной статистики либо ограничивать операции, которые потенциально могут привести к утечкам данных. Кроме того, важно, чтобы SOAR умела обрабатывать и сортировать оповещения, поступающие от внешних систем (например, SIEM), вести детальный журнал, быть источником для создания базы знаний о возможных атаках, предоставлять данные для аналитики и расследования инцидентов и к тому же была готова к интеграции с платформами киберразведки (Threat Intelligence).

SOAR может интегрировать данные об угрозах, поступающие из разных источников. Это достигается с помощью трех основных модулей, перечисленных далее [2]:

- Модуль реагирования на инциденты в области безопасности (Security Incident Response, SIR) облегчает процесс выявления происшествий. Он также импортирует информацию из других применяемых решений и настраивает ИБ-процедуры.

- Для приоритизации уязвимостей продукты класса SOAR используют модуль Response Vulnerability. Он помогает определить степень подверженности бизнес-систем угрозам.

- Модуль анализа угроз на основе данных киберразведки предназначен для выявления признаков возможной компрометации, а также для углубленного отслеживания угроз. Его основное преимущество заключается в том, что он поддерживает различные стандарты, применяемые для обмена данными об угрозах. Кроме того, этот модуль позволяет добавлять пользовательские источники и обмениваться информацией с внешними системами.

SOAR не заменяет, а дополняет другие системы, помогая автоматизировать рутинные задачи. В таблице 1 представлены все вышеперечисленные методы, их преимущества и недостатки.

Таблица 1 — Сравнение методов для решения ключевых проблем

Метод	Какие проблемы решает	Какие проблемы остаются нерешенными
Улучшение процессов и оптимизация рабочих процедур	+ Ускоряет реагирование за счет стандартизации процедур + Повышает координацию между командами + Облегчает расследование инцидентов	- Требуется значительных кадровых и временных ресурсов для внедрения и поддержки - Процессы все еще зависят от человеческого фактора
Автоматизированное управление угрозами без SOAR	+ Снижает количество ложных срабатываний в SIEM + Улучшает обнаружение сложных атак благодаря XDR и поведенческому анализу	- Не автоматизирует реагирование на угрозы, требуется ручное вмешательство - Высокая сложность настройки и поддержки
Автоматизация с использованием скриптов и RPA	+ Автоматизирует рутинные задачи (блокировка IP, сбор логов, изоляция хостов) + Ускоряет выполнение типовых операций	- Скрипты требуют ручного обслуживания и доработки - Сложно масштабироваться и централизуется

Искусственный интеллект и машинное обучение	+ Обнаруживает аномальное поведение и сложные угрозы + Снижает число ложных срабатываний + Анализирует прошлые атаки для предсказания новых	- Требуется больших объемов данных и ресурсов на обучение моделей - Возможны ложные срабатывания
Интеграция Threat Intelligence (TI)	+ Позволяет быстро выявлять угрозы на основе глобальных данных + Автоматически обновляет индикаторы компрометации (IoC)	- Требуется ручного анализа и адаптации данных под конкретные сценарии SOC
SOAR (Security Orchestration, Automation and Response)	+ Автоматизирует реагирование на инциденты и исключает рутинные задачи для аналитиков + Объединяет SIEM, XDR, EDR, NDR и TIP в единую систему + Использует плейбуки для быстрого реагирования + Оптимизирует работу аналитиков, снижает количество ложных срабатываний + Улучшает продуктивность SOC и снижает риск человеческих ошибок	- Требуется времени и ресурсов на настройку интеграций и плейбуков - Может быть сложным в развертывании

При сравнении всех перечисленных методов самым оптимальным выходит применение SOAR системы в SOC. Этому может быть подтверждением растущее количество исследований.

Исследование, проведенное американской компанией, оказывающей услуги в области информационной безопасности Palo Alto Networks, показало, что SOAR может сократить время реагирования на инциденты до 70% [8]. Другое исследование, проведенное Rapid7, показало, что SOAR может повысить производительность аналитиков на 35% [9].

SOAR повышает эффективность SOC несколькими способами. Во-первых, SOAR может автоматизировать задачи, которые в настоящее время выполняются аналитиками вручную. Это позволяет аналитикам сосредоточиться на более сложных задачах, таких как поиск угроз и расследование инцидентов.

Во-вторых, SOAR может оптимизировать рабочие процессы, предоставляя единую панель для управления операциями по обеспечению безопасности. Это может помочь сократить время, необходимое аналитикам для поиска нужной информации и принятия мер в случае инцидентов.

Кроме того, помимо решения ключевых проблем, SOAR также может помочь сократить расходы за счет автоматизации задач, снижения необходимости в сверхурочной работе и улучшения общего состояния безопасности, что может помочь предотвратить утечки данных. Внедрение SOAR системы позволяет улучшить общее состояние безопасности, обеспечивая лучшую видимость событий безопасности, автоматизируя реагирование на инциденты и улучшая интеграцию аналитики угроз.

Согласно исследованиям одной из ведущих компаний в сфере кибербезопасности — Palo Alto Networks SOAR, система может автоматизировать такие задачи, как сортировка, расследование и устранение инцидентов, что может помочь сократить время реагирования на инциденты до 70% [8]. На рисунке 2 представлено процентное соотношение времени реагирования на инциденты до и после внедрения SOAR.

Влияние SOAR на время реагирования на инциденты.

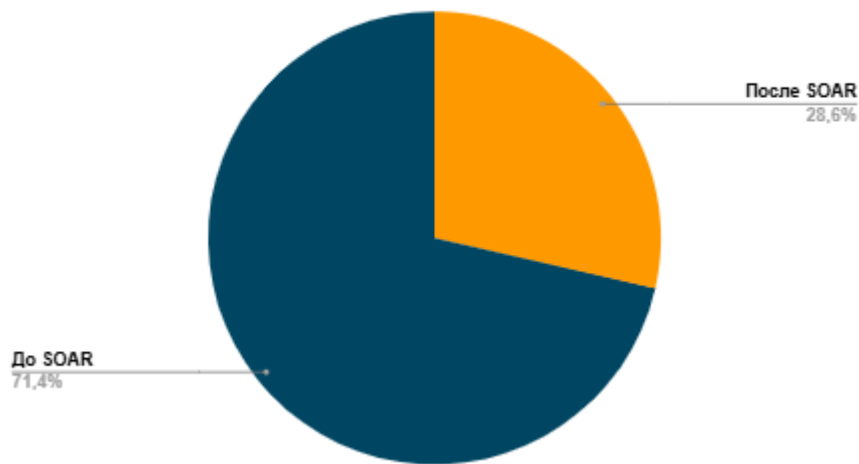


Рисунок 2 — Время реагирования на инциденты

Автоматизируя задачи и оптимизируя рабочие процессы, SOAR может освободить аналитиков, чтобы они могли сосредоточиться на более сложных задачах, повышая их производительность до 35% [9]. На рисунке 3 представлено процентное соотношение влияния SOAR на эффективность SOC до и после внедрения SOAR.

Влияние SOAR на эффективность SOC

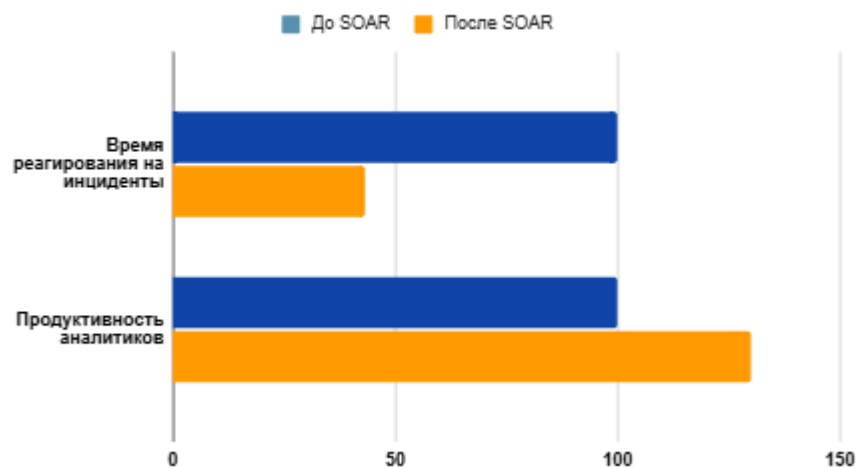


Рисунок 3 — Производительность аналитиков

SOAR может помочь снизить затраты за счет автоматизации задач, сокращения необходимости сверхурочной работы и улучшения общего состояния безопасности, что может помочь предотвратить дорогостоящие утечки данных [10]. На рисунке 4 представлено процентное соотношение затрат до и после внедрения SOAR.

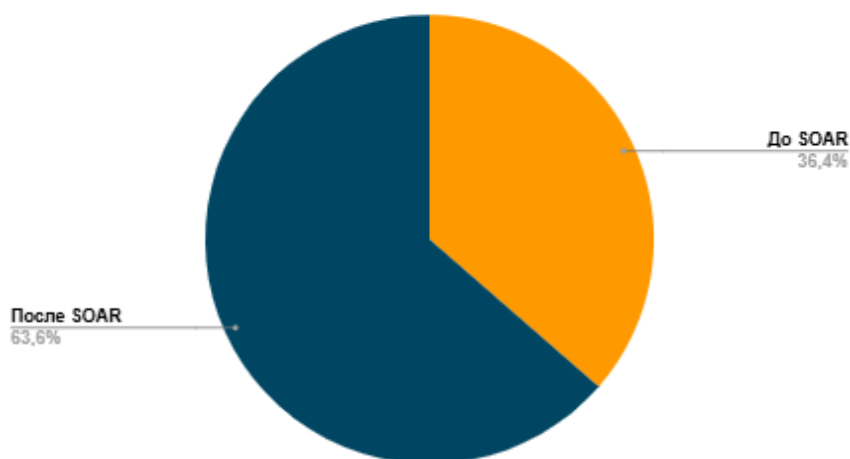
Влияние SOAR на снижение затрат

Рисунок 4 — Снижение затрат

Заключение

Таким образом, в настоящее время компании внедряют SOAR как решение, обеспечивающее максимальную эффективность работы информационных систем, учитывая представленные выше преимущества. Данный подход подтверждается реальными примерами успешного применения.

Например, известная финансовая организация внедрила SOAR в свою ИТ-инфраструктуру в 2018 году [11]. Перед внедрением SOAR команде SOC требовалась помощь, чтобы справиться с объемом предупреждений и инцидентов, что приводило к задержке реагирования на инциденты и повышенному риску компрометации [12].

После внедрения SOAR в организации сократилось время реагирования на инциденты на 60 %, а производительность аналитиков выросла на 20 % [11]. SOAR помог автоматизировать многие ручные задачи, которые ранее выполняли аналитики, такие как сортировка и расследование инцидентов [11]. Это позволило аналитикам сосредоточиться на более сложных задачах, таких как поиск угроз и управление уязвимостями [11].

Организация также значительно улучшила общий уровень безопасности [11]. SOAR предоставил команде SOC единую панель для управления всеми данными безопасности, что упростило выявление угроз и реагирование на них [11].

В ходе проведенного исследования были рассмотрены ключевые проблемы, влияющие на эффективность работы SOC: высокая нагрузка на персонал, длительное время реагирования на инциденты и разрозненность используемых инструментов и систем. Для решения этих проблем были изучены различные подходы, включая оптимизацию процессов, применение автоматизированных решений без SOAR, использование скриптов и RPA, внедрение технологий машинного обучения и интеграцию Threat Intelligence. Каждый из этих методов обладает своими преимуществами и ограничениями, позволяя частично устранить выявленные проблемы.

Однако самым оптимальным решением для повышения эффективности SOC является внедрение SOAR. Данный подход объединяет преимущества всех рассмотренных методов, обеспечивая автоматизацию реагирования на инциденты, интеграцию различных систем и снижение нагрузки на персонал. Использование SOAR позволяет значительно ускорить процесс обработки инцидентов, минимизировать рутинные задачи для аналитиков, улучшить корреляцию данных между различными решениями (SIEM, XDR, EDR, NDR, TIP) и повысить общую продуктивность SOC.

Таким образом, применение SOAR становится стратегически важным шагом для организаций, стремящихся к повышению уровня кибербезопасности, снижению времени реакции на угрозы и оптимизации работы аналитиков. Несмотря на необходимость

первоначальной настройки и поддержки системы, долгосрочные выгоды от использования SOAR значительно превосходят вложенные ресурсы, делая его наиболее эффективным решением для современных центров мониторинга информационной безопасности.

Литература

1. <https://www.securityvision.ru/blog/tekhnologiya-soar-i-ee-mesto-v-soc/> (дата обращения 01.02.2025)
2. https://www.anti-malware.ru/analytics/Market_Analysis/Security-Orchestration-Automation-and-Response-SOAR-Solution-Overview (дата обращения 01.02.2025)
3. Symantec (2019). SOAR: The Future of Security Operations. (дата обращения 05.02.2025)
4. McAfee (2018). SOAR: A New Approach to Security Operations. (дата обращения 05.02.2025)
5. Forrester Research (2018). SOAR: The Missing Piece of the Security Automation Puzzle. (дата обращения 05.02.2025)
6. McAfee (2018). SOAR: A New Approach to Security Operations (дата обращения 05.02.2025)
7. Pulyala, S. R., Desetty, A. G., & Jangampet, V. D.. (2019). The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT). <https://doi.org/10.61841/turcomat.v10i3.14323> (дата обращения 13.02.2025)
8. Palo Alto Networks (2019). SOAR Automation: A Game-Changer for SOC Efficiency (дата обращения 13.02.2025)
9. Rapid7 (2019). SOAR: A New Paradigm for Security Automation (дата обращения 13.02.2025)
10. Symantec (2019). SOAR: The Future of Security Operations (дата обращения 13.02.2025)
11. Palo Alto Networks (2019). SOAR Automation: A Game-Changer for SOC Efficiency (дата обращения 13.02.2025)
12. IBM (2018). SOAR: Orchestrating Security Automation for a More Efficient SOC (дата обращения 13.02.2025)

УДК 621.315.66

*И.В. Брякин¹, И.В. Бочкарев², Т.Э. Умаров²*¹*Институт машиноведения, автоматизации и геомеханики НАН КР*²*Кыргызский Государственный Технический Университет им. И. Раззакова*

КОНТРОЛЬ СОСТОЯНИЯ ЭЛЕМЕНТОВ ОПОР ЛИНИЙ ЭЛЕКТРОПЕРЕДАЧИ

Рассмотрены особенности конструкции и эксплуатации опор ЛЭП, проанализированы используемые на практике методы диагностики и контроля их элементов. Разработан феррозондовый датчик с новым принципом возбуждения на базе электромагнитно-акустического измерительного преобразования для неразрушающего контроля стальных и металлоемких элементов опор ЛЭП. Описаны конструктивное исполнение и принцип работы датчика, проанализированы протекающие в нем физические процессы. Выполнено математическое описание совместного действия электромагнитного, акустического и магнитомодуляционного эффектов в феррозондовом датчике. Новый тип феррозонда для дефектоскопии обеспечивает существенное конструктивное упрощение, которое связано с тем, что его обмотки совмещают такие две функции, как генерация переменного магнитного поля возбуждения; и регистрация информационного сигнала. Кроме того, он обладает повышенной помехозащищенностью и повышенной чувствительностью без ухудшения точности преобразования за счет использования различных физических эффектов при резонансном воздействии соответствующими физическими полями. Произведены экспериментальные исследования разработанного феррозондового датчика, которые показали, что разработанный датчик позволяет регистрировать дефекты на большой глубине залегания и имеет повышенную чувствительность.

Ключевые слова: линии электропередачи, опоры, дефектоскопия и неразрушающий контроль, феррозондовый датчик, модуляция магнитной проницаемости, электромагнитно-акустический эффект, акустические волны, магнитный поток, напряженность переменного магнитного поля.

Введение

Электроэнергетика является основной бюджетообразующей отраслью Кыргызстана. Энергетическая система республики полностью обеспечивает электрической энергией все отрасли экономики и население, а также позволяет осуществлять ее экспорт в другие страны [1]. Поэтому обеспечение высокой степени надежности ее работы является для Кыргызстана важной задачей.

Одной из ключевых составляющих любой энергетической инфраструктуры являются электрические сети, обеспечивающие передачу электроэнергии от мест ее генерации к местам потребления. Их особенность состоит в большой протяженности, что принципиально затрудняет процесс их эксплуатации. Например, общая протяженность линий электропередачи (ЛЭП) в Кыргызстане составляет примерно 70 000 км, причем многие ее участки находятся в эксплуатации уже длительное время, превышающее установленный срок их службы. Поэтому для обеспечения гарантированной надежности электроснабжения требуется оперативная реконструкция таких старых участков ЛЭП исходя из нормативных сроков их службы. Однако такая масштабная работа, с одной стороны, требует огромных капиталовложений и времени, а с другой – не всегда оправдана с технической точки зрения, поскольку не учитывает фактическое состояние различных элементов ЛЭП, и процесс такой реконструкции, основанной только на учете времени их нахождения в эксплуатации, может привести к выводу из эксплуатации и замене еще вполне исправного и работоспособного оборудования, что экономически совершенно не оправдано. Очевидно, что необходимо проводить «адресно-восстановительный ремонт» на базе результатов текущего диагностического контроля [2, 3].

Надежность работы ЛЭП обусловлена совокупностью целого ряда факторов и определяется надежностью функционирования всех элементов, входящих в ее состав. Поэтому в систему комплексной диагностики состояния воздушных линий электропередачи в обязательном порядке должен входить контроль состояния всех основных конструктивных элементов ЛЭП- проводов, заземляющих и грозоотводных тросов, изоляторов, опор, оттяжек и т.д. В данной работе рассматриваются вопросы диагностики и контроля технического состояния опор ЛЭП различных конструкций.

Цель исследования. Одну из ключевых функций в составе ЛЭП выполняют опоры, которые поддерживают провода на необходимой высоте, обеспечивая тем самым безопасную передачу электрической энергии. Очевидно, что их техническое состояние однозначно определяет безопасность и надежность работы всей ЛЭП в целом. Так, по статистическим данным, среди всех повреждений воздушных ЛЭП 6-10 кВ примерно 20% аварийных отключений по количеству и 28% по длительности обусловлены именно разрушением опор [4]. При этом выход из строя опор приводит к большим затратам, связанным с восстановлением ЛЭП, перерыву в электроснабжении и даже к рискам угрозы жизни и здоровью персонала и населения. Поэтому требуется их регулярное обследование, которое позволяет выявлять повреждения и дефекты на ранних стадиях их образования и развития, предотвращая тем самым аварийные ситуации и снижая экономические издержки на ремонт. Следовательно, контроль состояния опор линий электропередачи является весьма актуальной задачей, имеющей значительную практическую ценность.

Особенности конструкции и эксплуатации опор ЛЭП. Очевидно, что прочность конструкции ЛЭП, ее долговечность и устойчивость к воздействию внешних механических и природных факторов однозначно зависят от конструкции и типа опор. К основным элементам опор относят фундамент, стойки, подкосы, растяжки. При этом конструкции опор ЛЭП весьма разнообразны и в значительной степени зависят от материала, из которого они изготовлены. На воздушных ЛЭП применяются деревянные, стальные, железобетонные опоры, а также опоры из композитного материала. Кроме того, конструкции опор зависят от категории передаваемого ЛЭП напряжения, а также от условий в местах их установки (качество грунта, атмосферные и погодные условия, техногенные факторы и т.д.).

По конструктивному исполнению опоры ЛЭП можно разделить на два типа – свободностоящие и опоры на оттяжках. Оттяжки обычно выполняются из стальных тросов и служат для удержания деревянных или железобетонных опорных стоек в вертикальном положении и защищают их от падения или возможных наклонов и поперечных перемещений. При этом используют талреп, представляющий собой такелажное приспособление, позволяющее регулировать силу натяжения троса и выполненное в виде двойной винтовой стяжки, в которую с двух сторон закручивают винты с разнонаправленной резьбой. При повороте корпуса талрепа эти винты позволяют изменять рабочую длину и таким образом натяжение троса оттяжки. Следовательно, при диагностике опор второго типа необходим контроль как самого тела опоры, так и оттяжки.

На конструктивные элементы опоры ЛЭП в процессе их эксплуатации воздействуют различные внешние и внутренние факторы, основными из которых являются:

- климатические воздействия (ветер, снег, перепады температуры, землетрясения, оползни и т.п.);
- механическое воздействие в виде статических и динамических нагрузок, в том числе от электродинамической нагрузки электрической сети;
- коррозия и старение материалов.

Все указанные факторы приводят к износу опор, что может привести к возникновению различных аварийных ситуаций – к потере прочности и деформации опоры; к трещинам, разрушению и наклону опор; к нарушению целостности креплений и т.п. Например, в октябре 2021 года из-за обильного снегопада, сильного ветра и большого налипания мокрого снега на провода на горном перевала Сары-Кыр верхняя часть железной опоры загнулась, и все три отходящих фазных провода ЛЭП 110 кВ «Урумбаш — Жетиген» были оборваны. В

целом на аварийно-восстановительные работы ушло 13 дней. В ноябре 2021 года из-за сильного ветра упала железобетонная опора на подстанции Быстровка, а в феврале 2024 года из-за сильного ветра в селах Чырпыкты, Кош-Кол, Тамчи и Чок-Тал Иссык-Кульской области были повалены пять опор линии электропередачи, что привело к масштабным сбоям электроснабжения. Все это подчеркивает важность достоверной и своевременной диагностики и контроля технического состояния опор ЛЭП в реальных условиях эксплуатации.

Методы диагностики и контроля элементов опор ЛЭП

Диагностика и мониторинг технического состояния элементов ЛЭП должны осуществляться на всех этапах их жизненного цикла – при проектировании, изготовлении, строительстве, реконструкции и реновации. При этом существуют различные виды диагностики (плановая, периодическая, внеочередная, аварийной и др.), отличающиеся задачами и объемом контрольных мероприятий и, соответственно, различными методами и оборудованием [5].

На практике наиболее распространенным методом оценки технического состояния опор ЛЭП является визуальный контроль. Конечно, этот метод наиболее простой и экономичный, поскольку не требует никакого специального оборудования. Однако он позволяет зафиксировать только уже наступившие дефекты, причем лишь в тех местах, которые доступны для визуального осмотра. Внутренние дефекты, а тем более еще только зарождающиеся зоны отклонения параметров от их нормированного состояния, которые впоследствии могут привести к неминуемым аварийным ситуациям, такой метод контроля не может выявить в принципе. Поэтому требуются другие методы диагностики опор ЛЭП, которые позволяют осуществлять контроль их внутреннего состояния, причем непосредственно в режиме эксплуатации.

В настоящее время для диагностики технических объектов наиболее целесообразно применять неразрушающие способы контроля. Именно неразрушающий контроль (НК) является основой контроля различных технических объектов, обеспечивая их безопасную и надежную работу без ущерба для дальнейшего использования [6 - 8]. НК позволяет проводить оперативный мониторинг качества контролируемых объектов непосредственно в процессе эксплуатации, предотвращая тем самым их преждевременную поломку и аварию. При этом выбор метода контроля технического состояния опор зависит от их конструкции и материала, из которого они изготовлены. Следует отметить, что при диагностике элементов опор ЛЭП используют и разрушающие методы. Например, оценку темпа снижения механической прочности троса оттяжек опор проводят в лабораторных условиях путем механических испытаний на разрыв образцов оттяжек, полностью демонтированных с опоры. Однако очевидно, что такой способ контроля не только имеет большую трудоемкость, но и не может быть использован в полевых условиях непосредственно для контроля опор, находящихся в эксплуатации.

При реализации НК для выявления наличия дефектов или неоднородностей, их характера, размера и месторасположения могут использоваться различные способы, основанные на оптических, электрических, магнитных, акустических и других свойствах материалов [9, 10]. Поскольку опоры ЛЭП содержат компоненты, изготовленные из ферромагнитных конструкционных материалов, то НК их качества наиболее целесообразно проводить на основе магнитных измерений [11, 12]. В магнитной дефектоскопии для выявления подповерхностных дефектов преимущественно используют феррозондовые преобразователи, содержащие в своем составе феррозондовый датчик (ФД) [13, 14]. Их работа основана на поиске магнитных полей рассеяния, возникающих в зоне подповерхностных дефектов – в зонах концентрации продольных и поперечных напряжений, в зонах пластической деформации, в зонах изменения структуры металла, на участках предразрушения и разрушения металла. Это позволяет осуществлять контроль технического состояния ферромагнитного объекта. ФД осуществляет контроль изменения напряженности магнитного поля над дефектом и преобразует градиент напряженности поля в электрической

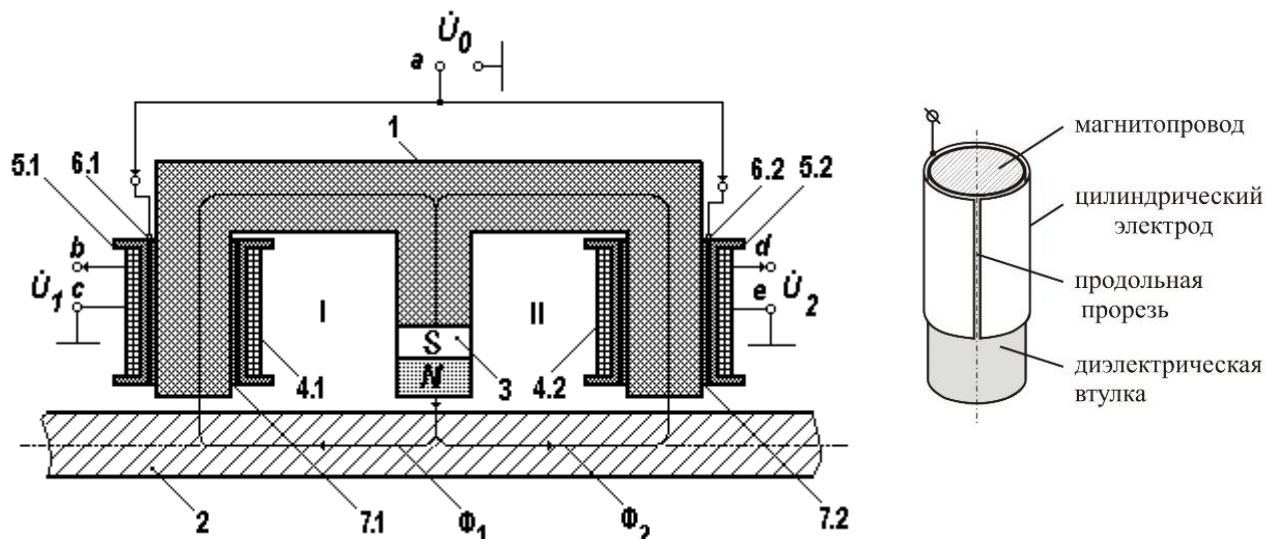
сигнал. По сравнению с другими датчиками $\Phi Д$ имеют ряд преимуществ, а именно, небольшие габариты и потребляемую мощность, высокие чувствительность и надежность работы, стойкость к внешним воздействиям, избирательность к локальным магнитным полям рассеяния и др. Бесконтактный магнитометрический метод-контроль технического состояния металлических конструкций опор ЛЭП с использованием $\Phi Д$ обеспечивает обнаружение и регистрацию дефектных участков в виде наличия трещин, раковин и т.п., а также позволяет классифицировать зарождающиеся и развивающиеся дефекты по степени опасности. Данный метод может быть использован для контроля металлических конструкций опор при их сооружении и периодических технических освидетельствованиях, а также для оптимизации объемов при капитальном ремонте ЛЭП. Поэтому системы НК на базе $\Phi Д$ в настоящее время активно развиваются и совершенствуются [15-19].

Наряду с магнитными способами контроля для НК опор на практике используются акустические методы, основанные на том, что в контролируемом объекте возбуждают акустические волны, последующий анализ которых позволяет получить информацию о структуре материала и его параметрах, изменяющихся при наличии дефектов. Контроль параметров ультразвуковой волны позволяет судить о структурных изменениях в материале опоры, содержании примесей, характере распределений внутренних напряжений и др. [20, 21]. При этом акустические методы НК имеют высокую чувствительность и проникающую способность, а также высокую производительность и безопасность выполнения контрольных процедур.

Таким образом, каждый из этих известных методов НК реализует какой-либо один физический эффект, который однозначно определяет как возможности самого метода, так и особенности его реализации. Очевидно, что повышения эффективности контроля технического и коррозионного состояния металлоконструкций опор ЛЭП можно добиться путем одновременного использования систем магнитного контроля и систем акустического контроля. Однако такие комплексные испытания, требующие применения различного специализированного оборудования, являются весьма трудоемкими и затратными.

Результаты исследования и их обсуждение

На базе проведенных исследований авторами разработан вариант $\Phi Д$ с новым принципом возбуждения, основанным на одновременном использовании электромагнитно-акустического и магнитомодуляционного эффектов (ЭМА-эффект и ММЭ-эффект). Посредством данного $\Phi Д$ фактически реализуется метод НК, объединяющий в себе потенциальные возможности трех магнитных методов НК: постоянного магнитного поля, переменного магнитного поля и феррозондового метода. При этом не требуется обязательная процедура предварительного намагничивания материала объекта контроля. В этом случае постоянное магнитное поле используется в качестве зондирующего физического поля, модулируемого через μ -преобразование переменными магнитным полем, а уровень вариативности этого процесса зависит от состояния структуры материала объекта контроля. Вариант конструкции нового типа $\Phi Д$ представлен на рисунке 1.



а)

б)

Рисунок 1 – Вариант конструктивного решения $\Phi Д$

На рисунке 1 обозначено: 1 – Ш-образный магнитопровод ($ШМ$) из диэлектрического ферромагнетика; 2 – объект контроля ($ОК$) в виде конструктивного элемента из ферромагнитного материала; 3 – постоянный магнит ($ПМ$); 4.1 и 4.2 – электрические обмотки соответственно первой и второй измерительных катушек ($ИК_1$ и $ИК_2$); 5.1 и 5.2 – диэлектрические каркасы соответственно $ИК_1$ и $ИК_2$; 6.1 и 6.2 – первый и второй цилиндрические электроды ($ЦЭ_1$ и $ЦЭ_2$), являющиеся элементами возбуждения соответственно для $ИК_1$ и $ИК_2$; 7.1 и 7.2 – диэлектрические цилиндрические втулки, локально расположенные на отдельных участках $МП$; a – клемма подключения напряжения возбуждения $\dot{U}_0$ относительно «корпуса»; b и d – клеммы съема выходных сигналов $\dot{U}_1$ и $\dot{U}_2$ соответственно $ИК_1$ и $ИК_2$ относительно «корпуса», являющиеся «началом» соответственно электрических обмоток 4.1 и 4.2. Цилиндрические электроды $ЦЭ_1$ и $ЦЭ_2$ выполнены из электропроводящего материала (медь, алюминий и т.д.) в виде тонкостенных трубок с прорезью вдоль образующей и расположены коаксиально на внутренней поверхности соответственно диэлектрических каркасов 5.1 и 5.2 (рис. 1, б). При контроле опоры ЛЭП в качестве $ОК$ используется ее элемент, подлежащий диагностике, например, стальная оттяжка.

Особенностью данного типа $\Phi Д$ является применение в качестве сигнальных выходов $ИК_1$ и $ИК_2$ (относительно «корпуса») одноименных выводов их электрических обмоток («начало» обмоток), что в свою очередь является одним из основных условий для нормального функционирования рассматриваемого варианта $\Phi Д$. Кроме того, $ЦЭ_1$ образует совместно с нижним проволочным слоем обмотки $ИК_1$ конденсатор связи $C'_{св}$, а $ЦЭ_2$ образует совместно с нижним проволочным слоем обмотки 4.2 $ИК_2$ конденсатор связи $C''_{св}$. Напряжение возбуждения $\dot{U}_0$ относительно «корпуса» подается через конденсаторы связи $C'_{св}$ и $C''_{св}$ соответственно на «начало» электрических обмоток $ИК_1$ и $ИК_2$, имеющих «согласное» пространственное расположение («начало-конец») на $ШМ$.

$ШМ$ образует вместе с $ОК$ два взаимосвязанных ферромагнитных контура $\Phi К-I$ и $\Phi К-II$, через которые определенным образом конфигурируются магнитные потоки Φ_1 и Φ_2 , инициируемые совмещенными физическими полями: постоянным магнитным полем $ПМ$ и переменными магнитными полями, создаваемыми токами возбуждения электрических обмоток $ИК_1$ и $ИК_2$,

При подаче от генератора высокой частоты электрического потенциала $\varphi_э$ относительно электрического потенциала «корпуса» (точки заземления) φ_0 на $ЦЭ_1$ и $ЦЭ_2$ на нижнем проволочном слое первой обмотки $ИК_1$ и нижнем проволочном слое обмотки $ИК_2$ будут индуцироваться соответствующие электрические потенциалы $\varphi'_э$ и $\varphi''э$. При этом вследствие симметричного пространственного расположения проходных катушек и идентичности их конструктивных параметров можно считать, что $\varphi'_э = \varphi''э = \varphi_э$. Необходимый уровень симметрии в пространственном расположении проходных катушек и балансировка минимального уровня нулевого сигнала обеспечивается соответствующим осевым перемещением секций проходных катушек относительно постоянного магнита.

Тогда в режиме последовательного электрического резонанса (на циклической частоте ω_p) токи через электрические обмотки $ИК_1$ и $ИК_2$ описываются выражением:

$$i_1(t) = i_2(t) = i(t) = (\varphi_э - \varphi_0) / R = u_0(t) / R = (U_{0m} \times \cos \omega_p t) / R, \quad (1)$$

где $\varphi_0 = 0$; $R = R_1 = R_2$; R_1 и R_2 – активные сопротивления соответственно секции 3' и 3'' обмотки катушки; U_{0m} – амплитуда электрического напряжения от генератора высокой частоты.

В этом случае напряженность переменного магнитного поля, создаваемая токами возбуждения $ИК_1$ и $ИК_2$, можно формализовать в следующем виде:

$$H_1(t) = H_2(t) = H(t) = \frac{2 \times \sqrt{2} \times w \times U_{0m}}{l \times R} \times \cos \omega_p t = H_m \times \cos \omega_p t, \quad (2)$$

где $l = l_1 = l_2$ – длина намотки электрических обмоток $ИК_1$ и $ИК_2$; $w = w_1 = w_2$ – количество витков электрических обмоток $ИК_1$ и $ИК_2$; H_m – амплитуда напряженности магнитного поля, создаваемая током $i(t)$:

$$H_m = \frac{2 \times \sqrt{2} \times w \times U_{0m}}{l \times R}. \quad (3)$$

Рассмотрим вопросы, связанные с особенностями формирования магнитных потоков Φ_I и Φ_{II} в магнитопроводах соответственно ΦK -I и ΦK -II.

В соответствии с законами электротехники для магнитных потоков Φ_I и Φ_{II} , создаваемых в каждом из ΦK -I и ΦK -II, можно соответственно записать:

$$\Phi_I = \frac{F_I}{R'_{IM} + R''_{IM} + R'''_{IM}} = \frac{F_I}{R^*_{IM} + R'''_{IM}}; \quad \Phi_{II} = \frac{F_{II}}{R'_{IIM} + R''_{IIM} + R'''_{IIM}} = \frac{F_{II}}{R^*_{IIM} + R'''_{IIM}}, \quad (4)$$

где $F_I = F_I^- + F_I^+$ – суммарная намагничивающая сила в ΦK I, F_I^- и F_I^+ – намагничивающие силы, создаваемые соответственно H_0 и $H(t)$ в ΦK -I; $F_{II} = F_{II}^- + F_{II}^+$ – суммарная намагничивающая сила в ΦK -II, F_{II}^- и F_{II}^+ – намагничивающие силы, создаваемые соответственно H_0 и $H(t)$ в ΦK -II; R'_{IM} – магнитное сопротивление участка OK , находящегося в рабочей зоне ΦK I и являющегося его контролируемым элементом; $R^*_{IM} = R'_{IM} + R''_{IM}$ – суммарное магнитное сопротивление конструктивных элементов ΦK I; R'_{IM} и R''_{IM} – магнитное сопротивление соответственно ферромагнитного и диэлектрического (воздушный зазор) конструктивных элементов ΦK -I; R'''_{IM} – магнитное сопротивление участка OK , находящегося в рабочей зоне ΦK -II и являющегося его контролируемым элементом; $R^*_{IIM} = R'_{IIM} + R''_{IIM}$ – суммарное магнитное сопротивление конструктивных элементов ΦK -II, R'_{IIM} и R''_{IIM} – магнитное сопротивление соответственно ферромагнитного и диэлектрического (воздушный зазор) конструктивных элементов ΦK -II.

Следует заметить, что $R^*_{IM} = R^*_{IIM} = R^*_M = \text{const}$, т.к. являются параметрами идентичных конструктивных элементов ΦK -I и ΦK -II, а R'''_{IM} и R'''_{IIM} являются вариативными параметрами контролируемых элементов соответственно ΦK -I и ΦK -II, которые при отсутствии дефекта в рабочих зонах ΦK -I и ΦK -II соответствуют условию $R'''_{IM} = R'''_{IIM} = R'''_M$. Кроме того, считается, что $R'''_{IM} \gg R^*_{IM}$ и $R'''_{IIM} \gg R^*_{IIM}$. С учетом этих замечаний из (4) получим:

$$\Phi_I = \frac{F_I}{\left(1 + \frac{G'''_{IM}}{G^*_{IM}}\right)} \times G'''_{IM} = F_I \times G'''_{IM} = F_I \times \mu'''_{IM} \times \frac{l'''_{IM}}{S'''_{IM}}; \quad (5)$$

$$\Phi_{II} = \frac{F_{II}}{\left(1 + \frac{G'''_{IIM}}{G^*_{IIM}}\right)} \times G'''_{IIM} = F_{II} \times G'''_{IIM} = F_{II} \times \mu'''_{IIM} \times \frac{l'''_{IIM}}{S'''_{IIM}},$$

где $G'''_{IM} = 1/R'''_{IM} = \mu'''_{IM} \times \frac{l'''_{IM}}{S'''_{IM}}$ и $G'''_{IIM} = 1/R'''_{IIM} = \mu'''_{IIM} \times \frac{l'''_{IIM}}{S'''_{IIM}}$ – магнитные проводимости

участков OK , находящихся в рабочих зонах соответственно ΦK -I и ΦK -II; $G^*_{IM} = 1/R^*_{IM}$ и

$G_{II_M}^* = 1/R_{II_M}^*$ суммарные магнитные проводимости конструктивных элементов соответственно $\Phi K-I$ и $\Phi K-II$; μ_{I_M}''' , l_{I_M}''' и s_{I_M}''' – соответственно магнитная проницаемость, длина и площадь сечения участка OK , находящегося в рабочей зоне $\Phi K-I$; μ_{II_M}''' , l_{II_M}''' и s_{II_M}''' – соответственно магнитная проницаемость, длина и площадь сечения участка OK , находящегося в рабочей зоне $\Phi K-II$; $G_{I_M}''' / G_{I_M}^* \ll 1$; $G_{II_M}''' / G_{II}^* \ll 1$.

Из анализа выражений (5) следует важный вывод о том, что свойство неизменности параметров магнитных потоков Φ_I и Φ_{II} во времени главным образом определяется уровнем вариативности параметров μ_{I_M}''' и μ_{II_M}''' .

Магнитная проницаемость μ является основным физическим параметром материала $МП$, который реагирует на внешние воздействия. В данном случае эти воздействия можно разделить на два типа:

- основным воздействием можно считать переменные магнитные поля, возбуждаемые измерительными катушками $ИК_1$ и $ИК_2$. Эти поля инициируют появление магнитомодуляционного эффекта (ММ-эффект);

- дополнительным воздействием является акустическое поле, являющееся проявлением электромагнитно-акустического эффекта (ЭМА-эффект).

Подобное совместное действие магнитных и акустических полей оказывает модулирующее действие на магнитную проницаемость, т.е. μ -преобразование осуществляется за счет одновременного совместного воздействия ММ-эффекта и ЭМА-эффекта. Поэтому с учетом вида физического поля и явлений его взаимодействия с материалом OK в предложенном $ФД$ в режимах излучения и приема в общем случае можно выделить четыре функциональных процесса работы:

- первый процесс – формирование возбуждающего переменного магнитного поля (режим индуктора);

- второй процесс – μ -преобразование за счет ММ-эффекта;

- третий процесс – формирование пространственно-периодических акустических волн (режим ЭМА-преобразователя);

- четвертый процесс – μ -преобразование за счет ЭМА-эффекта.

Следовательно, разработанный вариант $ФД$ по существу является параметрическим модулятором, где модуляция измеряемой величины (постоянное магнитное поле $ПМ$) осуществляется за счет двухфакторного воздействия на магнитную проницаемость μ , т.е. μ -преобразование за счет одновременного совместного воздействия ММ-эффекта и ЭМА-эффекта.

Физические процессы, протекающие в $ФД$

Далее рассмотрим вопросы, связанные с воздействием совмещенных магнитных полей (постоянных и переменных) в $ШМ$ $ФД$ непосредственно на структуру материала электропроводящих ферромагнитных конструктивных элементов ферромагнитных контуров.

Проанализируем подробнее процедуры воздействия на магнитную проницаемость μ каждого из указанных полей.

1) ММ-процесс. Заключается в изменении магнитного состояния ферромагнитного электропроводящего материала OK при одновременном намагничивании в переменном и измеряемом постоянном магнитных полях. Модуляция таким суммарным магнитным потоком возможна за счет нелинейных свойств магнитной цепи, а происходящие в ней процессы всегда связаны с взаимодействием минимум двух магнитных полей – внешнего измеряемого и переменного поля возбуждения, создаваемого, например, за счет протекания электрического тока в катушке возбуждения. С физической точки зрения ММ-процесс по своей сути является режимом функционирования феррозонда с продольным возбуждением. Поэтому в соответствии с существующей параметрической теорией феррозондов с продольным возбуждением можем записать:

$$B_{MM}(t) = \mu_0 \times \mu^*[H(t)] \times H_0 = \mu_0 \times \mu_{MM}^*(t) \times H_0, \quad (6)$$

где μ_0 – магнитная постоянная; $\mu^*[H(t)]$ – закон изменения магнитной проницаемости материала ферромагнитного сердечника под воздействием возбуждающего магнитного поля; $H(t) = H_m \times \sin \omega t$ – напряженность возбуждающего магнитного поля; H_m – амплитуда переменного магнитного поля H_1 ; ω – циклическая частота; H_0 – напряженность постоянного магнитного поля.

При заданной величине поля возбуждающего магнитного поля функция $\mu^*[H(t)]$ может рассматриваться как функция времени $\mu_{MM}^*(t)$.

2) ЭМА-процесс. В основе ЭМА-преобразования лежит явление взаимной трансформации электромагнитных и упругих полей на границе металлических материалов. Прямое ЭМА-преобразование заключается в преобразовании электромагнитных волн в упругие колебания, обратное – в преобразовании упругих волн в электромагнитные волны, а полный процесс преобразования «электромагнитное поле – упругие колебания – электромагнитное поле» является двойным ЭМА-преобразованием. При этом в соответствии с теоремой взаимности акустические характеристики ЭМА-преобразователей при излучении и приеме оказываются идентичными, в частности, сохраняются избирательность волн и диаграммы направленности излучения ЭМА-преобразователей.

Физическая сущность прямого ЭМА-преобразования состоит в том, что под действием падающей электромагнитной волны в среде, не обладающей ни пьезоэлектрическими, ни магнитострикционными свойствами, возбуждаются ультразвуковые волны той же или кратной частоты, причем в преобразовании участвуют подсистемы ферромагнетика различной физической природы: электрическая, магнитная, магнитоупругая и упругая. При этом непосредственным источником возбуждения выступает граница раздела сред, поскольку падение электромагнитной волны на границу проводящего твердого тела сопровождается возбуждением в нем ультразвуковых колебаний [22]. Этот процесс основан на явлении магнитострикции, связанном с взаимодействием магнитной и упругой подсистем магнитной среды и заключающемся в том, что под действием магнитного поля магнетики изменяют свои размеры и форму, за счет чего возникает дополнительная линейная генерация ультразвука. Для генерации упругих волн при использовании магнитострикции в линейном режиме необходимо использовать постоянное подмагничивающее поле [22, 23].

Физическая сущность обратного ЭМА-преобразования состоит в том, что акустические волны действуют на свободные электроны материала ферромагнитного сердечника ΦC_1 и ΦC_2 , за счет чего в электрических обмотках первой и второй измерительных катушек ($ИК_1$ и $ИК_2$) возникает ЭДС. Это свойство основано на том, что продольные упругие L -волны могут эффективно возбуждать спиновые волны [24, 25].

Достигающая поверхностного слоя ферромагнитного объекта исследования акустическая волна, например, отраженная от нижней границы этого объекта либо от имеющегося в нем включения (дефекта) с иными акустическими свойствами, вызывает деформацию доменов этого слоя. Вследствие проявления магнитоупругого эффекта происходит изменение магнитной проницаемости материала поверхностного слоя и, соответственно, изменение индукции B_0 постоянного магнитного поля как в поверхностном слое, так и в близко расположенной к нему плоскости витков обмотки. Последнее приводит к изменению магнитного потока постоянного магнитного поля через обмотку, что вследствие явления электромагнитной индукции вызывает появление в ней ЭДС, мгновенное значение которой функционально связано с характеристиками акустической волны.

Таким образом, двойное ЭМА-преобразование основано на проявлении трех эффектов взаимодействия электромагнитного поля с ОК: магнитострикционного, магнитного и электродинамического. Поэтому данное преобразование применимо только для объектов из проводящего материала (за счет проявления третьего эффекта) и (или) магнитного материала

(за счет проявления первого и второго эффектов). Следовательно, поскольку материал ОК является как магнитным, так и электропроводящим, возбуждаемые ЭМА-преобразователем акустические волны являются результатом всех трех видов взаимодействий, а ЭДС обмотки - суммой ЭДС, являющихся результатами также всех трех взаимодействий. Именно этим объясняет высокая чувствительность предложенного ФД к различным вариациям модулируемого постоянного магнитного поля. Следует отметить, что для рассматриваемых физических процессов под модуляцией понимается изменение состояния магнитной проницаемости материала конструктивных элементов МП ФК-I и ФК-II при воздействии на них физических полей.

Основные преимущества разработанного ФД обусловлены двойным μ -преобразованием за счет одновременного использования магнитомодуляционного и электромагнитно-акустического эффектов. По сравнению с традиционными системами, используемыми для решения задач дефектоскопии, к несомненным преимуществам предложенного ФД следует отнести следующие:

- отсутствие непосредственного контакта с ОК, поэтому предложенный ФД не подвержен трению и, следовательно, не изнашивается;
- расстояние от ФД до поверхности ОК может составлять до 10 мм, т.е. между поверхностью объекта контроля и поверхностью датчика могут располагаться различные среды, например, краска, пластик, грязь, воздух и другие токонепроводящие среды;
- отсутствие необходимости предварительной подготовки поверхности ОК (зачистки и шлифовки), которая необходима для обеспечения хорошего акустического контакта излучающей поверхности пьезопреобразователей с поверхностью контролируемых изделий;
- разработанный ФД не чувствителен к углу наклона его крепления на ОК, что упрощает процедуру его установки. Кроме того, за счет этого он может быть использован для дефектоскопии объектов сложной формы;
- акустическая волна формируется и распространяется непосредственно в ОК, минуя среду между ФД и ОК, за счет чего отсутствует искажение волны в этой среде. Следовательно, только сам объект контроля и содержащиеся в нем неоднородности способны изменить выходной сигнал, что повышает достоверность контроля;
- модуляция магнитной проницаемости осуществляется несколькими механизмами, обеспечивающими трансформацию энергии одного вида колебаний (электромагнитных) в энергию колебаний другого вида (упругих смещений) и наоборот. Такое комплексное воздействие и определяет высокую чувствительность предлагаемого ФД и повышает точность измерения координат дефектов.

Аналитическое описание процессов, протекающих в предложенном ФД

Новый принцип построения феррозонда для решения задач дефектоскопии основан на использовании бифакторного метода возбуждения чувствительного элемента феррозонда, осуществляющего двойное μ -преобразование за счет одновременной активации магнитомодуляционного и электромагнитно-акустического эффектов. Поэтому значительный интерес представляет получение математической модели разработанного ФД.

Исходя из сказанного выше, можно констатировать, что разработанный ФД выполняет функции индуктора (создает возбуждающее переменное и постоянное магнитные поля), функции генератора ультразвуковой волны непосредственно в исследуемом объекте, а также функции приемника ультразвуковых волн и магнитных полей и формирования выходного информационного сигнала.

За счет взаимодействия вихревых токов с индукцией магнитного поля, создаваемого постоянным магнитом (это поле выполняет функции подмагничивающего поля B_0), появляются силы F_A (сила Ампера), которые направлены вдоль поверхности объекта контроля и приводят к возникновению акустических колебаний [26]:

$$F_A = i_e \times B_0 \times dl, \quad (7)$$

где i_e – вихревой ток на участке OK длиной dl .

Эти упругие силы возникают в приповерхностном слое OK , определяемом глубиной скин-слоя δ :

$$\delta = \sqrt{2/(\omega \times \mu_0 \times \mu \times \sigma)}, \quad (8)$$

где ω – круговая частота колебаний; μ_0 – магнитная проницаемость вакуума; μ – относительная магнитная проницаемость; σ – электропроводность.

Для предложенного варианта конструктивного решения $\PhiД$ характерно одновременное излучение упругих волн из каждой точки на поверхности конструктивных элементов $\PhiК-I$ и $\PhiК-II$ $МП$, расположенной соответственно под $ИК_1$ и $ИК_2$. Следовательно, указанные волны распространяются во всех радиальных направлениях в поперечном сечении OK . Преимущественное возбуждение типа волн определяется взаимной ориентацией поля подмагничивания с индукцией B_0 и вихревых токов i_e , текущих по периметру OK .

В ферромагнитных материалах возникновение и распространение акустических волн обусловлено трансформацией волн на доменных границах, за счет чего возбуждаются связанные магнитоупругие колебания $q(k_n, t)$, приводящие к колебаниям намагниченности:

$$\Delta J_q(k_n, t) = \lambda \times q(k_n, t), \quad (9)$$

где k_n – волновой вектор; λ – коэффициент, зависящий от физических свойств материала OK , численное которого определяется величинами магнитоупругого тензора, волнового вектора k_n и разностью частот спиновой и упругой волн.

Учитывая, что магнитная проницаемость μ связана с магнитной восприимчивостью χ соотношением $\mu = 1 + \chi$, где $\chi = J/H$, получаем:

$$\mu = f[\zeta(t)] = \mu^*[\zeta(t)], \quad (10)$$

где $\zeta(t)$ – функция смещения структурных компонентов $\PhiК-I$ и $\PhiК-II$ магнитопровода.

Тогда с учетом соотношений (9), (10) для режима μ -преобразования за счет ЭМА-эффекта, аналогично (6), можно записать:

$$B_{AM}(t) = \mu_0 \times \mu^*[\zeta(t)] \times H_0 = \mu_0 \times \mu_{AM}^*(t) \times H_0, \quad (11)$$

где $\mu_{AM}^*[\zeta(t)]$ – функция, отражающая закон изменения магнитной проницаемости материала элементов $\PhiК-I$ и $\PhiК-II$ магнитопровода под воздействием возбуждающего акустического поля, которая при заданной амплитуде поля возбуждения может рассматриваться как функция времени $\mu_{AM}^*(t)$.

С учетом совместного модулирующего воздействия акустического и переменного магнитного полей на магнитную проницаемость материала элементов магнитопровода $\PhiК-I$ и $\PhiК-II$ запишем следующее выражение:

$$\mu^* = f[H(t); \zeta(t)]. \quad (12)$$

В соответствии с существующей параметрической теорией феррозондов с продольным возбуждением, где используется разложение функции $B(H_\Sigma)$ при $H_\Sigma = H(t) + H_0$ в ряд Тейлора по малому воздействию и с учетом того, что для рассматриваемого случая функция $\mu^* = f[H(t); \zeta(t)]$ является четной, можем записать:

$$\mu^*(t) = \mu_H \times [1 + (m_{MM} + m_{AM})] \times \cos(2\omega_p t), \quad (13)$$

где m_{AM} и m_{MM} – глубина соответственно акустической и магнитной модуляции; ω_p – циклическая частота возбуждения процессов преобразования на совпадающих частотах электромеханического и магнитного резонансов.

Глубину соответствующей модуляции магнитной проводимости можно определить по следующим формулам:

$$m_{AM} = \mu_m \times \eta_{AM} \times \zeta_m \times \mu_H^{-1}; \quad m_{MM} = \mu_m \times \eta_{MM} \times H_m \times \mu_H^{-1},$$

где η_{AM} и η_{MM} – коэффициенты соответственно акустомагнитного и магнитомодуляционного преобразований.

Из выражения (12) и (13) следует, что постоянное магнитное поле $H_0(t)$ ПМ, направленное аксиально к ферромагнитным элементам $\Phi K-I$ и $\Phi K-II$, за счет параметрической модуляции осциллирующей магнитной проницаемостью ферромагнитного материала ΦC_1 и ΦC_2 трансформируется в переменное магнитного поле с соответствующей индукцией:

$$\begin{aligned} B_I(t) &= \mu_0 \times \mu_I^*(t) \times H_0 = \mu_0 \times \mu_{IH} \times [1 + (m_{MM} + m_{AM}) \times \cos(2\omega_p t)] \times H_0; \\ B_{II}(t) &= \mu_0 \times \mu_{II}^*(t) \times H_0 = \mu_0 \times \mu_{IIn} \times [1 + (m_{MM} + m_{AM}) \times \cos(2\omega_p t)] \times H_0. \end{aligned} \quad (14)$$

Вариации магнитного поля ПМ, вызванные уже модулирующими процессами магнитной проницаемости, соответственно воздействуют на обмотки $ИК_1$ и $ИК_2$, индуцируя в них соответствующие э.д.с. $e_1(t) = -w \times d\Phi_I(t)/dt$.

Учитывая, что $e_1(t) = -w \times d\Phi_I(t)/dt$ и $e_2(t) = -w \times d\Phi_{II}(t)/dt$, можем записать:

$$e_1(t) = -s_1 \times w \times \frac{dB_I(t)}{dt} \quad \text{и} \quad e_2(t) = -s_2 \times w \times \frac{dB_{II}(t)}{dt}. \quad (15)$$

Подставляя (14) в (15), для каждой из измерительных катушек получим:

– для $ИК_1$

$$\begin{aligned} e_1(t) &= -s_1 \times w \times \mu_0 \times \left[\mu_I^*(t) \times \frac{dH_0}{dt} + H_0 \times \frac{d\mu_I^*}{dt} \right] = -s_1 \times w \times \mu_0 \times H_0 \times \frac{d\mu_I^*}{dt} = \\ &= -2 \times s_1 \times w \times \mu_0 \times \mu_{IH} \times \omega_p \times H_0 \times (m_{MM} + m_{AM}) \times \sin(2\omega_p t); \end{aligned} \quad (16)$$

– для $ИК_2$

$$\begin{aligned} e_2(t) &= -s_2 \times w \times \mu_0 \times \left[\mu_{II}^*(t) \times \frac{dH_0}{dt} + H_0(t) \times \frac{d\mu_{II}^*}{dt} \right] = -s_2 \times w \times \mu_0 \times H_0 \times \frac{d\mu_{II}^*}{dt} = \\ &= -2 \times s_2 \times w \times \mu_0 \times \mu_{IIn} \times \omega_p \times H_0 \times (m_{MM} + m_{AM}) \times \sin(2\omega_p t). \end{aligned} \quad (17)$$

Для выходных сигналов $u_1(t)$ и $u_2(t)$ соответственно $ИК_1$ и $ИК_2$ можем записать следующие соотношения:

$$u_1(t) = e_1(t) + u_{K1}(t); \quad u_2(t) = e_2(t) + u_{K2}(t), \quad (18)$$

где $u_{K1}(t)$ и $u_{K2}(t)$ – электрические напряжения, возникающие на электрических обмотках $ИК_1$ и $ИК_2$ при подаче на $\Phi Д$ напряжения возбуждения $\dot{U}_0$.

Исходя из того, что $\Phi Д$ функционирует в режиме градиентомера, для регистрируемого суммарного информационного сигнала $\Phi Д$ относительно «корпуса» с учетом того, что $u_{K1}(t) = u_{K2}(t)$, можем записать:

$$u_{\Sigma}(t) = u_1(t) - u_2(t) = e_1(t) + u_{K1}(t) - e_2(t) - u_{K2} = e_1(t) - e_2(t). \quad (19)$$

Тогда, исходя из (16), (17) и (19), будем иметь:

$$\begin{aligned} u_{\Sigma}(t) &= 2 \times s^* \times w \times \mu_0 \times \omega_p \times (m_{MM} + m_{AM}) \times (\mu_{IIn} - \mu_{IH}) \times H_0 \times \sin(2\omega_p t) = \\ &= 2 \times s^* \times w \times \mu_0 \times \omega_p \times (m_{MM} + m_{AM}) \times \Delta \mu_M''' \times H_0 \times \sin 2\omega_p t, \end{aligned} \quad (18)$$

где $s^* = s_1 = s_2$.

В выражении (18) четко прослеживается реализация принципа суперпозиции в виде бифакторного модулирующего воздействия от проявления двух основных физических эффектов, инициируемых соответствующими активизирующими физическими полями, что, в свою очередь, говорит о повышении эффективности μ -преобразования в целом, а также уровень вариативности этого процесса от наличия дефекта, проявляющегося в параметре $\Delta \mu_M'''$.

Для подтверждения состоятельности предлагаемых технических решений были проведены соответствующие экспериментальные исследования. При этом был использован способ относительного сравнения, основанный на сопоставлении результатов контроля, выполненного испытуемой системой НК, с результатами контроля, выполненного эталонной

системой НК, в качестве которой был выбран дефектоскоп-градиентометр ДФ-105, содержащий электронный блок и феррозондовый преобразователь ФП-4. Анализ полученных результатов показал, что испытуемая система НК по сравнению с эталонной системой обладает возможностью регистрации более мелких дефектов на больших глубинах их залегания.

Заключение

Своевременное обнаружение дефектов в металлосодержащих элементах опор ЛЭП положительно влияет на их надежность в процессе эксплуатации, что в свою очередь существенно снижает расходы, связанные с отказами и авариями ЛЭП в целом. Показано, что для решения данной проблемы широкое применение имеет магнитный неразрушающий контроль, одним из видов которого является феррозондовый метод, основанный на обнаружении и измерении с помощью магнитных полей рассеяния, возникающих в зоне дефектов.

Для решения задач дефектоскопии предложен новый принцип построения феррозондового датчика, основанный на использовании бифакторного метода возбуждения чувствительного элемента феррозонда, осуществляющего двойное μ -преобразование за счет одновременной активации магнитомодуляционного и электромагнитно-акустического эффектов. Разработана конструкция нового типа *ФД*, описан принцип его работы, рассмотрены физические процессы, протекающие в нем при реализации электромагнитно-акустического измерительного преобразования. Новый тип феррозонда для дефектоскопии обладает следующими преимуществами:

- существенное конструктивное упрощение, которое связано с тем, что $ИК_1$ и $ИК_2$ совмещают такие две функции, как генерация переменного магнитного поля возбуждения и регистрация информационного сигнала;
- повышенная помехозащищенность, за счет использования $ИК_1$ и $ИК_2$ в качестве плечевых элементов емкостно-индуктивного измерительного моста с разностным сигналом его измерительной диагонали (компенсация синфазных составляющих помехи и последствий температурного дрейфа);
- повышенная чувствительность без ухудшения точности преобразования, которая обеспечивается путем использования набора свойств материала конструктивных элементов *ФК-I* и *ФК-II МП*, проявляемых в виде различных физических эффектов при резонансном воздействии соответствующими физическими полями;
- пониженное энергопотребление.

Предложенный *ФД* легко использовать для мониторинга состояния стальных и железосодержащих элементов опор ЛЭП непосредственно в полевых условиях, поскольку для проведения контрольных операций его достаточно просто поднести к *ОК* и перемещать вдоль контролируемой зоны, фиксируя в ней наличие дефектов или структурной неоднородности.

Разработанный метод дефектоскопии и датчик для его реализации могут быть использованы наряду с контролем опор ЛЭП для контроля других металлических элементов и конструкций ЛЭП при их сооружении, периодических технических освидетельствованиях, при капитальном ремонте, в частности, для контроля металлических и сталеалюминиевых проводов или стальных сердечников самонесущих проводов в процессе их изготовления.

Литература

1. Джылкычиева Ж.Т., Бекибаев И.Ж. Оценка энергетического сектора Кыргызской Республики // Известия вузов Кыргызстана. – 2023. – № 6. – С. 216–219.
2. Гунгер Ю.Р., Чернев В.Т. Диагностика опор и фундаментов воздушных линий электропередачи. Современные методы оценки // Новости электротехники. – 2006. – № 2. – С. 134–136.

3. Глухов Д. А. Методика оценки приоритетности ремонта ЛЭП на основе риск-ориентированного анализа с учетом ремонтпригодности // *Электрооборудование: эксплуатация и ремонт.* – 2019. – № 12. – С. 27–34.
4. Кабашов, В.Ю. Исследование причин аварийных отключений сельских ВЛ 6-10 кВ / В.Ю. Кабашов // *Инновационная наука.* – 2017. – №04-3. – С. 70–73.
5. Арбузов Р.С., Овсянников А.Г. Современные методы диагностики воздушных линий электропередачи. – Новосибирск: Наука, 2009. – 135 с.
6. Ключев В. В. Неразрушающий контроль и диагностика. Справочник. – М.: Машиностроение, 2003. – 487 с.
7. Paipetis A. S., Matikas T. E., Aggelis D. G., Van Hemelrijck D. *Emerging Technologies in Non-Destructive Testing* V. London: CRC Press. – 2012. – 526 p.
8. Mao X., Zhao Y., Xiao T. Review of the development of metal non-destructive testing and imaging technology, 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, – 2018. – pp. 926-929, doi: 10.1109/ITOEC.2018.8740475.
9. Афанасьев В. Б., Чернова Н. В. Современные методы неразрушающего контроля // *Успехи современного естествознания.* – 2011. – № 7. – С. 73–74.
10. Петров О.Н., Сокольников А. Н., Верещагин В. И., Агровиченко Д. В. Методы неразрушающего контроля. – Красноярск: СФУ, 2021. – 132 с.
11. Бобров А.Л., Лесных Е.В. Основы магнитного неразрушающего контроля. – Новосибирск: Изд-во СГУПС. – 2018. – 108 с.
12. Ficili F. *Non-Destructive Testing by Magnetic Techniques.* – LAP Lambert Academic Publishing, 2012. – 140 p.
13. Афанасьев Ю.В. Феррозондовые приборы. – Л.: Энергоатомиздат, 1986. – 188 с.
14. Ripka, P. *Magnetic Sensors and Magnetometers.* – Boston: Artech house, 2000. – 494 p.
15. Miroshnikov, V.V., Petruchshenko, T.V., Dyadichev, V.V. Multiunit Ferroprobe Converters as an Effective Method of the Nondestructing Magnetic Inspection. In: Radionov, A.A., Gasiyarov, V.R. (eds) *Proceedings of the 8th International Conference on Industrial Engineering. ICIE 2022. Lecture Notes in Mechanical Engineering.* Springer, Cham. – 2023. – pp. 259–268. DOI 10.1007/978-3-031-14125-6_26.
16. Брякин И.В., Бочкарев И.В., Гунина М.Г. Система оперативного контроля технического состояния электрических кабелей // *Проблемы автоматизации и управления.* – 2018. – № 1 (34). – С. 55–63.
17. Bryakin I.V., Bochkarev I.V., Khramshin R.R. Two-Axis Fluxgate Magnetometer with a New Principle of Excitation // *International Russian Automation Conference (RusAutoCon).* – 2020. – Pp. 693 – 698. DOI 10.1109/RusAutoCon49822.2020.9208228.
18. Bochkarev I. V., Bryakin I. V., Khramshin V. R. Ferroprobe Magnetometer with Preset Excitation Field Induction Mode. 2021 International Ural Conference on Electrical Power Engineering (UralCon). – 2021. – pp. 31–36. DOI: 10.1109/UralCon52005.2021.9559463.
19. Брякин И.В., Бочкарев И.В. Измерительный датчик для систем неразрушающего контроля стальных канатов // *Электротехнические системы и комплексы.* – 2017. – № 2 (35). – С. 49–54. [https://doi.org/10.18503/2311-8318-2017-2\(35\)-49-54](https://doi.org/10.18503/2311-8318-2017-2(35)-49-54).
20. Бехер С. А., Бобров А. Л. Основы неразрушающего контроля методом акустической эмиссии. – Новосибирск: Изд-во СГУПС, 2013. – 145 с.
21. Далин М.А., Генералов А.С., Бойчук А.С., Ложкова Д.С., Основные тенденции развития акустических методов неразрушающего контроля // *Авиационные материалы и технологии.* – 2013, № 1 (26). – С. 64–69.
22. Шавров В. Г., Бучельников В. Д., Бычков И. В. Связанные волны в магнетиках: монография. – Москва: Физматлит, 2019. – 476 с.
23. Васильев А. Н., Бучельников В. Д., Гуревич С. Ю. Электромагнитное возбуждение звука в металлах. – Челябинск: Изд-во ЮУрГУ, 2001. – 339 с.

24. Бычков И. В., Кузьмин Д. А., Бучельников В. Д., Шавров В. Г. Влияние взаимодействия подсистем на динамические свойства магнетиков. – М.: Физматлит, 2016. – 176 с.
25. Прокофьев К.В., Шульгинов А.А., Гуревич С.Ю. Структура электромагнитного поля, наведенного над поверхностью ферромагнитного полупространства при падении сферического фронта акустической волны // Вестник ЮУрГУ. – 2002. – № 3. – С. 50–55.
26. Faria J. A. B. *Electromagnetic Foundations of Electrical Engineering*. – John Wiley & Sons, Ltd. 2008. – 420 p.

УДК 621.316.946:620.179.16

С.Н. Верзунов, verzunov@hotmail.com

Институт машиноведения, автоматики и геомеханики НАН КР

КОМПЛЕКСНЫЙ АКУСТО-ДИЭЛЕКТРОМЕТРИЧЕСКИЙ НЕРАЗРУШАЮЩИЙ МОНИТОРИНГ УСТРОЙСТВ И ОПОР ЛЭП С ПРИМЕНЕНИЕМ ВСТРОЕННОГО ПЕРИФЕРИЙНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Приведен систематический обзор современных технологий неразрушающего контроля (НК) высоковольтных объектов, в котором впервые объединены три подхода: акустическая эмиссия, диэлектрическая диагностика и встроенный периферийный искусственный интеллект (edge-AI). В качестве примеров таких объектов рассмотрены газоизолированные распределительные устройства (ГИРУ) напряжением 10–45 кВ и композитные/железобетонные опоры линий электропередачи (ЛЭП). Проанализированы данные из рецензируемых публикаций и нескольких открытых наборов сигналов (PD-Loc, VSB и др.). Рассмотрены актуальные алгоритмы обработки — сверточные нейронные сети (CNN), байесовское объединение многомодальных данных и квантованные модели для edge-AI. Сравнены функции ведущих промышленных систем (EA UltraTEV, Rugged CPM601, OMICRON PARADIMO) и предложена архитектура комплексного акусто-диэлектрического прибора; показано, что мультимодальный анализ способен снизить долю ложных тревог при обнаружении частичных разрядов. Обоснована практическая ценность комплексного мониторинга для перехода к прогнозно-ориентированному обслуживанию подстанций и опор ЛЭП, уменьшения утечек элегаза (SF_6) и повышения механической надежности конструкций.

Ключевые слова: неразрушающий контроль (НК); частичные разряды (ЧР, Partial Discharge); газоизолированные распределительные устройства; композитные и железобетонные опоры линий электропередачи; акустическая эмиссия и ультразвуковая диагностика; диэлектрическая спектроскопия; байесовское слияние данных; периферийные вычисления (edge computing); машинное обучение и искусственный интеллект; прогнозно-ориентированное обслуживание.

1. Введение

Надежность распределительного высоковольтного оборудования напрямую влияет на бесперебойность электроснабжения. По статистике, до 40% внеплановых отключений в распределительных сетях связаны с отказами оборудования подстанций, и во многих случаях причиной являются частичные разряды (ЧР) в изоляции [1]. Так, например, газоизолированные распределительные устройства (ГИРУ) на напряжение 10–45 кВ используют элегаз (SF_6) в качестве изоляционной среды. SF_6 — чрезвычайно мощный парниковый газ с потенциалом глобального потепления ~23 900 раз выше CO_2 и атмосферным сроком жизни около 3200 лет [2]. Поэтому предотвращение утечек SF_6 и отказов ГИРУ имеет не только экономическое, но и экологическое значение. Кроме того, композитные и железобетонные опоры линий электропередачи (ЛЭП) также требуют внимания: со временем в них накапливаются трещины, увлажнение, коррозия арматуры, что снижает механическую прочность конструкции.

Традиционные методы контроля — плановые осмотры, тепловизионный контроль, измерение тангенса δ (для изоляции), простукивание опор — обладают ограниченной чувствительностью и субъективностью. Для раннего выявления дефектов изоляции (например, ЧР, внутренние повреждения) и деградации материалов необходимы инновационные методы неразрушающего контроля. Перспективным подходом является одновременное использование ультразвуковой акустической диагностики и диэлектрических измерений, объединенных в одном приборе с поддержкой алгоритмов искусственного интеллекта. Идея состоит в том, что акусто-диэлектрометрический мониторинг позволит «видеть» как электрические дефекты (частичные разряды, изменение диэлектрических

свойств), так и механические дефекты (трещинообразование, разрывы волокон, ослабление структуры) в контролируемых объектах.

В данной работе рассматривается концепция комбинированного интеллектуального акустико-электрометрического прибора, реализующего такой подход. Этот интеллектуальный прибор – edge-устройство (выполняющее вычисления на месте сбора данных), объединяющее датчики акустической эмиссии/ультразвука и диэлектрометрические датчики и использующее встроенные алгоритмы глубокого машинного обучения для анализа сигналов в реальном времени. Далее проводится обзор существующих открытых данных и научных работ, наработанных методов обработки, а также уже доступных коммерческих решений в этой области. Кроме того, обсуждаются архитектура и потенциал внедрения такого интеллектуального прибора, и обосновываются преимущества интеграции акустического и диэлектрического контроля, усиленного edge-AI, для применения в условиях реальных объектов (10-45-кВ ГИРУ, опоры ЛЭП и др.). То есть в работе предложена единая акусто-диэлектрическая платформа, способная одновременно диагностировать электрические и механические дефекты (трещинообразование, увлажнение композитных/железобетонных опор ЛЭП). В опубликованных системах мониторинга эти задачи до сих пор решались отдельно: ЧР-комплексы контролируют только изоляцию, а структурную прочность опор оценивают другими методами. Кроме того, разработана edge-архитектура с аппаратным разделением задач: FPGA-ядро выполняет БПФ/вейвлет-анализ и формирует фазово-разрешенные диаграммы ЧР «на лету», тогда как встроенный нейропроцессор запускает компактные CNN-модели и байесовское объединение информации с нескольких сенсоров без обращения к облачной инфраструктуре. В литературе подобное распределение еще не описано.

2. Методы

Акустические методы диагностики. Акустический контроль включает использование ультразвуковых волн и акустической эмиссии для обнаружения дефектов. В контексте электрооборудования наиболее показателен ультразвук для выявления частичных разрядов: разряд в газовой или твердой изоляции генерирует высокочастотный звук (ультразвук), который может улавливаться датчиками. Например, портативные датчики ультразвука широко применяются для выявления коронного разряда и поверхностных ЧР на открытых токоведущих частях. Известно, что компания EA Technology разработала ручные детекторы типа UltraTEV, сочетающие ультразвуковой микрофон и датчик электромагнитных импульсов. В частности, прибор UltraTEV Detector² оснащен двумя сенсорами: ультразвуковой для фиксации поверхностных ЧР (в диапазоне выше слышимого звука) и емкостной датчик транзитных напряжений на корпусе (TEV) для регистрации внутренних ЧР [3].

Такое устройство позволяет сразу распознавать как поверхностные разряды, так и внутренние дефекты в выключателях и шкафах ГИРУ. Ультразвук применяется и для локализации источников разрядов. Например, массив из трех ультразвуковых датчиков, расположенных Г-образно, способен не только обнаруживать ЧР, но и определять направление на источник по разности времен прихода сигналов. В лабораторных испытаниях подобная установка показала точность локализации порядка 0,1 м при расстоянии между датчиками 0,2 м [1].

В конструкции предлагаемого интеллектуального прибора предполагается использование высокочувствительного акустического сенсора – либо контактного пьезодатчика, либо микрофона для воздушного ультразвука, в зависимости от сценария. Кроме того, акустическая эмиссия (АЭ) – перспективный метод контроля механических дефектов: он улавливает упругие волны, возникающие при зарождении и росте трещин в материале. Метод АЭ давно применяется для мониторинга железобетона [4] – формирующиеся микротрещины издают импульсные сигналы, которые фиксируются датчиками. В композитных опорах ЛЭП акустические датчики могут улавливать звук

разрыва волокон или слоев. Кроме того, ультразвуковые измерения можно использовать для оценки упругости материала: скорость распространения ультразвуковой волны через толщу опоры позволит судить о степени растрескивания или увлажнения. Таким образом, акустический канал интеллектуального прибора обеспечивает как раннее обнаружение ЧР в электрическом оборудовании, так и выявление трещин и иных структурных нарушений в опорах.

Диэлектрические методы диагностики. Диэлектрометрический контроль охватывает все методы, связанные с измерением электрических свойств изоляционных материалов и электромагнитных эмиссий от дефектов. В случае ГИРУ ключевую информацию дают импульсные электрические сигналы от частичных разрядов. Разряд генерирует кратковременный высокочастотный ток и электромагнитное излучение. Для их регистрации используются: высокочастотные токовые трансформаторы (ВЧТТ) на заземлении, емкостные датчики (например, связь через слой изоляции), антенны УВЧ-диапазона, TEV-датчики на корпусе и пр. Современные стационарные системы мониторинга ЧР обычно поддерживают подключение сразу нескольких типов датчиков. Так, система Rugged Monitoring CPM601-C представляет собой универсальный двухдиапазонный регистратор ЧР (КВ и УКВ), который работает с акустическими/ультразвуковыми датчиками, ВЧТТ, TEV, соединительными емкостями и УВЧ антеннами. Такое многообразие входных каналов позволяет охватить все виды частичных разрядов в разных устройствах – от ГИРУ и трансформаторов до кабельных линий [5].

В предлагаемом интеллектуальном приборе диэлектрометрический канал может быть представлен, к примеру, небольшим встроенным УВЧ-датчиком (для регистрации электромагнитных импульсов ЧР в ГИРУ) или емкостным сенсором, прикрепляемым к поверхности изоляции. Для контроля опор ЛЭП метод может принимать форму диэлектрометрии – измерения диэлектрической проницаемости или сопротивления бетона/композита. Известно, что диэлектрическая проницаемость бетона сильно зависит от влажности: наблюдается высокая корреляция между ϵ_r и содержанием влаги. Это можно использовать для косвенного определения влажности в защитном слое бетона, что важно для оценки риска коррозии арматуры [6].

Таким образом, контролируя диэлектрические параметры опоры (например, с помощью высокочастотного емкостного датчика или портативного прибора типа георадара), предлагаемый интеллектуальный прибор может выявлять увлажнение и деградацию изоляционных свойств материала опоры.

Алгоритмы обработки данных (Edge AI). Сочетание разнородных датчиков требует интеллектуальной обработки для извлечения диагностической информации. В последние годы в электроэнергетике активно применяются методы машинного обучения для распознавания шаблонов частичных разрядов, а также для оценки состояния оборудования. Классические подходы основывались на методах поверхностного обучения и пороговом анализе, например фазово-разрешенные диаграммы ЧР (PRPD) или статистические параметры импульсов [7]. Однако такие методы требовали участия экспертов и чувствительны к помехам [7]. Глубокие нейронные сети (глубокое обучение) позволяют автоматизировать этот процесс. Особенно эффективно зарекомендовали себя сверточные нейросети (CNN) для анализа временных рядов: они способны самостоятельно идентифицировать характерные паттерны по сигналу разряда, выделяя скрытые закономерности [7]. Прямое применение глубокого обучения к задаче обнаружения ЧР уже демонстрирует отличные результаты. Например, в соревновании VSB Power Line Fault Detection (публичный датасет частичных разрядов, собранный Техническим университетом Острова) методы с глубоким обучением достигли высоких показателей и заняли лидирующие места [7]. Этот датасет включает более 8700 сигналов с метками наличия повреждения изоляции на высоковольтной линии 22 кВ, и стал открытым бенчмарком для алгоритмов обнаружения ЧР [7]. Другой пример – открытый набор PD-Loc на IEEE DataPort, содержащий разнообразные акустические сигналы (импульсы, шум, реально

зарегистрированные ЧР), собранные с помощью прецизионной 32-канальной решетки микрофонов [8]. PD-Loc предназначен для отладки алгоритмов локации источников разрядов и служит источником данных для исследований по акустическим методам мониторинга. Наличие таких открытых данных значительно облегчает обучение нейросетей интеллектуального прибора для различных задач (классификация типа дефекта, фильтрация помех, определение местоположения дефекта и т.д.).

Edge-архитектура прибора подразумевает, что тяжелые вычисления выполняются на месте, на самом устройстве, без необходимости постоянно передавать большой объем сырого сигнала в облако. Это предъявляет требования к эффективности алгоритмов – часто применяются компактные модели или специальные методы, как знание-дистилляция и квантование сетей. В литературе предлагаются гибридные схемы: например, в работе [9] реализована облачно-периферийная система, где предварительная обработка и снижение размерности признаков выполняется на краю (edge), а обучение глубоких моделей происходит в облаке; затем обученная модель выгружается обратно на edge-устройства для работы в реальном времени [9]. Подобный подход позволяет регулярно обновлять интеллект приборов на основе собираемых данных. В контексте интеллектуального прибора можно предусмотреть, что сеть из таких приборов будет собирать телеметрию с объектов, периодически отправлять обобщенную информацию в центр (облако) для дообучения моделей и получать обновленные веса нейросети. Но основная задача – моментальное выявление дефекта на месте – решается за счет локального ИИ. Например, сразу на устройстве может работать сверточная сеть, различающая характер акустического импульса (напряженный звук трещины vs. фоновый шум) или классифицирующая форму ЧР-импульса в ВЧ-сигнале (разряд по поверхности vs. внутренний дефект и т.д.).

Слияние данных и байесовский подход. Для принятия решения о состоянии объекта интеллектуальный прибор должен объединять результаты от акустических и диэлектрических сенсоров. Байесовские методы предоставляют формальный аппарат для слияния разнородной информации с учетом неопределенности. Каждое измерение (например, уровень акустической эмиссии, величина импульсного тока ЧР, диэлектрическая проницаемость материала) может рассматриваться как признак с определенной апостериорной вероятностью дефекта. Байесовская сеть или фильтр способны объединить эти признаки и вычислить интегральную оценку состояния – например, вероятность того, что изоляция повреждена. В инженерной диагностике подобные модели применяются для повышения достоверности: один датчик может давать ложное срабатывание, но совместная вероятность двух независимых признаков существенно снижает риск ошибки.

Так, апостериорная вероятность наличия дефекта D при совместном наблюдении акустического импульса X_A и электромагнитного всплеска X_E определяется по правилу Байеса:

$$P(D|X_A, X_E) = \frac{P(X_A|D)P(X_E|D)P(D)}{P(X_A, X_E)}.$$

В нашем же случае комбинация акустического и электрического «зрения» позволяет более надежно выявлять дефекты. Например, ЧР проявляется как одновременно электромагнитный всплеск и акустический щелчок – фиксация обоих сигналов даст почти стопроцентную уверенность, тогда как каждый по отдельности мог быть вызван помехой (электромагнитной или акустической). Аналогично для опоры ЛЭП: резкий скачок акустической эмиссии, сопровождающийся изменением диэлектрического отклика материала, укажет на трещину, в которую проникла влага. Тем самым объединение данных с разных сенсоров, поддерживаемое ИИ, повышает чувствительность и специфичность диагностики. Данные литературы подтверждают эффективность таких подходов – например, совмещение ультразвукового метода с оптическим (камера) уже применялось для идентификации конкретного дефектного изолятора после акустической локализации ЧР [1]. В интеллектуальном приборе заложена возможность расширения: помимо двух основных каналов (акустика и диэлектрика), могут интегрироваться и другие – например, датчики

температуры, влажности, вибрации – а edge-алгоритмы ИИ не будут проводить многофакторный анализ.

Результаты и обзор решений

Открытые данные и современные алгоритмы. Рассмотренные методы уже опробованы на практике и в исследованиях. Открытые наборы данных позволили исследователям обучить и проверить ИИ-алгоритмы диагностики. Так, на датасете VSB (разряды на ЛЭП) сверточные сети достигли высокого показателя $MCC \approx 0.63$, уверенно различая сигналы поврежденной изоляции [10]. Для сравнения моделей использован показатель Мэттьюса (MCC):

$$MCC = \frac{TP \cdot TN - FP \cdot FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

где TP , TN , FP , FN — истинно-положительные, истинно-отрицательные, ложноположительные и ложноотрицательные решения соответственно.

Авторы той работы отмечают, что их подход занял 4-е место на финальном тестировании среди десятков решений [7]. Набор PD-Loc стал базой для разработки методов акустической локации ЧР по сигналам с 32-канального массива микрофонов [8]. Его появление значительно продвинуло вперед исследование алгоритмов 3D-пеленгации дефектов по звуку. Помимо академических данных, ценные результаты дают и полевые испытания. К примеру, в эксперименте литовских инженеров ультразвуковая установка успешно зафиксировала ЧР на расстоянии до 30 м в открытом распреустройстве и правильно определила дефектный ввод трансформатора, используя комбинированную обработку сигналов и классификатор SVM [1]. Эти результаты подтверждают работоспособность акустических методов в реальных условиях подстанций.

Существующие коммерческие решения. На рынке уже присутствует оборудование, показанное в таблице 1, частично реализующее описанные подходы.

Таблица 1 – Сравнительные характеристики коммерческих систем мониторинга частичных разрядов и предлагаемого акусто-диэлектрического комплекса

Система	Форм-фактор / установка	Измерительные каналы (✓ — встроено • — доступно как опция)	Встроенный ИИ / edge-аналитика	Диапазон применимости	IP-класс	Ключевые возможности	Основные ограничения
EA UltraTEV Plus ²	Ручной портативный прибор «обходного» контроля	УЗ-микрофон ✓ TEV-датчик ✓	Только пороговая логика; без нейросетей	КРУ, ГИРУ 6–35 кВ	IP54	Быстрый скрининг ЧР; индикация «зел / жёлт / красн»	Нет стационарной работы; не анализирует мех. дефекты
Rugged Monitoring CPM601-C	Стационарный модуль (до 8 каналов)	HFCT ✓ • УВЧ-антенна ✓ • АЭ датчик •	Правила + спектральные пороги; ИИ отсутствует	Трансформаторы, GIS, кабели 6–400 кВ	IP65	Суточный тренд ЧР; IEC 61850, MQTT	Нет диэлектрометрии; нет классификации по типу дефекта
OMICRON PARADIMO 100	Стационарный UHF-блок для GIS/GIL	УВЧ-антенны ✓ (1–2 ГГц)	Да — CNN-классификатор PD-паттернов	GIS/GIL > 72 кВ	IP66	Автоклассификация ЧР; веб-GUI; оптоволоконная сеть узлов	Мониторит только электрические дефекты, без акустики
Предлагаемый комплекс	Портативный и стационарный режим	УЗ/АЭ ✓ UHF / HFCT ✓ Диэлектрометрия ✓	Да — NPU 0.5 TOPS, байес. влияние	ГИРУ 10–45 кВ + опоры ЛЭП	IP65 (портативн.) / IP67 (стац.)	Одновременный контроль ЧР и трещин; автономный анализ; Wi-Fi 6, LTE-M1, IEC 61850	Прототип; требуется калибровка под разные материалы

Компания EA Technology (Великобритания) предлагает портативные приборы серии UltraTEV для экспресс-обследования распределительного устройства. UltraTEV Plus², например, способен одновременно измерять уровень ультразвука и импульсы TEV, выдавая оператору индикацию степени ЧР-активности [3]. Он помогает эксплуатационному персоналу быстро выявить ячейки ГИРУ с подозрением на частичные разряды (зелёный/жёлтый/красный индикатор по уровню PD)[3], а также на слух различить характерный треск разряда в ультразвуковом диапазоне [3]. Однако такие приборы предназначены для периодического ручного контроля и зависят от квалификации оператора. Для непрерывного мониторинга существуют стационарные системы. Rugged Monitoring (Канада) выпускает систему CPM601, способную круглосуточно снимать и анализировать ЧР-сигналы от нескольких датчиков (до 8 каналов) в высокочастотном и ультра-высокочастотном диапазонах [5]. Это промышленное устройство, рассчитанное на установку непосредственно на объекте (степень защиты IP65) и интеграцию в АСУТП предприятия по стандартным протоколам (Modbus, MQTT, IEC 61850 и др.)[5]. В CPM601 заложены алгоритмы фильтрации помех и накопления статистики, однако о применении нейросетей не заявлено – пороговая обработка и передача данных на верхний уровень. Компания OMICRON (Австрия) предложила новейшую систему PARADIMO 100, ориентированную на мониторинг ГИРУ и газовых шин (GIL). Особенность PARADIMO – встроенный модуль edge-вычислений и интеллектуального анализа: прибор автоматически детектирует и классифицирует тип дефекта изоляции и формирует тревожные оповещения для службы эксплуатации [11]. Фактически, PARADIMO 100 является примером специализированного edge-AI устройства для ЧР-мониторинга ГИРУ. Он подключается к предустановленным УВЧ-антеннам в корпусе ГИРУ, охватывая широкий диапазон частот для уверенного обнаружения сигналов ЧР даже на фоне помех [12]. Несколько таких узлов могут объединяться по оптоволоконной сети, покрывая всю подстанцию и передавая данные на центральный сервер с веб-интерфейсом [11]. Таким образом, возможности PARADIMO во многом превосходят функции интеллектуального прибора в части диагностики ЧР в элегазовом оборудовании.

Однако ни одно из перечисленных решений не нацелено на одновременный контроль электрических и механических параметров. Системы типа PARADIMO и CPM601 концентрируются исключительно на частичных разрядах и состоянии электрической изоляции. Контроль же состояния опор ЛЭП (механической прочности) обычно осуществляется другими средствами – например, периодическим инструментальным контролем прочности бетона, измерением вибраций опоры при ветровой нагрузке или визуальным осмотром. В этом смысле концепт интеллектуального прибора является уникальным интегрированным подходом: один прибор, оснащенный мультимодальными сенсорами и AI-аналитикой, способен обслуживать две задачи одновременно – мониторинг электроизоляции и диагностику конструкции.

Возможности интеллектуального прибора и предлагаемая архитектура. На рисунке 1 представлена структурная схема прибора, в которой выделены восемь взаимосвязанных подсистем.

1. Акустический модуль – принимает импульсы акустической эмиссии или посылает/принимает ультразвуковые сигналы. Состоит из пьезодатчика (либо УЗ-передатчика-приемника), предусилителя на 40 дБ и быстрого коммутатора режима прием/передача.
2. Диэлектрометрический модуль – регистрирует электромагнитные всплески частичных разрядов и измеряет диэлектрические параметры материала. Включает HFCT-вход, малошумящую UHF-антенну либо контактный ϵ -электрод, а также полосовой фильтр с усилителем.
3. Модуль аналоговой обработки – универсальный фронт-энд: мультиплексирует датчики, отфильтровывает помехи, формирует синхронные триггеры; оцифровка выполняется парой независимых АЦП.

4. Модуль цифровой обработки – ядро вычислений: четырехъядерный SoC Cortex-A55 и FPGA-блок, который аппаратно рассчитывает БПФ/вейвлет-преобразования и формирует фазово-разрешенные диаграммы ЧР.
5. Модуль ИИ – встроенный нейропроцессор производительностью 0,5 TOPS, реализующий сверточные сети и байесовское слияние данных в реальном времени.
6. Модуль памяти – eMMC 16 ГБ и съемная μ SD до 128 ГБ для круглосуточного буфера «сырых» сигналов и хранения моделей.
7. Модуль безопасности – TPM 2.0 / Secure Element, отвечающий за защищенную загрузку и аппаратное шифрование трафика.
8. Модуль питания и управления – промышленный DC/DC 24/48 В $\rightarrow$ 5 В/3,3 В, резервный Li-ion аккумулятор 12 Вт·ч с MPPT-зарядкой и служебный микроконтроллер-диспетчер со сторожевым таймером.
9. Коммуникационный модуль – проводной Gigabit Ethernet с PoE и беспроводные интерфейсы Wi-Fi 6, LTE-M1, BLE 5.3; поддерживает протоколы OPC UA и IEC 61850 для интеграции в цифровые подстанции.

Такое портативное, но функционально насыщенное устройство обеспечивает полный цикл «датчик $\rightarrow$ фильтрация $\rightarrow$ ИИ-анализ $\rightarrow$ передача результата», позволяя проводить комплексный неразрушающий контроль на месте установки оборудования без внешних вычислительных ресурсов.

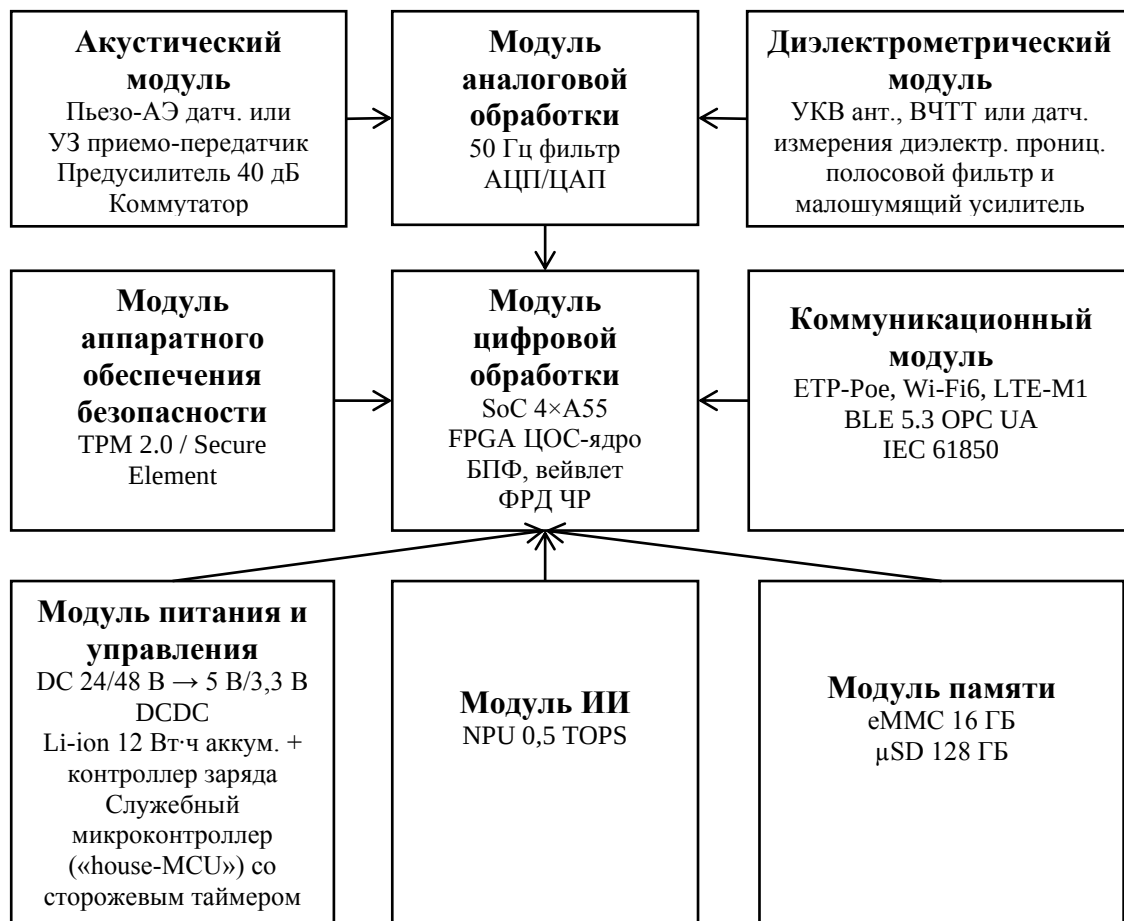


Рисунок 1 – Структурная схема интеллектуального комплекса на базе периферийного ИИ

В полевых условиях интеллектуальный прибор может применяться двумя способами: передвижной контроль и стационарный мониторинг. В первом случае прибор используется инспектором: например, при обходе оборудования инженер прикрепляет магнитно/клеевым

креплении прибор к корпусу оборудования или к опоре ЛЭП, после чего запускает режим сканирования. Прибор возбуждает ультразвуковую волну и замеряет отклик материала, прослушивает акустическую эмиссию за определенный интервал, одновременно измеряет уровни ЧР в электросигналах. По завершении цикла в течение нескольких минут прямо на месте выдаются диагностические показатели: степень ЧР-активности, наличие аномальных акустических событий (например, «обнаружен звук трещины, рекомендуется дополнительная проверка опоры»), оценка влажности бетона и т.п. В стационарном варианте несколько приборов могут быть установлены постоянно – например, один на каждую опору секции ЛЭП или на каждый отсек распределительного устройства. Тогда интеллектуальный прибор выступает как узел системы предиктивной диагностики: непрерывно отслеживает состояние и в случае превышения порогов (или обнаружения характерного паттерна, распознанного ИИ) отправляет тревогу на пульт эксплуатационников.

Архитектурно интеллектуальный прибор мог бы использовать обработку сигналов в реальном времени: аналоговые сигналы с датчиков оцифровываются АЦП высокой частоты (для ЧР – ≥ 100 Мвыб/с, для ультразвука – в диапазоне МГц при импульсном прозвучивании), затем предобрабатываются (фильтрация, усиление, декомпозиция). Выделенные признаки (спектры, огибающие, фазовые распределения разрядов и др.) подаются на вход встроенной нейросети, которая выдает классификацию или регрессионную оценку состояния. Например, сеть может классифицировать тип ЧР (поверхностный, внутренний, корона) по форме импульса – аналогично тому, как PARADIMO отличает дефекты в GIS [12]. Другая модель может оценивать степень поврежденности бетона по сочетанию признаков (уровень АЭ, диэлектрическая проницаемость) – фактически предсказывать остаточный ресурс или необходимость ремонта. Все эти вычисления выполняются автономно на процессоре устройства, что соответствует концепции Edge AI – интеллектуализации приборов на местах обслуживания.

Следует отметить, что на рынке уже появляются решения с частичным перекрытием функционала предлагаемого интеллектуального прибора. Например, компания ЕА, помимо поиска ЧР, развивает технологию мониторинга состояния деревянных опор (UltraTEV WoodPole Inspect) на основе акустического отклика при ударе. Хотя материалы и дефекты иные, принцип – анализ отклика опоры через встроенный алгоритм – схож с частью задач предлагаемого интеллектуального прибора. Тем не менее комбинирование в одном приборе контроля высоковольтной изоляции и механической прочности опор является новым шагом. Главным преимуществом такого объединения станет комплексная оценка состояния узлов энергосистемы. Например, при диагностике разъединителя 35 кВ, смонтированного на опоре, интеллектуальный прибор сможет одновременно указать состояние его элегазовой изоляции (есть ли ЧР в приводе, утечка газа) и состояния опоры (нет ли трещин в зоне крепления). Это особенно ценно, учитывая, что повреждения разных подсистем часто взаимосвязаны (разряд мог закоптить изолятор и ослабить диэлектрическую прочность; механическое повреждение опоры могло привести к перекосу оборудования и повышенной напряженности поля и т.п.).

Обсуждение

Практическая применимость и внедрение. Применение edge-AI-приборов, подобных предлагаемому, в энергетической инфраструктуре открывает новые возможности для предиктивного обслуживания. По сравнению с существующими подходами, комплексный интеллектуальный прибор предлагает инженерам простое в использовании решение «двух в одном», снижающее потребность в нескольких разных приборах и экспертной расшифровке данных. Внедрение такой системы может происходить поэтапно. На первом этапе – опытная эксплуатация: несколько устройств устанавливаются на пилотных объектах (например, на самой загруженной 35-кВ подстанции и на участке ЛЭП с имеющейся историей дефектов). С помощью открытых и накопленных данных обучаются модели обнаружения дефектов, настроены пороги чувствительности под реальные условия (электромагнитные помехи в РУ, фоновые шумы на ЛЭП – ветер, дождь и пр.). Далее интеллектуальный прибор

интегрируется в существующие системы техобслуживания: данные от него могут передаваться в SCADA или специализированный программный комплекс. В случае тревоги диспетчер получит уведомление с рекомендациями.

Важно подчеркнуть, что периферийный ИИ означает автономность и скорость. Даже при сбоях связи или отсутствии высокоскоростного канала прибор на месте способен сам принять решение и сигнализировать локально (световая сигнализация, звуковой сигнал или передача по резервному каналу SMS). Это особенно ценно для удаленных ЛЭП: опоры, оборудованные интеллектуальным прибором, могли бы по радиоканалу отправлять сигналы непосредственно ремонтной бригаде при обнаружении сильной трещины (например, после урагана).

Ограничения и дальнейшие направления. Естественно, описываемая система имеет свои технические вызовы. Комбинированный прибор должен быть очень помехоустойчивым: электроразряды генерируют широкий спектр частот, а ультразвук может ложноположительно срабатывать на внешние факторы (дождь, вибрация от транспорта). Решение – тщательная фильтрация и алгоритмы на основе ИИ, обученные отличать помехи от значимых сигналов [7]. Кроме того, устройство должно отвечать высоким требованиям по климатическому и механическому исполнению (для наружной установки на опорах – широкий диапазон температур, защита от влаги IP65+, виброустойчивость). Питание может быть реализовано от литиевых аккумуляторов с солнечной подзарядкой в случае автономных узлов на ЛЭП. Еще одна задача – калибровка. Акустический контакт с разными материалами (сталь корпуса, композит, бетон) требует адаптивных настроек или разных видов датчиков. Возможно, интеллектуальный прибор будет иметь сменные насадки/датчики для различных поверхностей либо автоматическую подстройку усиления под коэффициент отражения сигнала.

В плане алгоритмов дальнейшее развитие видится в расширении библиотек обнаруживаемых дефектов. Обучение на большем количестве эталонных данных (например, добавление данных из Scientific Reports исследований, где опубликованы формы сигналов различных дефектов) повысит надежность классификации. Интеграция байесовского слияния позволит выдавать обобщенный индекс состояния, понятный конечному пользователю – например, процент от износа или риск отказа в баллах. Такой интегральный подход облегчит принятие решений о ремонте.

Выводы

Выполненный обзор демонстрирует, что сочетание ультразвуковых и диэлектрических методов контроля, подкрепленное алгоритмами искусственного интеллекта, представляет собой мощный инструмент для диагностики состояния высоковольтного оборудования. Edge-AI-поддерживаемая акусто-диэлектрическая система способна обнаруживать опасные дефекты изоляции (частичные разряды, утечки элегаза) и ранние признаки деградации конструкций (трещины, увлажнение) до того, как они приведут к аварии. Примером служат современные устройства: от портативных детекторов EA Technology с двойными датчиками до edge-комплексов типа OMICRON PARADIMO 100, автоматически классифицирующих дефекты GIS [11]. Концептуальный прибор развивает эти идеи дальше, предлагая унифицированное решение для обслуживания как электрической, так и механической подсистем энергоинфраструктуры.

Основные преимущества подхода предлагаемого прибора заключаются в комплексности диагностики и оперативности. Комбинация двух физических методов повышает достоверность контроля и расширяет охват выявляемых дефектов. Встроенный интеллект на уровне прибора (edge) обеспечивает мгновенный анализ и выдачу рекомендаций персоналу без необходимости длительной расшифровки записей. Применение таких систем в масштабах энергокомпаний позволит перейти от реактивного ремонта к прогнозированию отказов, что снизит затраты на аварийные простои и повысит безопасность. Кроме того, предотвращение крупных аварий в элегазовом оборудовании поможет сократить утечки SF₆ и соответствующий экологический ущерб.

В заключение: акусто-диэлектрометрический мониторинг с edge-AI можно рассматривать как перспективное направление развития средств технического обслуживания высоковольтных сетей. Дальнейшие исследования покажут эффективность данного подхода на практике. Ожидается, что подобные интеллектуальные приборы станут неотъемлемой частью цифровой инфраструктуры электроэнергетики, обеспечивая более надежную, длительную и экологичную работу распределительных сетей.

Литература

1. Samaitis V., Mažeika L., Jankauskas A., Rekuviene R. Detection and Localization of Partial Discharge in Connectors of Air Power Lines by Means of Ultrasonic Measurements and Artificial Intelligence Models // *Sensors*. 2021. Vol. 21, № 1. P. 20. DOI: 10.3390/s21010020. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7792959/> (дата обращения: 05.05.2025).
2. Blackman J., Averyt M., Taylor Z. SF₆ Leak Rates from High Voltage Circuit Breakers – U.S. EPA Investigates Potential Greenhouse Gas Emissions Source // *Proc. 2006 IEEE Power Engineering Society General Meeting*. Montréal, 18–22 Jun 2006. DOI: 10.1109/PES.2006.1709084. URL: https://www.epa.gov/system/files/documents/2022-05/leakrates_circuitbreakers.pdf (дата обращения: 05.05.2025).
3. EA Technology. UltraTEV® Detector²: Hand-Held Dual-Sensor Partial Discharge Detector [Электронный ресурс]. 2024. URL: <https://eatechnology.com/solutions/partial-discharge-solutions/partial-discharge-detection/ultratev-detector/> (дата обращения: 05.05.2025).
4. Ohtsu M., Isoda T., Tomoda Y. Acoustic Emission Techniques Standardized for Concrete Structures // *Journal of Acoustic Emission*. 2007. Vol. 25. P. 21–28. URL: <https://www.ndt.net/article/jae/papers/25-021.pdf> (дата обращения: 05.05.2025).
5. Rugged Monitoring. CPM601-C Dual-Frequency Partial Discharge Monitor [Электронный ресурс]. 2024. URL: <https://www.ruggedmonitoring.com/product/cpm601-c/> (дата обращения: 05.05.2025).
6. Jacobs L.J., Kurtis K.E., Sherman R.J., Burney D.C. Recommendations for Nondestructive Testing (NDT) of Concrete Components for Performance-Based Specifications. Final Rep. FHWA-GA-22-2015. Atlanta: Georgia DOT, 2022. 118 с. URL: https://rosap.ntl.bts.gov/view/dot/64475/dot_64475_DS1.pdf (дата обращения: 05.05.2025).
7. Michau G., Hsu C-C., Fink O. Interpretable Detection of Partial Discharge in Power Lines with Deep Learning // *Sensors*. 2021. Vol. 21, № 6. P. 2154. DOI: 10.3390/s21062154. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8003486/> (дата обращения: 05.05.2025).
8. Chelmiah E.T., Madigan C.D., Kavanagh D.F. Partial Discharge – Localisation (PD-Loc) Dataset [Электронный ресурс]. IEEE DataPort, 2024. DOI: 10.21227/yu7g-2p79. URL: <https://ieee-dataport.org/open-access/partial-discharge-localisation-pd-loc-dataset> (дата обращения: 05.05.2025).
9. Jia Z., Fan S., Wang Z., Shao S., He D. Partial Discharge Defect Recognition Method of Switchgear Based on Cloud-Edge Collaborative Deep Learning // *Scientific Reports*. 2025. Vol. 15. Art. 10956. DOI: 10.1038/s41598-024-81478-9. URL: <https://www.nature.com/articles/s41598-024-81478-9> (дата обращения: 05.05.2025).
10. VSB Power Line Fault Detection Dataset [Электронный ресурс]. Kaggle, 2019. URL: <https://www.kaggle.com/competitions/vsb-power-line-fault-detection> (дата обращения: 05.05.2025).

11. Partial Discharge Monitoring System // PAC World Magazine. 2024. Issue 68. URL: <https://www.pacw.org/partial-discharge-monitoring-system> (дата обращения: 05.05.2025). <https://www.pacw.org/partial-discharge-monitoring-system>
12. OMICRON Energy. PARADIMO 100 – Ultra-High-Frequency Partial Discharge Monitoring System for GIS and GIL [Электронный ресурс]. 2025. URL: <https://www.omicronenergy.com/en/products/paradimo-100/> (дата обращения: 05.05.2025).

С.М. Насирдинова, В.И. Саньков, Н. Дегембаева
Кыргызский Государственный Технический Университет им. И. Раззакова

ИССЛЕДОВАНИЕ СОЛНЕЧНОЙ СИСТЕМЫ ТЕПЛОСНАБЖЕНИЯ СЕЗОННОГО АККУМУЛИРОВАНИЯ ТЕПЛА ДЛЯ УЛУЧШЕНИЯ ЭКОЛОГИЧЕСКОЙ ОБСТАНОВКИ

В работе рассматриваются экологические факторы, влияющие на здоровье населения, и предлагаются методы их устранения с применением возобновляемых источников энергии. Исследование проводится для условий города Бишкек, Кыргызская Республика. В качестве примера расчетным путем определены выбросы одной средней образовательной школы нашей столицы, которая в отопительный период для теплоснабжения использовала уголь. В результате расчета определено количество выбрасываемых вредных веществ в атмосферу за один отопительный период. Далее нами предлагается метод решения данной проблемы. Целью работы является оценка выбросов вредных веществ при сжигании твердого топлива и методы их устранения за счет использования солнечных коллекторов и сезонного аккумулирования тепла.

Ключевые слова: солнечное теплоснабжение, сезонное аккумулирование тепла, возобновляемые источники энергии, загрязнение атмосферного воздуха, выбросы загрязняющих веществ, угольное отопление, теплоизоляция зданий, теплопотери, солнечные коллекторы, бак-аккумулятор тепла, экологическая безопасность, расчет тепловой нагрузки, Бишкек, школа №19, базальтовое волокно, коэффициент теплоотдачи, система отопления, энергоэффективность, программа расчета теплопотерь, термическое сопротивление.

Введение

Одним из серьезнейших экологических факторов, затрагивающих здоровье каждого человека, является загрязнение атмосферного воздуха.

Столица Кыргызстана г. Бишкек в последние годы каждую зиму занимает передовые места в мировом рейтинге по уровню загрязнения воздуха, и это обстоятельство создает большую экологическую угрозу для нашей страны.

Зимой этого года столица Кыргызстана вновь оказалась в топе мирового рейтинга по качеству воздуха. В декабре 2022 и январе 2023 года в среднем данные датчиков показывали не ниже 200 IQA, что является нездоровым показателем [9].

В этот период, по данным сайта контроля качества воздуха, уровень загрязнения составлял в определенных районах 430 AQI и оценивался как чрезвычайно опасный для здоровья.

В течение дня человек пропускает через свои легкие более чем два миллиона литров воздуха, совершая при этом около 20 тысяч вдохов. Почти все вещества, принесенные воздухом, попадая в легкие человека, минуя печень, растворяются в крови. Далее вредные частицы распределяются по всем органам и больше всего вредят работе сердца [1].

Существует множество успешных действий, одно из которых предлагается ниже.

Бишкек является одним из крупнейших и наиболее населенных городов в стране. В столице для теплоснабжения различных зданий, в том числе и школ, существуют 160 котельных. Из них 46 работают на твердом топливе, а остальные на газе. Кроме этого, вокруг Бишкека насчитывается 54 жилмассива, где проживают около 300 тысяч человек. Соответственно, в частном секторе люди в зимний период времени для теплоснабжения используют низкокалорийный уголь. [10].

Он меньше горит, но больше дымит. Но и уголь тоже для многих жителей жилмассивов недоступен. Вместо него используют текстильные отходы, резину, поскольку это бесплатно. Существенную роль загрязнения атмосферного воздуха, конечно же, оказывает угольное отопление, но и не только, другие факторы тоже.

С целью исследования причин экологической обстановки в Бишкеке и для предложения метода решения нами был выбран объект исследования, которым является средняя образовательная школа (СОШ).

Был проведен анализ угольных котельных среднеобразовательных школ [3]. Уголь, являясь ископаемым топливом, при сжигании выделяет огромное количество углекислого газа (CO₂) и других вредных веществ. К примеру, за 2019 год угольная котельная СШ №21

использовала 186,900 тонны угля (в перерасчете в условное топливо составляет 108403,275 т.у.т.), что естественно привело к значительным выбросам углекислого газа, загрязняя при этом атмосферу. Такая же ситуация наблюдается и в угольных котельных СШ №19 и СШ №40 [3].

Нами проведена оценка выброса вредных веществ в атмосферу СШ №19 при сжигании твердого топлива в количестве 204240,0 тонны угля за отопительный период 2022/23 года. Расчет выполнен по методике, которая предлагается в литературе [2].

Предположим, использовали местный сулюктинский уголь, у которого следующие теплотехнические характеристики:

- низкая теплота сгорания сулюктинского угля — $Q_H = 18.4$ МДж/кг;
- зольность угля (на рабочую массу) $A = 17\%$;
- содержание серы (на рабочую массу) $S = 0.7\%$.

Согласно расчетам, расход угля в самый холодный месяц потребляется 2,2 тонны угля в день с учетом продолжительности отопительного периода около 165 дней, тогда в среднем за месяц потребляется для отопления 37,14 тонны.

При сжигании твердого топлива в атмосферу от котельной выбрасываются твердые частицы, диоксиды азота и серы и оксид углерода.

1) Валовой выброс твердых частиц в дымовых газах (в тоннах за отопительный период) [2]:

$$M_{\tau} = A \cdot m \cdot x \cdot \left(1 - \frac{\eta_{\tau}}{100}\right), \quad (1)$$

где A — зольность топлива в %, M — количество израсходованного топлива в год, η_{τ} — эффективность золоуловителя (≈ 97), x — безразмерный коэффициент, характеризующий долю уносимой с дымовыми газами летучей золы, зависит от топки и топлива.

Максимально разовый выброс твердых частиц в дымовых газах, г/с [2]:

$$G_{\tau} = A \cdot m' \cdot x \cdot \left(1 - \frac{\eta_{\tau}}{100}\right). \quad (2)$$

Расчет предельно-допустимых выбросов загрязняющих веществ проводится для случая максимального расхода топлива.

2) Количество оксида углерода (CO), выбрасываемого в атмосферу (г/с, тонна за отопительный период) при сжигании жидкого и твердого топлива, рассчитывают по формуле [2]:

$$M_{CO} = C_{CO} \cdot m \cdot \left(1 - \frac{q_4}{100}\right) \cdot 0.001, \quad (3)$$

где C_{CO} — выход оксида углерода при сжигании топлива, кг/т, или:

$$C_{CO} = q_3 \cdot R \cdot Q_H, \quad (4)$$

где q_3 — потери вследствие химической неполноты сгорания топлива в %.

Для угля $q_3 = 2$, R — коэффициент, учитывающий долю потери тепла вследствие химической неполноты сгорания топлива, обусловленную наличием в продуктах неполного сгорания оксида углерода, для угля $R = 1$ — теплоты, вызванной механической неполнотой сгорания топлива, для угля $q_4 = 8$ [2].

3) Расчет выбросов оксида азота:

$$M_{NO_2} = m \cdot Q_H \cdot K_{NO_2} \cdot (1 - \beta) \cdot 10^{-3}, \quad (5)$$

где: K_{NO_2} — параметр, характеризующий количество окислов азота в кг, образующихся на один ГДж тепла, $K_{NO_2} = 0.15$ кг/кДж, β — коэффициент, учитывающий степень снижения выбросов окислов азота в результате применения технических средств, $\beta = 0$ [2].

Максимально разовый выброс:

$$G_{NO_2} = m \cdot Q_H \cdot K_{NO_2} \cdot (1 - \beta) \cdot 10^{-3}, \text{ г/с.} \quad (6)$$

3) Расчет выбросов оксидов серы (SO_2):

$$M_{SO_2} = 0.02 \cdot m \cdot S \cdot (1 - \eta'_{SO_2}) \cdot x \cdot (1 - \eta''_{SO_2}), \quad (7)$$

где S — содержание серы в топливе на расчетную массу, %, η'_{so_2} — доля оксидов серы, связываемых летучей золой топлива и для прочих углей =0.1, $\eta''_{\text{so}_2} = 0.02$ для масла [2], η''_{so_2} — для оксидов серы, улавливаемых в золоуловителе, в данном случае равно нулю [2].

Максимально разовый выброс оксида серы, г/с:

$$G_{\text{SO}_2} = 0,02 \cdot m' \cdot S \cdot (1 - \eta'_{\text{SO}_2}) \times (1 - \eta''_{\text{SO}_2}). \quad (8)$$

Таким образом, при сжигании 240204 тонн угля за отопительный период, при отсутствии системы очистки продуктов сгорания, расчетные данные показывают, что за отопительный сезон выбрасывается в атмосферу 12,43 тонны экологически вредных веществ, результат которых представлен в таблице 1.

Таблица 1 — Количество вредных веществ, выбрасываемых в атмосферу

Единица измерения	SO ₂ (оксид серы)	CO	NO ₂ (оксид азота)	Твердые вещества (зола)
Тонна за отопительный период	2,57	6,91	0,56	2,39
г/с	0,17	0,469	0,038	5,35

Таким образом, если только одна школа за отопительный период выбрасывает такое количество вредных веществ, не трудно представить количество вредных веществ от всех других организаций и частного сектора вокруг столицы, которые отапливаются только углем.

Методика расчета солнечной системы теплоснабжения сезонного аккумулирования тепла

Нами предлагается метод аккумулирования тепловой энергии с использованием сезонного бака-аккумулятора тепла, и ниже приведены расчеты для ее реализации [5;7]. Этот способ можно применить не только для всех образовательных учреждений, но и для всех других организаций, где применяется для теплоснабжения уголь. Использование газа для отопления, конечно, очень привлекательно, но надо учитывать тот фактор, что газ для нас тоже импортируемое топливо, а это означает — зависимость.

Под сезонным аккумулированием тепла понимается накопление тепла в баке-аккумуляторе с помощью солнечных коллекторов вне отопительного периода с 1 апреля по 31 октября [7].

Основным параметром, определяющим потребность здания в тепловой энергии, является его тепловая нагрузка. В основном тепловая нагрузка определяется теплофизическими свойствами строительных материалов, конструкцией, объемом здания, а также климатологическими факторами, где расположено здание.

Для этой цели, разработанной ранее нами методикой, определены тепловые потери СШ №19, которая построена в 1965 году и расположена в г. Бишкеке.

Из проекта плана здания школы определены следующие параметры: расчетная высота $h=3,2$ м, расчетная общая площадь 1-го и 2-го этажей школы

$$F=2323,1 \text{ м}^2.$$

Школа двухэтажная, кирпичные стены, кровля местами металлическая, местами шиферная. В аудиториях: полы и двери деревянные с советских времен, окна—пластиковые, в вестибюле и в коридорах полы бетонные.



Рисунок 1 – Средняя образовательная школа №19

Для расчета тепловых потерь здания нами было построена расчетная схема, которая приведена на рисунке 2.

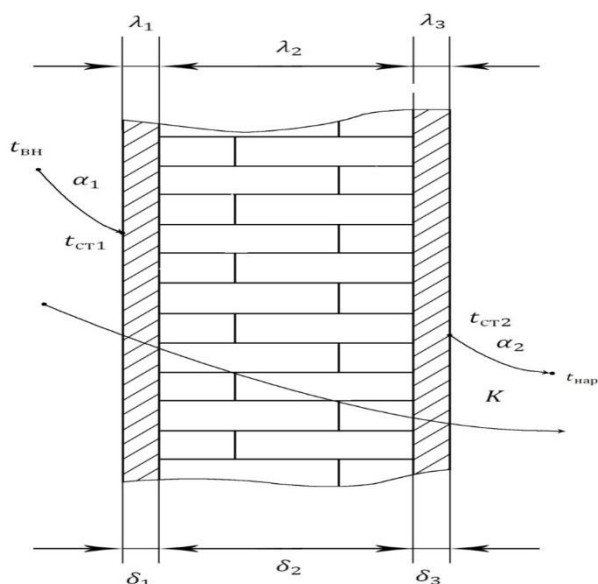


Рисунок 2 – Расчетная схема ограждающей конструкции зданий (фрагмент),

где $t_2 = t_n$ – температура наружного воздуха не постоянная; $t_{вн} = t_1$ – температура внутри здания, принимается согласно СНиП; δ_1 – толщина штукатурки из цементно-песчаного раствора с внутренней стороны стены; δ_2 – толщина кирпичной стены; δ_3 – толщина штукатурки наружной стены; λ_1 – коэффициент теплопроводности штукатурки с внутренней стороны стены; λ_2 – коэффициент теплопроводности кирпичной стены; λ_3 – коэффициент теплопроводности штукатурки с внутренней стороны стены; α_1 – коэффициент теплоотдачи внутри помещения; α_2 – коэффициент теплоотдачи снаружи помещения.

Как было нами отмечено ранее, для расчета тепловых потерь здания с учетом реального изменения среднегодовых величин температуры окружающего воздуха необходимо каждый раз определять величину коэффициента теплоотдачи α_2 снаружи помещения и осуществлять коррекцию теплотерь с учетом этих изменений. Т.е. практически задачи определения тепловых потерь здания в сравнении с классическим (холодная пятидневка при -19^0C) подходом переходит в задачу с нестационарным режимом теплопередачи.

Для решения этой задачи нами был использован следующий подход.

Величину теплотери здания определяли как:

$$Q = (t_1 - t_2) \cdot F \cdot K \cdot x \cdot y, \quad (9)$$

где $F = a \cdot b$ – поверхность стены, окна, двери и пола и т.д.; a – ширина здания, $a \neq const$; b – высота здания, $b \neq const$ задаются; x – добавки на стороны света; Y – коэффициент на две и более стен.

Коэффициент теплопередачи есть функция термического сопротивления:

$$K = \frac{1}{R_0}, \quad (10)$$

Сопротивление теплопередачи – R_0 можем определить как:

$$R_0 = \frac{1}{\alpha_1} + \sum_{i=1}^n R_{\lambda i} + \frac{1}{\alpha_2}, \quad (11)$$

где $R_{\lambda i} = \frac{\delta_i}{\lambda_i}$ – термическое сопротивление ограждающей конструкций 1-го слоя.

В данном случае поскольку температура внутри помещения постоянная, то коэффициент теплоотдачи α_1 является величиной постоянной, тогда как коэффициент теплоотдачи снаружи помещения α_2 есть функция некоторых параметров и может быть записана как:

$$\alpha_2 = \frac{Nu \cdot \lambda}{l}. \quad (12)$$

Число Нуссельта определяется по критериальному уравнению в зависимости от режима течения жидкости:

$$Nu = C(Gr \cdot Pr)^{0,25} (Pr_{ж}/Pr_{ст})^{0,25}, \quad (13)$$

где $(Pr_{ж}/Pr_{ст})^{0,25} = 1$ так как для воздуха их отношение стремится к 1; $Pr_{ст}$, $Pr_{ж}$ – критерий Прандтля соответственно для воздуха и стенки выбирается из таблицы /7/; C – постоянное число, которое зависит от режима течения жидкости; Gr – критерий Грасгофа, который определяется по формуле:

$$Gr = \frac{g\beta(t_c - t_2) l^3}{\nu^2}, \quad (14)$$

где g – скорость свободного падения, m^2/c ; β – коэффициент объемного расширения, $\beta = 1/(1+273,15)$, $1/K$; t_c – температура стенки, $^{\circ}C$; t_2 – температура воздуха, $^{\circ}C$; ν – коэффициент кинематической вязкости, который выбирается из таблицы [7]. Физические свойства воздуха по заданной температуре, которая изменяется в течение отопительного периода, тоже определяются из этой же таблицы, т.е. $\lambda = f(t)$; $Pr = f(t)$. Критерий Грасгофа определяется, предварительно задавая температурой наружной поверхности стенки t_c .

Знание коэффициента теплоотдачи α_2 и коэффициента теплопередачи K позволяет определить плотность теплового потока из уравнений:

$$q_a = K \cdot (t_1 - t_2), \quad (15)$$

$$q_b = \alpha_2 \cdot (t_c - t_2). \quad (16)$$

Теперь можем уточнить температуру стенки:

$$t_{cуточ} = t_c + q_a \frac{1}{\alpha_2}. \quad (17)$$

Эта процедура должна повторяться до тех пор, пока не выполняется условие равенства плотности теплового потока $q_a = q_b$ и условие равенства температуры наружной стенки $t_{cуточ} = t_{ci} \pm 0,01^{\circ}C$.

Данные условия обеспечивают достаточную точность расчетов при определении коэффициентов теплоотдачи α_2 и теплопередачи K . После достижения этих условий и получения окончательных значений α_2 и K определяем тепловые потери через заданную поверхность по уравнению (9).

Разработка алгоритма программы для определения тепловой нагрузки (тепловой потери) здания

Тепловые потери определяются как сумма потерь через все наружные поверхности здания на основании вышеизложенной методики расчета. Нами был разработан алгоритм программы определения тепловых потерь здания.

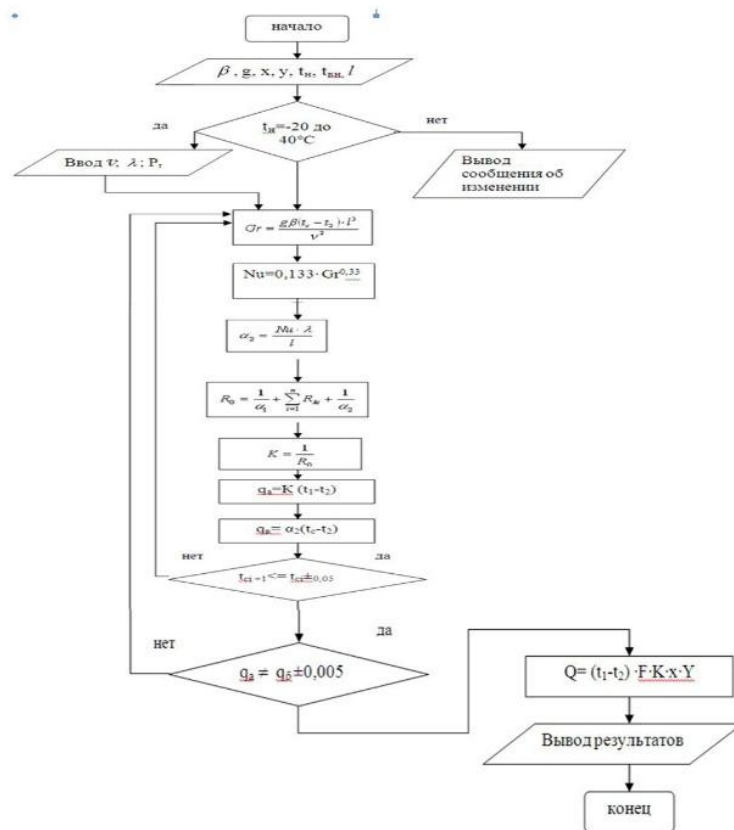


Рисунок 3 — Блок-схема программы теплотерь здания

С использованием разработанной программы исследовали влияние теплотехнических параметров средней школы на величину теплотерь.

Теплопотери

☒ Автообновление (Параметры):

Высота: 2,89

Ширина: 6,03

Площадь здания: 17,4267

Температура:

Наружного воздуха: -2,7

Внутри здания: 19

Стенок: -2,6

Добавки:

На стороны света: 1,05

Коэффициент на две и более стен: 1

Вычисления:

Alfa1: 8,7

alfa2: 87,55196

Beta: 0,00370

Gr: 546060109,75228

Nu: 106,24168

Rki: 1,94684

RO: 2,07320

K: 0,48235

t c. y.: -2,58045

Qa: 10,46689

Qb: 10,46689

Q: 191,52350

Стена

Значение	Дельта	Лямбда
ШТУКАТУРКА ЦЕМ-НО ПЕСЧ. Р-РОМ	0,02	0,76
УТЕПЛИТЕЛЬ "ISOVER"	0,05	0,037
КИРПИЧНАЯ КЛАДКА	0,38	0,7
ШТУКАТУРКА ЦЕМ-НО ПЕСЧ. Р-РОМ	0,02	0,76

Вычислить

Рисунок 4 – Интерфейс программы тепловых потерь здания средней школы

Расчеты теплопотерь здания проведены при среднемесячной температуре воздуха за отопительный период с ноября по март. Данные результатов расчета приведены в таблице 2.

Таблица 2 – Расчеты теплопотерь здания школы

	Ноябрь 2,5 °С	Декабрь -2,7 °С	Январь -5 °С	Февраль -2,9 °С	Март 4 °С	Суммарные теплопотери школы (с учетом, что школа 2-этажная), кДж за отопительный период
Изоляция дома при	Q _{пз} , Вт за месяц					
δ _{из} = 0 см	55386,7	58090,83	60956,7	58016,29	54899,24	1,554939*10 ⁹
δ _{из} = 10см	10545,95	10949,18	12115,05	11674,64	10457,59	288963469
δ _{из} = 20см	5632,6	6036,79	7202,66	6762,86	5545,2	146085690
δ _{из} = 30см	3703,9	4108,03	5273,9	4833,79	3616,44	111642728

Суммарные теплопотери здания школы определили по формуле:

$$Q_{\text{пз}}^{\delta=0} = \sum Q_{\text{пз}}^{\text{мес}} \cdot 30 \cdot (3600 \cdot 10^{-3}) \cdot 24, \text{ кДж за 5 месяцев. (17)}$$

Результаты расчета представлены в таблице 2.

По данным таблицы 2 построена диаграмма теплопотерь здания в отопительный период, которая приведена на рисунке 5.

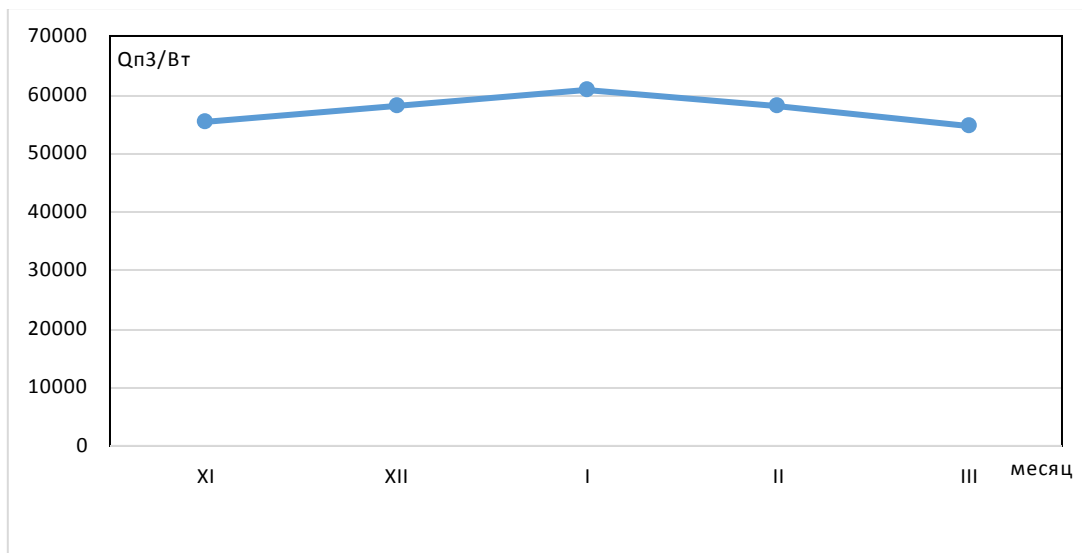


Рисунок 5 —Теплопотери без изоляции средней школы №19 за отопительный период, кДж

Отслеживание характера изменения кривой в зависимости от температуры окружающей среды показывает адекватность полученных результатов. Так, на диаграмме видно, что максимальная величина теплопотерь здания достигается в январе, что соответствует самой низкой среднемесячной температуре воздуха (-5°C).

Таким образом, можно констатировать, что разработанная методика и предложенная программа позволяют осуществить более точный расчет теплопотерь здания и тем самым способствуют правильному проектированию и выбору системы отопления.

Как известно, использование теплоизоляционных материалов для утепления здания путем облицовки внешних ограждающих конструкций существенным образом позволяет снизить теплопотери. С использованием разработанной программы нами были исследованы влияния толщины изоляционного материала и его теплотехнические свойства на величину теплопотерь.

При этом в качестве изоляционного материала было выбрано базальтовое волокно как наиболее широко используемое в практике строительства, коэффициент теплопроводности которого составляет $(0,039 \text{ Вт/м К})$.

Надо отметить, что программа позволяет исследовать теплоизоляционные материалы и других видов с разными коэффициентами теплопроводности.

Результаты расчетов представлены в виде диаграмм на рисунке (6).

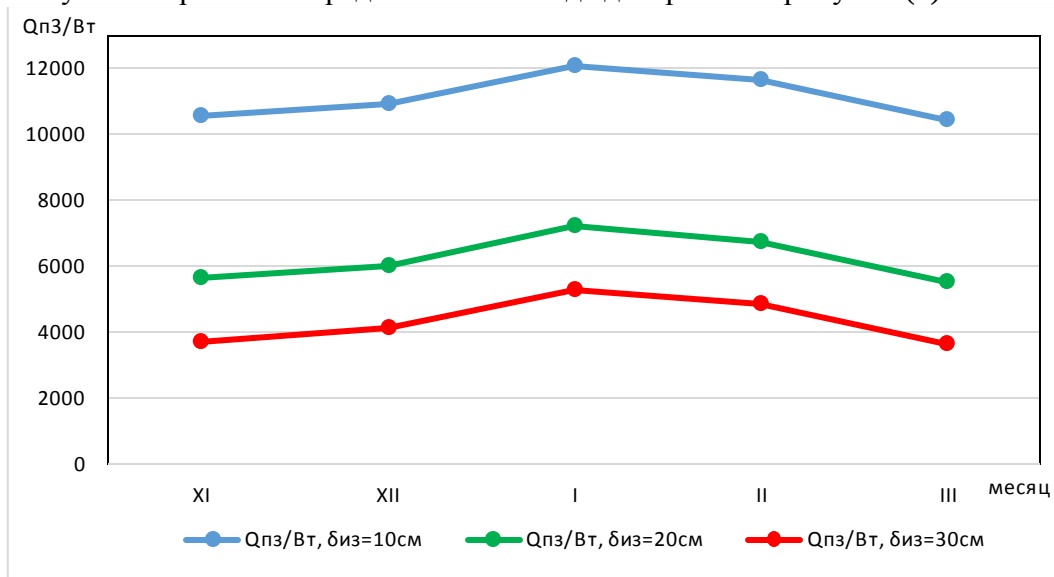


Рисунок 6 – Теплотери средней школы №19 за отопительный период (кДж) с разной толщиной изоляции

Результаты и сравнения

По результатам исследований из полученных диаграмм можно увидеть, как меняются теплотери здания с разной толщиной изоляции. В данном случае расчет теплотери здания проводился также лишь для отопительного периода времени. Как видно из полученных диаграмм, увеличение толщины материала приводит к существенному снижению теплотери. Однако это зависимость явно не линейная. Если первоначальное увеличение толщины изоляции лишь в 10 см приводит практически к снижению теплотери на 70–80%, то дальнейшее увеличение толщины до 30 см уже не дает такого эффекта. Этот вывод очень хорошо согласуется с известным положением в критически оптимальной величине толщины изоляционного материала при превышении, когда эффективность практически сводится к нулю.

Например, когда здание школы изолируем с толщиной изоляции 30 см, тогда теплотери в самое холодное время по сравнению с неизолированным зданием сокращаются в 11,5 раза. В цифровых значениях в январе теплотери неизолированного дома составляет $157,99 \cdot 10^6$ кДж в сутки (рис.5), а теплотери здания с изоляцией 30 см равны $13,67 \cdot 10^6$ кДж в сутки.

Здание без изоляции в это же время по сравнению со зданием школы с изоляцией 10 см имеет теплотери в 5 раз больше, поскольку здание с изоляцией 10 см дает значение $31,402 \cdot 10^6$ кДж в сутки.

Разница теплотери между зданием с изоляцией 30 см и с изоляцией 10 см составляет 2,29 раза, а если изоляцию сократим от 30 см до 20 см, тогда теплотери увеличатся в 1,36 раза.

Солнечная система сезонного аккумулирования тепла

Для покрытия теплотери здания мы должны удовлетворить условие $Q_{пз} = Q_j$. Мы предварительно определили поступление солнечной радиации с 1410 м^2 коллекторов с учетом наклона солнечных коллекторов, которое составило $Q_j = 146696400$ кДж за отопительный период. Предположим, если размер солнечного коллектора 2×1 , то для покрытия тепловой нагрузки здания понадобится 705 штук солнечных коллекторов.

Теперь перед нами стоит задача аккумулирования этой энергии и определение ориентировочного объема бака-аккумулятора [6].

Нам известно, что потери здания $Q_{пз}$ должны быть равны количеству тепла бака-аккумулятора $Q_{ба}$, т.е. $Q_{пз} = Q_{ба}$, а $Q_{ба} = V \cdot \rho \cdot C_p \cdot (t_2 - t_1)$.

Тогда:

$$Q_{пз} = Q_{ба} = V \cdot \rho \cdot C_p \cdot (t_2 - t_1), \quad (18)$$

где V – объем бака-аккумулятора, м^3 ; ρ – плотность теплоносителя, $\text{кг}/\text{м}^3$; C_p – теплоемкость теплоносителя, $\text{кДж}/\text{кг}$; t_2 – температура воды к началу отопительного периода, $^{\circ}\text{C}$; t_1 – температура воды к 1 апреля, которая должна согреться до 95°C к 31 октября.

Из формулы (19) определяем ориентировочный объем бака при разной толщине изоляции дома. Здание без изоляции, ($\delta_{из} = 0$ см):

$$V = [Q_{пз} / (\rho \cdot C_p \cdot (t_2 - t_1))] = 1,554939 \cdot 10^9 / (1000 \cdot 4,19 \cdot (95 - 10)) = 4365,96 \text{ м}^3. \quad (19)$$

Аналогичным образом определили объемы баков с разной толщиной изоляции дома:

при $\delta_{из} = 10$ см: $V = 811 \text{ м}^3$;

при $\delta_{из} = 20$ см: $V = 410,18 \text{ м}^3$;

при $\delta_{из} = 30$ см: $V = 313,47 \text{ м}^3$.

Заключение

Из вышеизложенного можно сделать следующие выводы:

1. Для оценки экологической обстановки в Бишкеке, а также для исследования тепловой нагрузки здания объектом была выбрана СОШ №19. Из типового проекта здания (технический паспорт школы) определены его конструктивные и архитектурно-планировочные решения.

2. Разработанная нами методика расчета тепловых потерь здания и коэффициента теплоотдачи с учетом изменяющихся параметров внешней среды позволила создать блок-схему алгоритма расчета. На основе этого алгоритма нами разработана компьютерная программа расчета теплотерь здания с использованием программного продукта DELFI.

3. Обобщение многолетних метеорологических данных, взятых из климатологического центра о температуре воздуха в городе Бишкек, позволило получить реальное изменение среднемесячных температур воздуха в годовом цикле, т.е. $t_n = t(\tau)$.

4. Результат расчета показывает, что с учетом реальной температуры окружающего воздуха компьютерная программа позволила выбрать оптимальную толщину изоляции здания школы. Рекомендуемой толщиной изоляции здания является 20 см изоляционного материала базальтового волокна, как широко распространенного на нашем рынке.

5. Для покрытия теплотери здания определили поступление солнечной радиации с 1410 м² коллекторов, что соответствует 705 штукам солнечных коллекторов размером 2×1.

6. На основе исследования влияния толщины теплоизоляции на теплотери здания установлено, что имеется разумный предел толщины теплоизоляции, который не должен превышать 30 см. Для покрытия теплотери здания школы рекомендуется ориентировочный объем сезонного бака-аккумулятора, который равен $V = 410,18 \text{ м}^3$ при толщине изоляции дома $\delta_{из} = 20 \text{ см}$.

В целом разработанная нами методика позволяет определить тепловую потребность любого здания, также подобрать систему солнечного теплоснабжения к этому зданию.

Литература

1. Аналитическое исследование ЦППИ «Экологическая катастрофа в Бишкеке: необходимо внедрять лучшие модели поведения для обеспечения чистого воздуха» [Электронный ресурс]: <https://center.kg/article/295>, 4 февраля 2021 года.
2. Бондалетова Л.И., Новиков В.Т., Алексеев Н.А. «Расчеты выбросов загрязняющих веществ при сжигании твердого топлива в котлоагрегатах котельных». Методическое пособие по выполнению практических занятий по курсу «Промышленная экология». – Томский политехнический университет, 2000 г.
3. <https://studfile.net/preview/3914754/>
4. Мэрия города Бишкек. КП «Бишкектеплоэнерго». Расход угля и газа за один отопительный сезон <https://bishkek.gov.kg/ru/resolution/97>
5. Национальный статистический комитет Кыргызской Республики [Электронный ресурс]: <http://www.stat.kg/ru/opendata/category/435/>
6. Мазуренко А.С., Климчук А.А. и др. Разработка схемы комбинированной системы теплоснабжения с использованием сезонного аккумулирования тепла от гелиосистем. Одесский национальный политехнический университет. – Украина, Одесса, 2015. – С.15–20.
7. Насирдинова С.М. Результаты экспериментальных исследований процессов теплопередачи в солнечном баке-аккумуляторе (<https://kstu.kg/journal/journalkstu@gmail.com>) Известия, КГТУ им. И. Раззакова, 1(34). – Бишкек, 2015. – С.165–170.

8. H. Godd, S. Werner. Thermal energy storage systems for district heating and cooling. «Advances in Thermal Energy Storage Systems», Methods and Applications. Wood head Publishing series in Energy, 2015, Pages 467–478.
9. <https://www.sciencedirect.com/science/book/9781782420880>
10. Загрязнение атмосферного воздуха (воздуха вне помещений), 19 декабря 2022 года. [https://www.who.int/ru/news-room/fact-sheets/detail/ambient-\(outdoor\)-air-quality-and-health](https://www.who.int/ru/news-room/fact-sheets/detail/ambient-(outdoor)-air-quality-and-health)
11. Самые загрязненные страны и регионы мира, 2018–2023 годы. <https://www.iqair.com/ru/world-most-polluted-countries>
12. https://kaktus.media/doc/433823_ndpk_15:_novostroyki_eto_bishkek.html#:~:text=% . (Дата обращения 17.03.2021)

УДК 621.3.016.4:620.9

Н.А.Суюнтбекова¹, nurasuuntbekova@gmail.com

¹КГТУ им. И.Раззакова

К.А.Сатаркулов²

²Институт машиноведения и автоматизации НАН КР

СПОСОБ ИЗУЧЕНИЯ СОВМЕСТНОГО ВЛИЯНИЯ РАЗЛИЧНЫХ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ЭЛЕКТРОЭНЕРГИИ НА ПОТЕРИ В МИКРОСЕТИ НА ЕГО ФИЗИЧЕСКОЙ МОДЕЛИ

В данной статье разработана экспериментальная установка с элементами АСНИ для автоматизации отдельных операций эксперимента в локальных микросетях электроснабжения (например, исследование дополнительных потерь при изменении качества электроэнергии).

Предложена схема лабораторной установки с автотрансформаторным датчиком тока для исследования гармонического состава тока нагрузки с нелинейными характеристиками и калориметрический способ измерения потерь ЭЭ, который по мнению исследователей, является одним из чувствительных и точных методов экспериментальных исследований, позволяющих установить практически все причины, приводящие к потерям в исследуемых элементах.

Модифицировано устройство с калориметром, содержащее необходимые элементы для проведения измерения тепловых потерь в физической модели элемента электрической сети.

Ключевые слова: потери и качество электроэнергии; датчик тока; способ измерения потерь; калориметр; нелинейная нагрузка; гармонический состав.

Введение

Экспериментальный метод исследования является заключительным этапом при установлении адекватности разработанной теоретической (аналитической) модели исследуемого процесса, в том числе и результатов, полученных на компьютерной модели (КМ) процесса, так как КМ разрабатывается на основе математической модели (ММ).

Выше отмеченное относится и к проверке адекватности моделей, построенных для исследования влияния качества электрической энергии на потери в элементах электрической микросети различного назначения.

Многими специалистами отмечается актуальность продолжения исследований как теоретического, так и экспериментального характера для уточнения возможных причин, приводящих к возникновению дополнительных потерь (ДП) электроэнергии в элементах, современных микросетях, от которых получают питание множество нагрузок, ухудшающих качество электроэнергии [1-6]. Эти исследования необходимы для проверки выдвигаемых исследователями научных гипотез о механизмах ДП.

Постановка задачи

Предложить способ и различные устройства, обеспечивающие исследования дополнительных потерь как при совместном изменении нескольких показателей качества электроэнергии (несимметрия напряжения, искажение синусоидальности кривой тока, отклонения напряжения от номинального), так и влияние их по отдельности при стохастическом характере изменения нагрузки.

Решение задачи

Предложенный способ представляет различные схемные решения, на основе которых можно создать экспериментальную установку (ЭУ), позволяющую решить поставленную задачу. При этом ЭУ позволяет автоматизировать отдельные экспериментальные операции, так как в ее составе содержатся элементы АСНИ (автоматизированная система научных исследований). Возможный вариант ЭУ в блочном представлении показан на рисунке 1, где:

1. Распределительная коробка с необходимыми коммутационно - защитными и измерительными устройствами.

2. Лабораторные автотрансформаторы (ЛАТР - SUNTEK 5000ВА, 0-300 Вольт, 20 Ампер) (3 шт.) для поддержания трехфазного напряжения на необходимом для проведения исследования уровне.

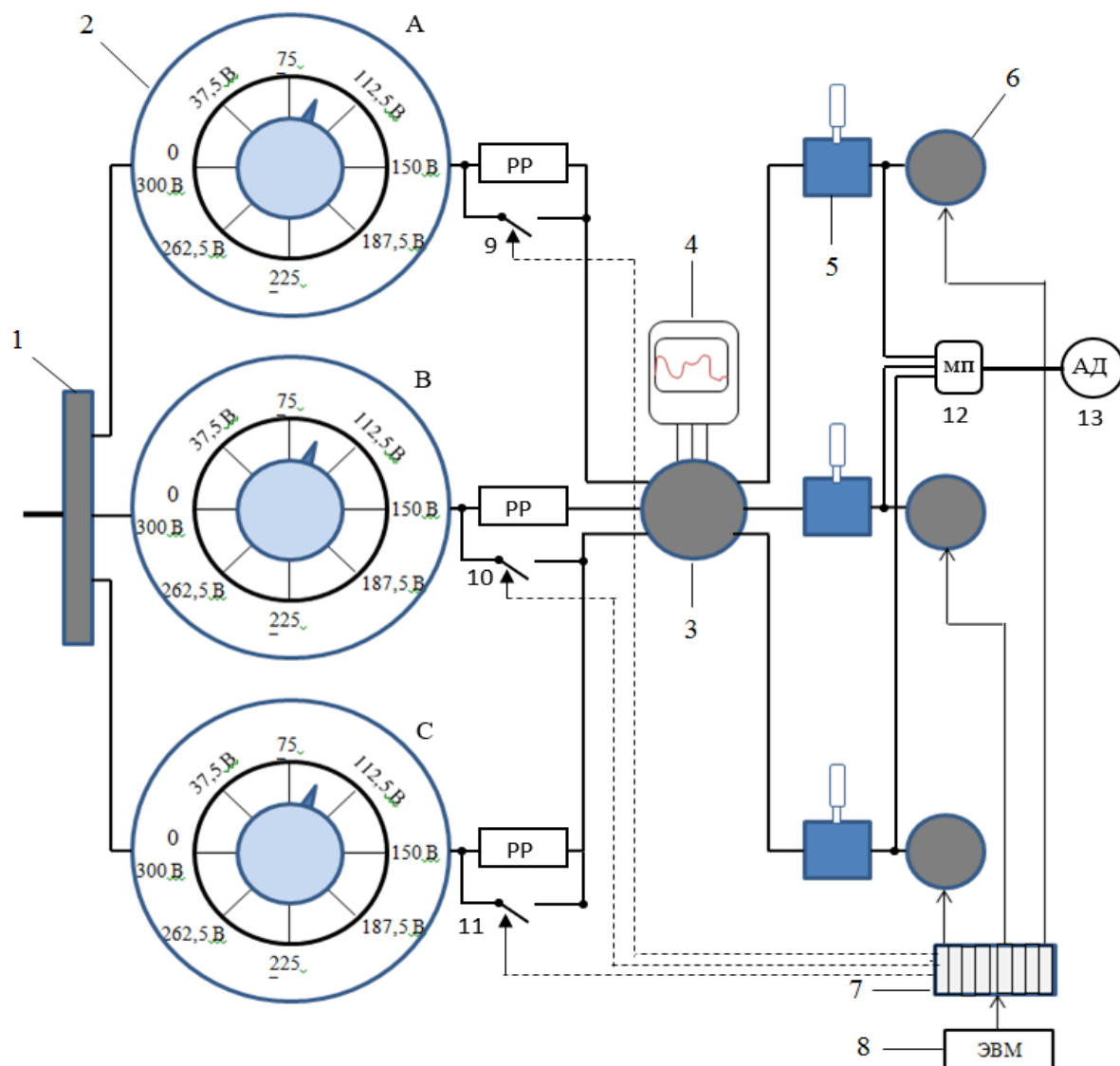


Рисунок 1 – Схема электрического соединения основных элементов экспериментальной установки с элементами АСНИ

3. Устройство для мониторинга и исследования гармонического состава линейных токов нагрузки [7, 8].

4. Двухлучевой осциллограф (FNIRSI – 1013D).

5. Устройство для калориметрического измерения потерь с датчиком температуры в количестве 3 штук на каждой фазе [9, 10].

6. Программно-управляемые от ЭВМ электрические нагрузки.

7. Устройство сопряжения экспериментальной установки с ЭВМ.

8. ЭВМ.

9. 10, 11 – коммутационные ключи в фазных проводах *A, B, C* для шунтирования или расшунтирования соответствующих регулируемых резисторов (РР).

12. Магнитный пускатель (МП) асинхронного двигателя (АД) – 13.

Рассмотрим более подробно специальные нетиповые устройства лабораторной установки. К ним относятся:

- устройство 3 (рис.1) для исследования гармонического состава магнитных полей от токов нелинейных нагрузок, а также для исследования гармонического состава токов в линейных проводах, питающих различные нелинейные нагрузки;

- калориметр с датчиком температуры 5 (рис.1);

- устройство сопряжения экспериментальной установки с ЭВМ, являющейся элементом АСНИ.

Устройства для исследования гармонического состава токов нелинейных нагрузок и магнитных полей от этих токов

Первое устройство конструктивно подобно асинхронной машине с фазным ротором (АМФР) небольшой мощности, работающей в трансформаторном режиме ($s = 1$), когда по соответствующим фазным обмоткам статора, состоящего из нескольких витков, протекают исследуемые линейные токи нагрузки (рис.2). Ротор такой машины может с помощью специального поворотного устройства занимать любое положение относительно статора.

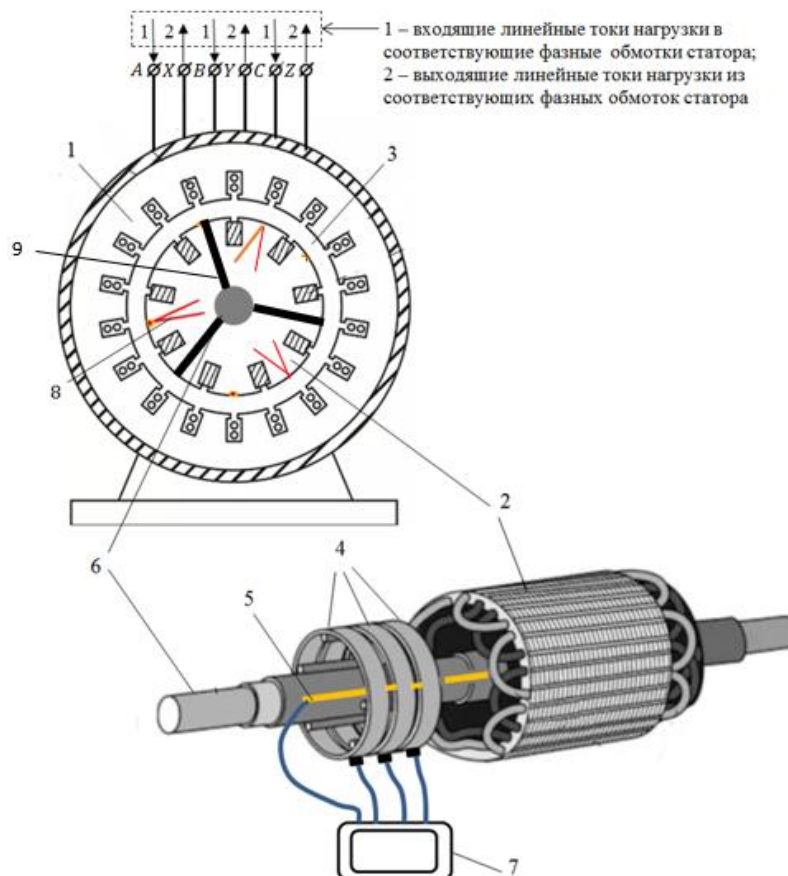


Рисунок 2 – АМФР, работающая в трансформаторном режиме

Конструктивно ротор разделен на три симметричных сектора, изолированных друг от

друга теплоизолирующими прокладками – 9. Температура поверхности ротора каждого сектора измеряется соответствующими датчиками температуры – 8.

АМФР (рис. 2) предназначена для исследования теплового действия гармонического состава магнитных полей от токов нелинейной нагрузки, где фазные обмотки статора разъединены, т.е. не имеют между собой гальванической связи, концы обмоток фазного ротора соединены в звезду, а общая точка соединения выведена наружу (рис. 3), свободные концы подведены к контактным кольцам. Для измерения температуры поверхности сердечника ротора использованы соответствующие датчики (8 — термопары).

Наведенные сигналы в фазных обмотках неподвижного ротора магнитными полями линейных токов нагрузки, протекающих по фазам статора, с помощью щеток, находящихся в скользящем контакте с кольцами, подаются для гармонического анализа на входы осциллографа 7 (рис.2, 3).

На рисунке 2 в развернутом и модифицированном виде показаны отдельные компоненты АМФР, работающей в трансформаторном режиме, где:

1 – сердечник статора с обмотками; 2 – сердечник ротора с обмотками; 3 – зазор между статором и ротором; 4 – контактные кольца; 5 – выведенный наружу проводник, соединяющий концы фазных обмоток ротора; 6 – вал; 7 – осциллограф; 8 – термопары; 9 – теплоизолирующие прокладки.

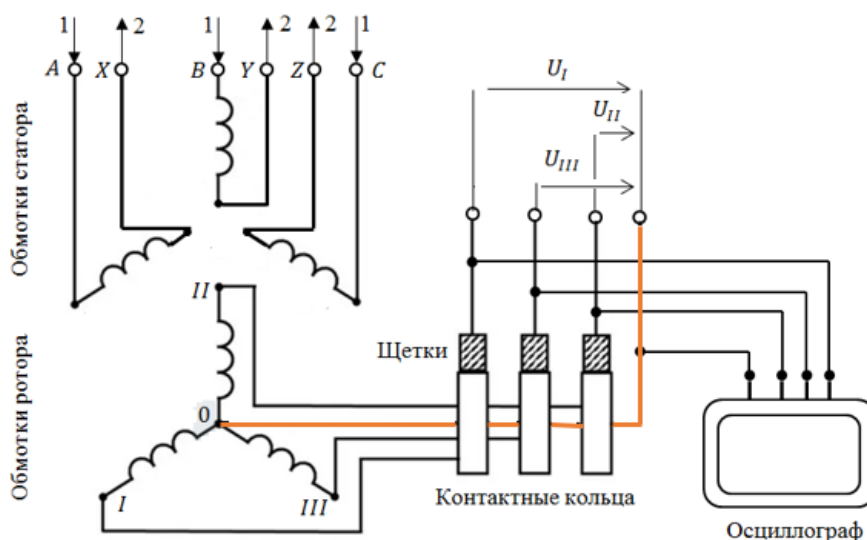


Рисунок 3 – Электрическая схема АМФР для исследования гармонического состава магнитных полей от токов нелинейной нагрузки

На рисунке 3 изображена электрическая схема АМФР, где 1, 2 – соответственно начало и конец статорной обмотки фаз A, B, C ; I, II, III – начало роторной обмотки, соединенной в звезду, концы которых соединены в узле 0; U_I, U_{II}, U_{III} – наведенные напряжения в обмотках ротора относительно узла 0, значения которых подаются на сигнальные входы осциллографа.

Следует отметить, что когда асинхронные машины (в нашем случае с фазным ротором) используются по своему прямому назначению и подключены прямо в трехфазную сеть (рис. 4, а), то они являются для сети электрическими нагрузками, и потребляемые токи характеризуются параметрами самой машины (Z_A, Z_B, Z_C – комплексные сопротивления обмоток статора) и подчинены закономерностям, свойственным этим машинам. В нашем

случае, когда АМФР подключена как устройство для исследования гармонического состава линейных токов нагрузки (УИГС) (рис. 4, *b*), то сигналы, наведенные в фазных обмотках ротора (Z'_A, Z'_B, Z'_C – комплексные сопротивления обмоток статора, образованные небольшим количеством витков) от магнитных полей линейных токов нагрузки и снимаемые через контактные кольца, характеризуют характер влияния различных нагрузок на гармонические составы линейных токов.

На рисунке 4 изображены только фазные обмотки статора АМФР.

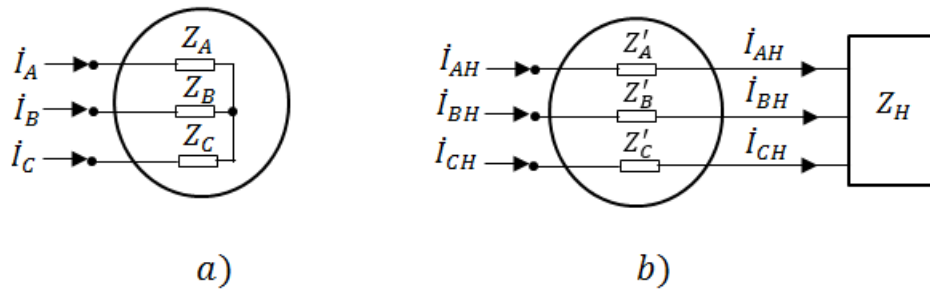


Рисунок 4 *a* – прямое подключение АМФР в трехфазную сеть;
b – подключение АМФР как устройства для исследования гармонического состава линейных токов нагрузки, Z_H

Второе устройство представляет собой автотрансформаторный датчик тока, предназначенный для исследования гармонического состава тока в линейных проводах от различных нелинейных нагрузок, например, светильник с люминесцентной лампой (рис. 6).

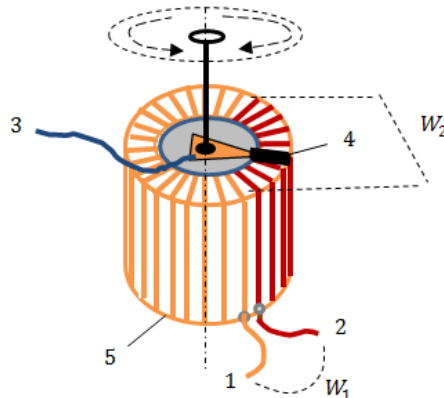


Рисунок 5 – Конструктивные элементы автотрансформаторного датчика тока

На рисунке 5 показаны основные конструктивные элементы автотрансформаторного датчика тока (АТДТ), который конструктивно подобен лабораторному автотрансформатору (ЛАТР). Их отличие в том, что часть обмотки W_1 намотана проводом большего сечения, так как по этой части обмотки протекает ток нагрузки, который может принимать большое значение. Количество витков этой части обмотки равно W_2 . Обе обмотки выполнены медным проводом и намотаны на тороидальный магнитопровод 5. При этом скользящий контакт 4 перемещается по торцу обмотки W_2 . Скользящий контакт 4 имеет гальваническую связь с проводом 3. Отличие АТДТ от ЛАТР заключается еще в том, что его вход является для ЛАТР выходом. На рисунках 5 и 6 нумерация элементов и обозначения обмоток идентичны. Для исследования влияния гармонического состава тока нелинейной нагрузки R на потери в физической модели проводника предназначена лабораторная установка (ЛУ) (рис. 6), с

помощью которой нагрузка подключена к зажимам (6-3) источника e .

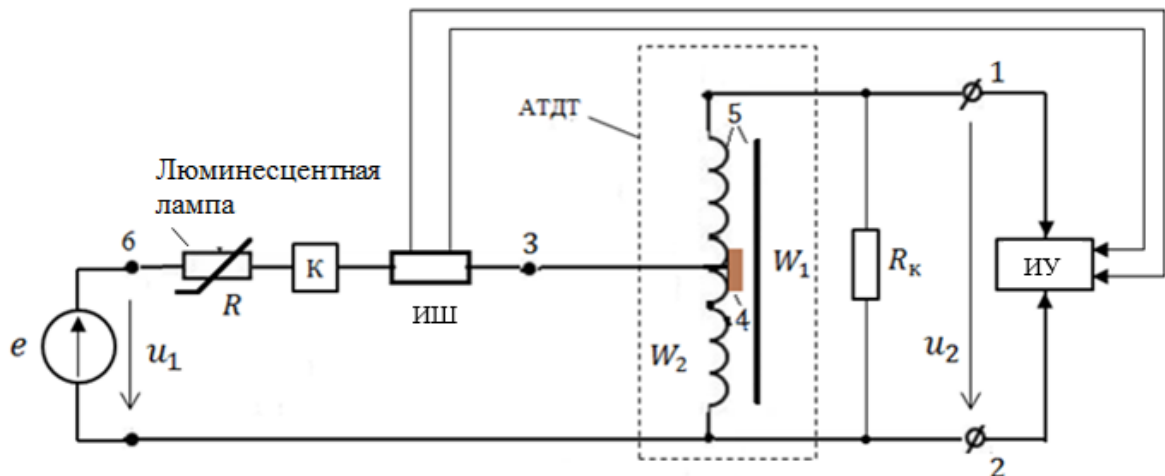


Рисунок 6 – Схема лабораторной установки с автотрансформаторным датчиком тока для исследования гармонического состава тока нагрузки и измерения потерь ЭЭ

На рисунке 6 принято следующее сокращение и обозначение элементов ЛУ: W_1 – количество витков обмотки АТДТ, концы которого выведены на зажимы (1-2); W_2 – некоторая часть витков обмотки W_1 , намотанных проводом большего сечения, электрический сигнал с которого снимается скользящим контактом 4, имеющим гальваническую связь с зажимом 3. Обмотка W_1 намотана на тороидальный магнитопровод 5. ИШ – линейный измерительный шунт, R – люминесцентная лампа (ЛЛ), ИУ – измерительное устройство (прибор), которое в зависимости от поставленной задачи может быть вольтметром или осциллографом, R_K – калиброванный резистор, К – калориметр.

ЛУ, представленная на рисунке 6, позволяет исследовать влияния на потери электроэнергии (ПЭ) в питающем однофазную нелинейную нагрузку проводе от искажения синусоидальности кривой тока (ИСКТ), вызванная этой нагрузкой, например люминесцентной лампой. При этом ЛУ позволяет исследовать влияния на ПЭ при одновременном изменении двух показателей качества электроэнергии, например ИСКТ и отклонения напряжения от номинального (ОН). Потери измеряются калориметром (К). Преимущество калориметрического способа (КС) измерения потери заключается в том, что в нем фиксируются все механизмы, вызывающие потери мощности, которые нагревают теплоносители калориметра. При этом надо учитывать инерционность процесса измерения, так как процесс нагрева теплоносителя калориметра за счет оглашенной потери ЭЭ требует некоторого времени.

Конструктивно АТДТ может быть в двух исполнениях, в первом случае обмотки намотаны на ферромагнитный сердечник, во втором – сердечник из немагнитного материала, следовательно, в первом случае датчик тока нелинейный, во втором – линейный.

В процессе эксперимента для визуализации сигналы, снимаемые с ИШ и с АТДТ через калиброванный резистор – R_K , подаются на входы ИУ. ИУ в данном случае представляет современный четырехлучевой цифровой осциллограф (ЧЛЦО). Программное обеспечение ЧЛЦО позволяет проводить спектральный анализ этих сигналов, представляющих падения напряжения в ИШ и R_K . В результате эксперимента может быть решена поставленная в работе задача.

Следует отметить, что ЭУ позволяет дополнительно изучить, насколько сигнал,

снимаемый с АТДТ через калиброванный резистор – R_k , отличается по спектральному составу от сигнала от ИШ. Очевидно, что основой этих сигналов является ток нагрузки, протекающий через нелинейный элемент – ЛЛ.

Устройство для калориметрического измерения потерь электроэнергии в физической модели элемента электрической сети

На основе изучения научных публикаций [9, 10, 11], где рассмотрены различные методы измерения потерь в элементах электрорадиотехники, находящиеся под электромагнитным воздействием, нами выбран калориметрический метод измерения потерь. По мнению исследователей, калориметрический метод является одним из чувствительных и точных методов экспериментальных исследований, позволяющих установить практически все причины, приводящие к потерям в исследуемых элементах.

На рисунке 7 показана предлагаемое в работе конструктивное исполнение устройства с калориметром для измерения потерь в физической модели элемента электрической (ФМЭ) сети.

Устройство состоит из калориметрической системы – 1, а также коммерчески доступного устройства для измерения температуры – 2, представляющего собой систему из АЦП, микроконтроллера и дисплея, расположенных в одном корпусе, а также отдельно отстоящую термопару – 3. Все эти элементы устройства скреплены на поверхность диэлектрической пластины – 4, которая жестко скреплена со стержнем 5 и вмонтирована в раму – 6.

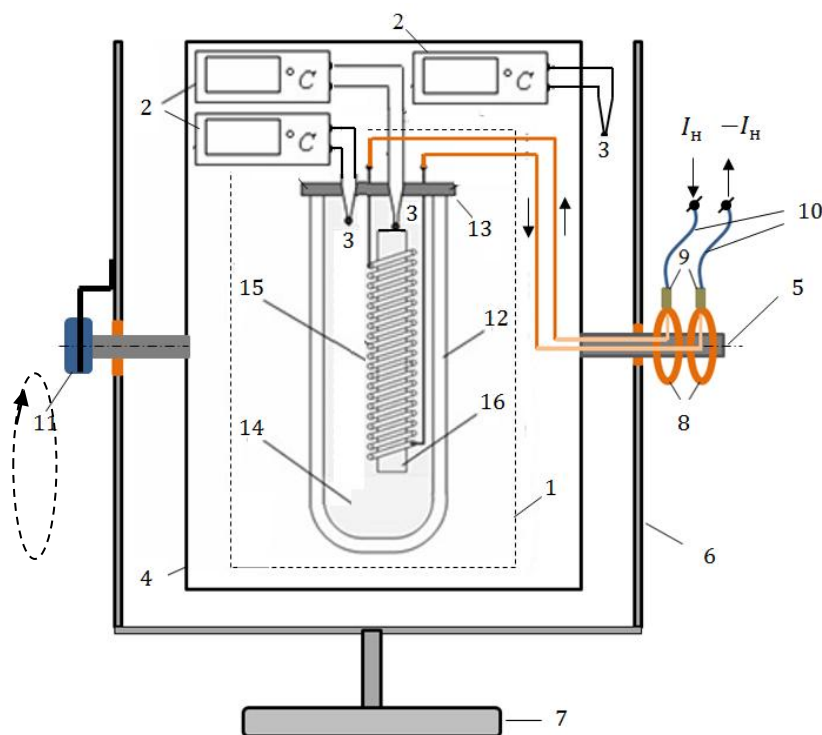


Рисунок 7 – Устройство с калориметром, содержащее необходимые элементы для проведения измерения тепловых потерь в физической модели элемента электрической сети

Рама установлена неподвижно на горизонтальной поверхности 7. Пластина 4 со

стержнем 5 имеет возможность вращаться (на рис. 7 показано стрелкой вращение, скорость вращения медленная) относительно рамы 6. При этом совместно с ними вращаются и два контактных кольца 8, которые жестко насажены на стержень 5. С контактными кольцами 8 соприкасаются щетки 9, имеющие скользящие контакты с ними, с помощью которых через одного из проводов 10 из сети подтекает исследуемый ток, направляющийся после прохождения через ФМЭ электрической сети в нагрузку по другому проводу 10, нагревая физическую модель.

Основным элементом калориметрической системы является прямоугольная пластина 16 из алюминия с выемкой для нагревателя – ФМЭ, помещенная в теплоизолированный корпус сосуда из стекла 12 (термос) (рис. 7).

Пространство между стеклом (стенка термоса) и блоком заполняются дистиллированной водой 14. Измерение температуры проводится термopарами, расставленными в различных точках калориметра, в том числе на стенке алюминиевой пластины и поверхности ФМЭ и на некотором расстоянии от нее. Напряжение с термопар поступает на МК через АЦП. На начальном этапе все элементы калориметра должны иметь одинаковые начальные температуры. Измерения должны проводиться через равные промежутки времени, устанавливаемые исследователем. В процессе эксперимента рама должна периодически раскачиваться или медленно вращаться, чтобы жидкость в сосуде 12 перемешивалась для установления равной температуры жидкости по всему объему сосуда 12.

Калориметр, использованный в работе [9, 10] для определения тепловых потерь в светодиодном модуле (СДМ), представлен на рисунке 8.

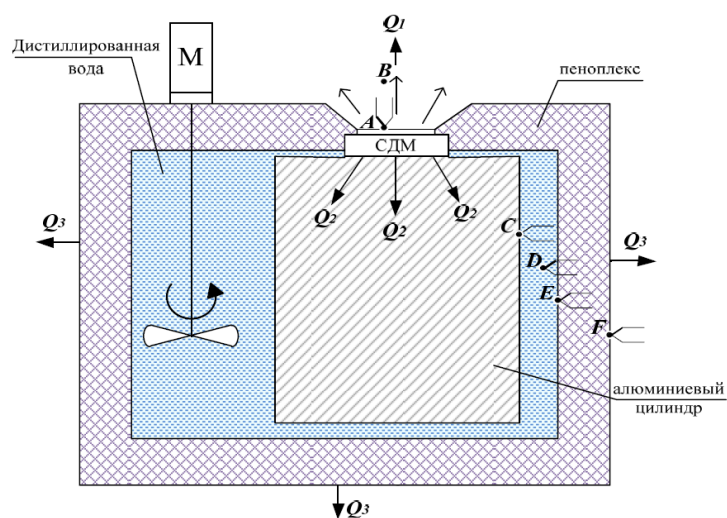


Рисунок 8 – Калориметр для измерения энергии тепловых потерь, в СДМ [9, 10]

Где Q_1 – энергия, испускаемая с поверхности СДМ; Q_2 – энергия, полученная калориметром; Q_3 – энергия, отданная калориметром в окружающую среду, которая складывается из излучаемой Q_k энергии и энергии, уносимой конвекционным потоком Q_k .

На рисунке 7 эти тепловые величины Q_1 , Q_2 , Q_3 , Q_k , Q_k не показаны, но они существуют и аналогичные по смыслу.

Выделяемая в исследуемом элементе тепловая энергия Q определяется в виде суммы тепловых энергий:

$$Q = Q_1 + Q_2 + Q_3. \quad (1)$$

Приведенные в выражении (1) тепловые величины определяются по соответствующим формулам термодинамики и теплопередачи [12]. Значение Q используется для расчета

потери электроэнергии в физической модели элемента электрической сети, при этом надо использовать известное эквивалентное соотношение:

$$1 \text{ кВт} \cdot \text{ч} = 3,6 \cdot 10^6 \text{ Дж.}$$

Например, если в процессе эксперимента калориметром измерена выделенная тепловая энергия $0,548 \cdot 10^3 \text{ Дж}$, то она будет соответствовать $0,152 \cdot 10^{-3} \text{ кВт} \cdot \text{ч}$ электрической энергии, если эксперимент длился 20 минут, то потери мощности будут равны $0,506 \cdot 10^{-3} \text{ кВт} = 0,506 \text{ Вт}$.

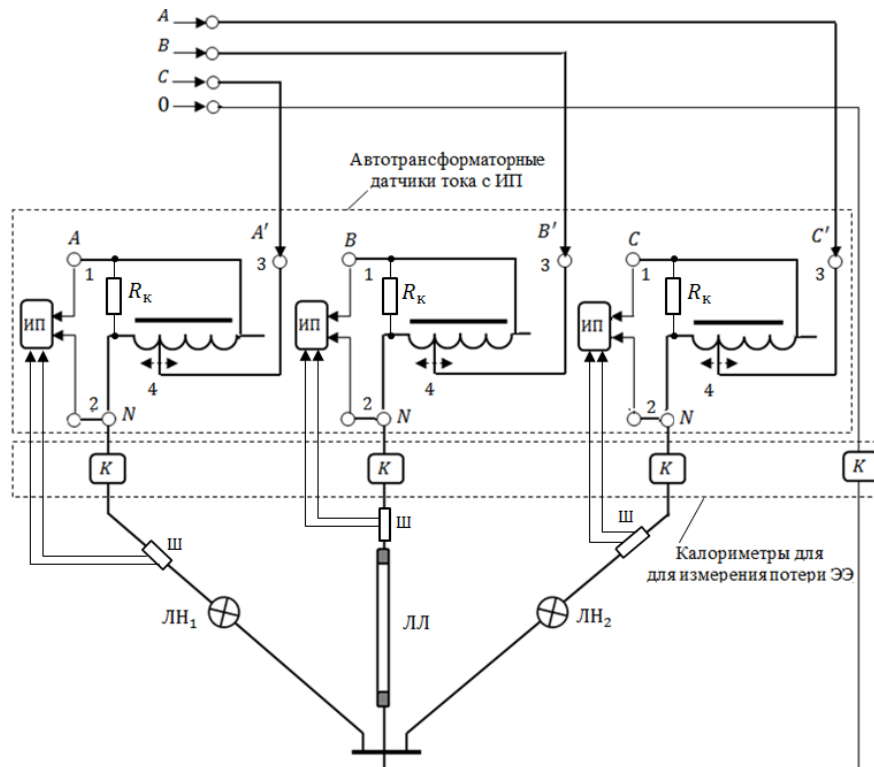


Рисунок 9 – Схема ЛУ для исследования гармонического состава тока в ЭП с нелинейными характеристиками и измерение потерь ЭЭ

На рисунке 9 – ЛН, ЛЛ соответственно светильники с лампами накаливания и люминесцентной лампой, а лабораторная установка (рис. 9), в отличие от ЛУ (рис. 6), предназначена для исследования влияния гармонического состава на потери в трехфазной несимметричной цепи. Как было сказано, потери электроэнергии в элементах цепи измеряются с помощью калориметра. **Процесс** функционирования установки аналогично работе ЛУ рисунка 6.

Заключение

1. Разработана экспериментальная установка с элементами АСНИ для автоматизации отдельных операций эксперимента в локальных микросетях электроснабжения (например, исследование дополнительных потерь при изменении качества электроэнергии).

2. Предложена схема лабораторной установки с автотрансформаторным датчиком тока для исследования гармонического состава тока нагрузки с нелинейными

характеристиками и калориметрический способ измерения потерь ЭЭ, который, по мнению исследователей, является одним из чувствительных и точных методов экспериментальных исследований, позволяющих установить практически все причины, приводящие к потерям в исследуемых элементах.

3. Модифицировано устройство с калориметром, содержащее необходимые элементы для проведения измерения тепловых потерь в физической модели элемента электрической сети.

Литература

1. Тимчук С. А., Мирошник А. А. Определение потерь электроэнергии в зависимости от ее качества в нечеткой форме в сельских распределительных сетях // Восточно-Европейский журнал передовых технологий. – 2015. – Т.1, №8 (73). – С. 4–10.
2. Боровиков В.С., Харлов Н.Н. Оценка добавочных потерь активной мощности и электроэнергии в линиях с высоким коэффициентом искажения синусоидальности тока // <http://www.lib.tpu.ru/fulltext/v/Conferences/2010/K02/1001.pdf>.
3. О необходимости включения добавочных потерь от высших гармоник тока в технологические потери при передаче электрической энергии / В. С. Боровиков, Н. Н. Харлов, Т. Б. Акимжанов. // Известия Томского политехнического университета / Томский политехнический университет (ТПУ). – Томск, 2013. – Т. 322, № 4. – Энергетика. – С. 91–93.
4. Карташев И. И. Качество электроэнергии в системах электроснабжения. Способы его контроля и обеспечения [Текст] / И. И. Карташев; под ред. М. А. Калугиной. – М.: Изд-во МЭИ, 2000. – 120 с.
5. Железко Ю. С. Потери электроэнергии. Реактивная мощность. Качество электроэнергии: Руководство для практических расчетов [Текст] / Ю.С. Железко. – М.: ЭНАС, 2009. – 456 с.
6. Массов А. А., Козлов П. М., Кумаритов Б. Х., Кирилин И. В. Создание имитационной модели для выявления искажений форм кривых токов и напряжений в сетях рудников // Промышленная энергетика, 2011. – № 5. – С. 44–49.
7. Эралиева Г.Ш. Оценка изменения спектрального состава тока нагрузки при переходном процессе в линии электропередачи / Г.Ш. Эралиева // Наука, новые технологии и инновации Кыргызстана. – 2024. – № 3. – С. 27–33.
8. Сатаркулов К.А. Катушка индуктивности с новым способом намотки как устройство диагностики / К. Сатаркулов, Г.Ш. Эралиева, Г.Н. Ниязова, А.К. Асанов, Н.А. Суюнтбекова // Проблемы автоматизации и управления. 2024. – № 3 (51). – С. 28–36.
9. Савкова Т.Н. Измерение энергии тепловых потерь мощного светодиодного модуля / Т.Н. Савкова, А.И. Кравченко // Вестник ТГТУ – 2013. – №3. – С. 88–92.
10. Савкова Т.Н. Определение средней рассеиваемой мощности светодиодным модулем / Т.Н. Савкова, А.И. Кравченко, Е.Н. Подденежный, Ю.Н. Колесник, А.А. Бойко // Вестник ТГТУ. – 2015. – Т.2. – №2. – С. 273–278.
11. Суюнтбекова Н.А. Способ определения отдельных видов потерь электроэнергии в компонентах электрической сети на их физических моделях / Н.Т. Ниязов, Г.К. Усубалиева, У.А. Калматов, Н.А. Суюнтбекова // Сборник трудов XIII Всероссийского совещания по проблемам управления ВСПУ-2019. Институт проблем управления им. В.А. Трапезникова РАН. 2019. – С. 2765–2773.
12. Болгарский, А.В. Термодинамика и теплопередача: учеб. для вузов / А.В. Болгарский Г. А., Мухачев В. К., Щукин. – М.: Высш. шк., 1975. – 495 с.

УДК 621.396

М. М. Калипанов, Kmm75565@mail.ru

Военно-инженерный институт радиоэлектроники и связи МО РК

ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ КООРДИНАТ РАДИОЛОКАЦИОННЫХ СТАНЦИЙ

В статье рассматриваются основы радиолокационных систем координат, используемых для определения местоположения цели. Описаны такие параметры, как наклонная дальность, азимут и угол места, а также их связь с различными системами координат. Особое внимание уделено сферической и цилиндрической системам координат, а также их применению в радиолокации. Рассматриваются локальные и глобальные системы координат, включая географическую (геодезическую) и геоцентрическую (геосферическую) системы. Приводятся формулы, позволяющие определить координаты объекта в этих системах, и описывается их связь с реальной моделью Земли. Упрощение математической модели Земли для целей радиолокации также обсуждается в контексте использования вычислительных машин для решения сложных задач.

Ключевые слова: радиолокация, наклонная дальность, азимут, угол места, системы координат, сферическая система координат, цилиндрическая система координат, географическая система координат, геоцентрическая система координат, геодезическая широта, геодезическая долгота, модель Земли, радиус Земли, вычислительные машины.

Введение

Умение правильно ориентироваться имеет исключительное значение на войне. Разобраться в окружающей обстановке, определить свое местонахождение, выдержать заданное направление – чрезвычайно важно во всяком бою. Опыт многих войн убеждает, что умение ориентироваться, особенно ночью, в туман и при плохой видимости, иногда играет решающую роль в ведении боя. Незнание приемов ориентирования может привести порой к весьма печальным последствиям [1].

Появление средств спутниковой навигации, казалось бы, окончательно решило проблему ориентации в пространстве людей и технических средств. Но опыт военных действий в Ираке и Югославии убедительно показал, что полагаться на системы спутниковой навигации нужно с осторожностью, так как они подвержены подавлению и спуффингу (искажению координат).

Радиолокационное ориентирование в пространстве воздушных объектов развивается достаточно давно [2, 3, 4, 5], однако при радиолокационном ориентировании наземных объектов появляются специфические проблемы.

Ошибки ориентирования РЛС приводят к появлению ошибок определения координат воздушных целей, что, в свою очередь, приводит к неточным целеуказаниям для зенитных комплексов.

Постановка проблемы (задачи)

За топогеодезическое обеспечение и привязку элементов боевого порядка отвечают начальники штабов полков, а за ориентирование средств – заместители командиров полков по вооружению. В подразделениях по части назначаются офицеры, ответственные за топографическую привязку средств.

Основными задачами топогеодезического обеспечения боевых действий являются:

заблаговременная подготовка территории в топогеодезическом отношении и доведение исходных астрономо-геодезических данных до частей и подразделений;

пополнение запасов топографических и специальных карт и своевременное обеспечение ими частей и подразделений по полной норме в установленные сроки;

топогеодезическая подготовка позиционных районов;

топогеодезическая привязка элементов боевого порядка.

Наиболее сложные задачи топогеодезического обеспечения, требующие специальной подготовки личного состава и применения высокоточной топографической техники, выполняет топографическая служба соединений и частей. Топографическую привязку элементов боевого

порядка командных пунктов и зенитных ракетных дивизионов выполняют штатные топогеодезические отделения топопривязчиков.

Информация о координатах радиолокационных станций передается в автоматизированную систему управления (АСУ) войсками, в задачу которой входит перерасчет координат обнаруженных целей из локальных систем координат радиолокационных станций в локальную систему координат зенитного комплекса при выдаче целеуказаний. Эта процедура занимает некоторое время Δt . За это время цель смещается на дистанцию $\Delta l = \Delta t \cdot v$, где v – скорость цели. Это может приводить к ошибке целеуказания $\Delta \alpha = \Delta l / D$, где D – наклонная дальность цели.

Если цель движется со скоростью 800 км/час на дистанции 150 км, а время, необходимое АСУ для выполнения задач вторичной и третичной обработки, идентификации цели и формирования целеуказаний, принять 100 секунд, то ошибка целеуказания может достигать значений:

$$\Delta \alpha = \frac{\Delta t \cdot v}{D} = \frac{(100/3600) \cdot 800}{150} = 0,15 \text{ рад} = 8,3^\circ$$

что явно неприемлемо для зенитного комплекса. Такая же ошибка целеуказания на БПЛА, летящий со скоростью 100 км/ч на дистанции 10 км, может достигать значений:

$$\Delta \alpha = \frac{\Delta t \cdot v}{D} = \frac{(100/3600) \cdot 100}{10} = 0,28 \text{ рад} = 15,6^\circ$$

Таким образом, существует необходимость выдачи целеуказания на зенитные средства, минуя АСУ, что потребует решения задачи преобразования систем координат либо в РЛС разведки, либо в зенитном комплексе, либо в обеих системах одновременно.

Цель статьи

Рассмотреть ограничения по точности определения местоположения радиолокационных станций с применением существующих методов, способных влиять на ошибки целеуказания.

Методы исследования

В качестве основных методов исследования в данной статье были использованы методы преобразования систем координат.

Изложение основного материала (результаты/обсуждения)

Системы координат (СК), используемые в радиолокации [6, 7]. При радиолокационном определении местоположения наиболее часто применяют *местную сферическую систему координат*, начало которой находится в точке размещения антенны. В наземной РЛС одна из осей координатной системы обычно совпадает с северным направлением меридиана, проходящего через позицию антенны РЛС, а местоположение цели Ц находится по результатам измерения наклонной дальности D , азимута α и угла места β (рис. 1, а). При этом система координат неподвижна относительно земной поверхности. Если РЛС располагается, например, на движущемся объекте, то ось X координатной системы совмещается с продольной осью объекта, а ось Y – перпендикулярна ей и лежит в плоскости погона объекта (рис. 1, б), образуя с осью H , направленной по нормали вверх, левостороннюю декартову систему координат. В этом случае для определения местоположения цели измеряются наклонная дальность D , курсовой угол цели α и угол места β . Такая связанная с объектом система координат перемещается относительно земной поверхности со скоростью, равной скорости движения объекта, и поворачивается вокруг Земли при его эволюциях.

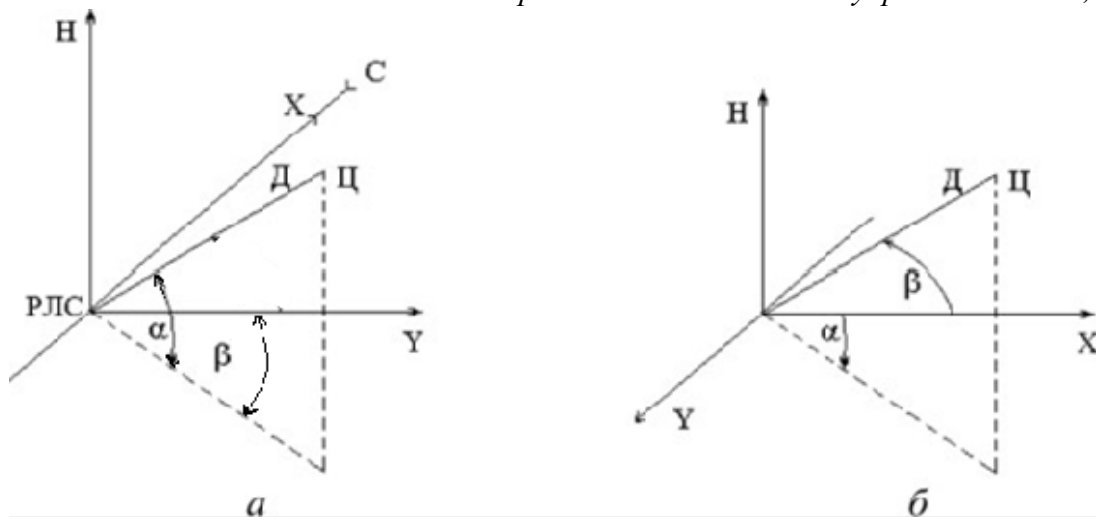


Рисунок 1 – Местные сферические системы координат:

а – при расположении РЛС на поверхности Земли; б – при расположении РЛС на борту летательного аппарата

Наклонная дальность D представляет собой расстояние по прямой от радиолокационной станции (РЛС) до цели. Азимут цели α – это угол между вертикальной плоскостью, которая проходит через цель, и начальным направлением отсчета. Азимут называют истинным пеленгом, если отсчет ведется от северного меридиана, или курсовым углом (КУ), если отсчет производится относительно продольной оси летательного аппарата (ЛА) или диаметральной плоскости корабля.

Угол места β – это угол между направлением на цель и его проекцией на горизонтальную плоскость.

Когда РЛС установлена на летательном аппарате (ЛА), ось X координатной системы совпадает с продольной осью ЛА, а ось ZZ направлена вдоль правого крыла (рис. 1.б). В таком случае для определения местоположения цели измеряют наклонную дальность D , курсовой угол — азимут цели α и угол места β . Эта система координат, связанная с ЛА, движется по земле с той же скоростью, что и ЛА, и поворачивается относительно Земли в зависимости от его маневров.

Кроме сферической системы координат, в радиолокации используется цилиндрическая система, где координатами являются горизонтальная дальность D_g , азимут α и высота H (рис. 2).

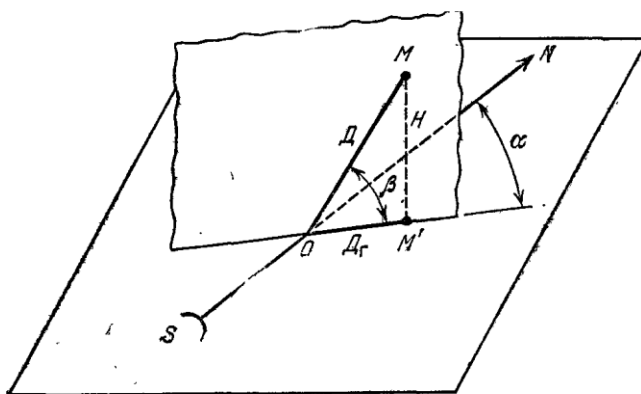


Рисунок 2 – Цилиндрическая система координат

Горизонтальная дальность $D_g = OM'$, OM' – это проекция наклонной дальности на горизонтальную плоскость. Высота цели H – это длина перпендикуляра, опущенного из точки M на горизонтальную плоскость, то есть $H=MM'$.

Очевидно, что:

$$D_r = D \cos \beta; H = D \sin \beta; \quad (1)$$

$$D = \sqrt{D_r^2 + H^2}. \quad (2)$$

Для определения местоположения используют как локальные системы координат (рис. 1, 2), так и глобальные. Локальные системы применяются для дальностей D , не превышающих несколько сотен километров (в пределах прямой видимости), в то время как глобальные используются для больших расстояний. Глобальные системы координат жестко привязаны к Земле и охватывают всю поверхность или значительную ее часть. Наиболее известными глобальными системами являются географическая (геодезическая) и геоцентрическая (геосферическая) системы координат.

В географической (геодезической) системе координат СК $O_G X_G Y_G$ (рис. 3) Земля представлена эллипсоидом вращения. В СССР, согласно Постановлению Совета министров от 7 апреля 1946 года, был принят эллипсоид Красовского, малая полуось которого составляет 6 356 863 м, а большая — 6 378 245 м. В других странах используется эллипсоид Хейфорда-Кларка, чьи размеры отличаются от эллипсоида Красовского на несколько сотен метров. Положение точки C на поверхности эллипсоида определяется геодезическими координатами: географической широтой φ_G и географической долготой λ_G .

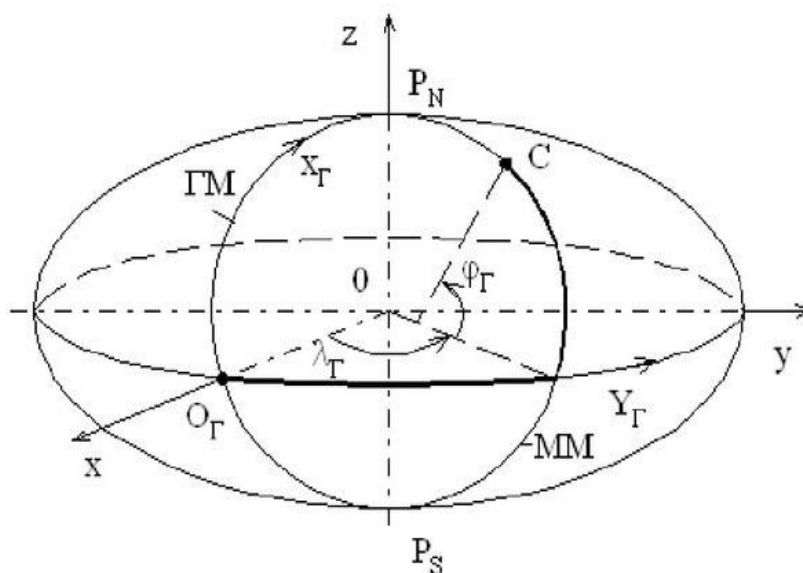


Рисунок 3 – Географическая (геодезическая) система координат

Географической широтой точки называется угол между плоскостью экватора и нормалью к поверхности эллипсоида в этой точке. Нормаль обычно не пересекает экватор в его центре. Широта измеряется от плоскости экватора к Северному и Южному полюсам, от 0 до ± 90 градусов.

На рисунке 3 буквами o , x , y , z обозначена основная система координат, связанная с центром Земли и вращающаяся вместе с ней.

Географическая долгота — это угол между плоскостью начального меридиана (Гринвичского) и местным меридианом точки C , который проходит через проекцию объекта на земную поверхность. Долгота измеряется от 0 до 360 градусов, причем восточная долгота имеет знак плюс, а западная — минус.

Хотя поверхность эллипсоида математически точно описана, задачи радиолокации решаются с помощью высокоскоростных цифровых вычислительных машин, так как вычисления слишком сложны для обычных методов. Поэтому часто используется упрощенная модель Земли в виде шара с радиусом 6 371 110 м.

Геоцентрическая (геосферическая) система координат $O_{гц}X_{гц}Y_{гц}Z_{гц}$ основывается на представлении Земли в виде шара (рис. 4). В этой системе геоцентрическая широта $\varphi_{гц}$ определяется как угол между экваториальной плоскостью и направлением радиуса-вектора от объекта к центру Земли. Способ отсчета геоцентрической долготы (λ) аналогичен географической долготе.

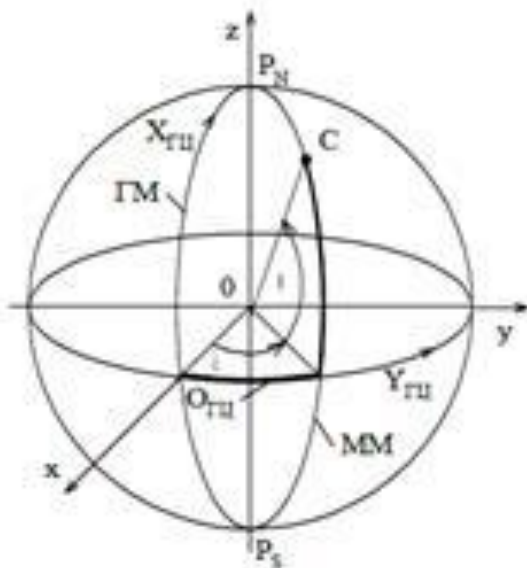


Рисунок 4 – Геоцентрическая (геосферическая) система координат

Таким образом, в современной радиолокации используются местные и глобальные СК. Следует отметить, что местные системы декартовых координат – левосторонние, а глобальные системы – правосторонние, что следует учитывать при преобразовании систем координат.

Для правильного преобразования координат необходимо знание реальных местоположений, как радиолокатора разведки, так и зенитного комплекса. Учитывая, что координаты месторасположения являются секретной информацией и они могут меняться в ходе боевых действий, то необходима либо передача этих координат между станцией разведки и зенитным комплексом, либо передавать данные о координатах цели необходимо в некой промежуточной системе координат. Такой промежуточной системой координат могла бы служить одна из глобальных систем координат. В этом случае при передаче данных целеуказания радиолокатор разведки не передавал бы координаты своего месторасположения, а зенитный комплекс мог бы, зная свои текущие координаты, преобразовывать полученные координаты цели в целеуказания в свою (локальную) СК.

В общем случае преобразование одной декартовой системы координат в другую разделяется на 2 этапа:

- поворот систем координат таким образом, чтобы оси локальной системы координат стали параллельны осям той СК, в которую нужно преобразовать координаты цели;
- смещение системы координат вдоль их осей на такую величину, чтобы совпали центры систем координат обеих СК.

Поворот систем координат осуществляют с помощью матриц поворота

$$R_x(\alpha) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & \sin \alpha \\ 0 & -\sin \alpha & \cos \alpha \end{bmatrix}; \quad (3)$$

$$R_y(\alpha) = \begin{bmatrix} \cos \alpha & 0 & -\sin \alpha \\ 0 & 1 & 0 \\ \sin \alpha & 0 & \cos \alpha \end{bmatrix}; \quad (4)$$

$$R_z(\alpha) = \begin{bmatrix} \cos \alpha & \sin \alpha & 0 \\ -\sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}. \quad (5)$$

Положительным углом поворота считается поворот против часовой стрелки, если смотреть навстречу оси поворота. Для поворота по часовой стрелке знак угла поворота необходимо изменить на противоположный.

Сдвиг систем координат (при переходе к глобальной СК) обычно осуществляется переносом системы координат в центр Земли. Однако это не обязательно. Достаточно, чтобы обе стороны знали о том, где расположен центр промежуточной СК. Возможна разработка такой системы пересчета координат, при которой центр промежуточной СК может меняться ежедневно или еженедельно. Противник, не зная о том, какая точка принята в качестве центра в промежуточной СК, не сможет правильно идентифицировать цель, на которую передается целеуказание.

Так как местные системы координат в радиолокации – левосторонние, а глобальные СК – правосторонние, то промежуточную глобальную СК целесообразно выбрать также левосторонней, что упростит преобразование координат с помощью матриц поворотов.

Заключение

По результатам проведенных исследований можно сделать следующие выводы:

1. Передача целеуказаний о воздушных, минуя АСУ, приводит к снижению времени их передачи и, соответственно, ошибок целеуказания.
2. При передаче целеуказаний координаты целей целесообразно передавать в промежуточной глобальной системе декартовых координат.
3. Глобальную СК целесообразнее использовать левостороннюю.
4. Динамическое изменение во времени координат центра промежуточной СК повысит безопасность передачи данных о воздушных целях.

Благодарности. «Исследование выполнено при финансовой поддержке Комитета науки МОН РК» (Грант № AP148036/0222)

Литература

1. М.Ф. Беляков. Ориентирование на местности без карты. – М.: Воениздат, 1955. <https://docs.yandex.kz/docs/view?tm=1722406241&tld=kz&lang=ru&name=geokniga>.
2. Scannapieco, A.F., Graziano, M.D., Fasano, G., Renga, A. (2019) Improving radar-based mini-UAS navigation in complex environments with outlier rejection. AIAA Scitech 2019 Forum. https://www.researchgate.net/publication/330196408_Improving_radar-based_mini-UAS_navigation_in_complex_environments_with_outlier_rejection.
3. Scannapieco, A.F., Renga, A., Fasano, G., Moccia, A. (2017) Ultralight radar for small and micro-UAV navigation. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives, 42(2W6), страницы 333–338 https://www.researchgate.net/publication/319413337_ULTRALIGHT_RADAR_FOR_SMALL_AND_MICRO-UAV_NAVIGATION.
4. Неусыпин К. А. (2009) Современные системы и методы наведения, навигации и управления летательными аппаратами. Гироскопия и навигация. <https://elibrary.ru/item.asp?id=19642445>.
5. Костоусов А.В., Костоусов В.Б. (2007) Распределенные вычисления и моделирование процесса навигации по радиолокационным изображениям. Автоматика и телемеханика PACS 07.05.Тр. <https://naukarus.com/raspredeleennyie-vychisleniya-i-modelirovanie-protssessa-navigatsii-po-radiolokatsionnym-izobrazheniyam>.
6. Бакулев П.А. Радиолокационные системы: Учебник для вузов. – М.: Радиотехника, 2004.
7. Белоцерковский Г.Б. Основы радиолокации и радиолокационные устройства. – М.: Советское радио, 1975.

8. Дмитриев Д.Д. и др., Боевое применение подразделений РТВ ВВС. Радиолокационная станция П-18: [Учебное пособие]//Красноярск: СФУ, 2011. – 166с.
9. Radar equations for modern radar. Author(s), Barton, David K. Publication, Norwood: Artech House, 2012. - 448 p.
10. Конкин Ю. В. Разработка системы определения координат летательного аппарата на основе совмещения радиолокационной и картографической информации // Диссертация на соискание ученой степени кандидата технических наук, Рязанский государственный радиотехнический университет, Рязань, 144 стр.