УДК 533.95

В. С. Славин, И. А. Кузоватов, А. В. Минаков

ПРИМЕНЕНИЕ РАЗНОСТНОЙ СХЕМЫ ЭКСПОНЕНЦИАЛЬНОЙ ПОДГОНКИ ДЛЯ ЧИСЛЕННОГО МОДЕЛИРОВАНИЯ НЕСТАЦИОНАРНЫХ ПРОЦЕССОВ, ПРОТЕКАЮЩИХ В КАНАЛЕ ЛИНЕЙНОГО МГД-УСКОРИТЕЛЯ

Разработан и протестирован высокоэффективный численный алгоритм, позволяющий решать широкий класс двумерных нестационарных конвективно-диффузионных задач. Проведено математическое моделирование нестационарных процессов, протекающих в канале линейного МГД-ускорителя. В полной постановке решена двумерная задача магнитной гидродинамики с учетом эффекта Холла. В результате моделирования обнаружен эффект отклонения токового слоя от направления, перпендикулярного электродам ускорителя. Полученные результаты качественно согласуются с экспериментальными данными.

Ключевые слова: экспоненциальная подгонка, математическое моделирование, вычислительная гидродинамика, токовый слой.

Планируемые в недалеком будущем пилотируемые полеты к планетам Солнечной системы потребуют разработки ракетного двигателя с высокой тягой и удельным импульсом. Это позволит существенно сократить время пребывания человека в условиях жесткой космической радиации, сократить расход рабочего тела и, соответственно, уменьшить необходимый запас топлива на борту корабля, увеличив тем самым массу полезного груза. Удовлетворить эти требования могли бы электрические ракетные двигатели (ЭРД) – устройства, которые используют интенсивный импульс электрического тока (порядка $10^4…10^6$ А) для создания высокоскоростной (порядка $10^3…10^5$ м/с) плазменной струи. Существующие в настоящее время образцы подобного рода устройств нашли широкое применение в космической технике, а также во многих научных экспериментах как источники плазмы. Но, к сожалению, они обладают очень низким уровнем тяги (не более 1 Н), что делает нецелесообразным их применение в качестве маршевых двигателей для космических кораблей.

Низкая сила тяги современных ЭРД связана с самим принципом их работы. Поскольку большинство современных ЭРД работают только с однородным стационарным плазменным потоком, то для предотвращения возникновения различного рода неустойчивостей, стремящихся эту однородность разрушить, данные устройства вынуждены работать при очень низких давлениях, что и обусловливает низкий уровень тяги. Эту проблему может решить создание индукционного ЭРД фарадеевского типа с неоднородной токовой структурой. Существование таких нестационарных, стабильных плазменных структур – так называемых Т-слоев, которые появляются в плазменном потоке, движущемся в поперечном магнитном поле, – было обнаружено в результате численного моделирования в 60-х гг. прошлого века. Т-слои являются результатом развития перегревной неустойчивости, которая в условиях МГД-ускорителя неизбежно возникает, как только плазма из-за охлаждения холодным газом переходит в состояние слабой ионизации. Т-слои – это плазменные поршни, ориентированные вдоль вектора электрического поля и движущиеся вместе с газовым потоком, и поэтому их можно использовать для ускорения неоднородного газоплазменного потока в фарадеевском МГД-канале.

Принципиальная возможность использования Т-слоя для данных целей была показана в работах [1–3]. Одномерное численное моделирование работы индукционного ЭРД с неоднородной токовой структурой показало возможность достижения средней скорости на выходе канала порядка 40…50 км/с при величине расхода рабочего тела 10…50 г/с, что обеспечивает значения тяги в диапазоне 400…2 000 Н.

Однако результаты одномерного моделирования не дают ответа на вопрос, является ли токовый слой устойчивым по отношению к многочисленным возмущениям, которые с неизбежностью будут возникать в канале МГД-ускорителя. Так, в частности, в работах [4; 5] был описан эффект так называемого накренения (*canting*) токового слоя, который заключается в отклонении плазменного сгустка от направления, перпендикулярного электродам в канале линейного МГД-ускорителя. Искривленный токовый слой создает поперечную электродам компоненту силы тяги ЭРД, из-за чего появляется дополнительный вращательный момент, который ухудшает управление космическим кораблем. Кроме того, дополнительная поперечная сила тратит энергию на разгон газа, не преобразуя ее в полезную тягу. Таким образом, в данном случае двумерный эффект приводит к существенному ухудшению характеристик МГД-ускорителя. В связи с этим была поставлена задача изучения нестационарных двумерных процессов в канале линейного ускорителя, чтобы построить и отработать на имеющихся экспериментальных данных математическую модель, которую затем можно будет использовать для более детального изучения процессов в разрабатываемом индукционном ускорителе фарадеевского типа.

Физическая модель. Для проведения численного моделирования процесса ускорения плазменного сгустка использовались данные эксперимента, описанного в [4; 5]. Линейный МГД-ускоритель, или рельсотрон (рис. 1), представляет собой два медных электрода, разделенных диэлектрической вставкой и подключенных к электрической цепи с батареей конденсаторов емкостью 10 мкФ и катушкой индуктивности 100 нГн. Боковые стенки ускорителя выполнены из прозрачного материала – пирекса – для проведения скоростной фотосъемки. Длина МГД-канала 60 см, ширина 10 см, расстояние между электродами 5 см.

В начальный момент МГД-канал заполнен холодным непроводящим аргоном при давлении 100 мторр. При замыкании электрической цепи в МГД-канале происходит пробой холодного газа, формируется дуговой разряд, который затем развивается в токовый слой. Возникающее при этом магнитное поле, параллельное плоскости электродов, ускоряет плазменный сгусток. Под действием теплового и силового факторов происходит формирование плазменного поршня (Т-слоя), который ускоряет участок газового потока, оказавшийся перед ним. Впереди Т-слоя следует сжатый им массовый сгусток, плотность которого резко падает при переходе к волне разрежения, возникающей за Т-слоем. Низкое давление плазмы в хвосте токового слоя приводит к тому, что параметр Холла в волне разряжения становится достаточно большим. В результате возникает холловская компонента силы тока, а вместе с ней – и перпендикулярная потоку компонента силы Лоренца, которая способствует тому, что токовый слой отклоняется от ортогонального к электродам направления (рис. 2).

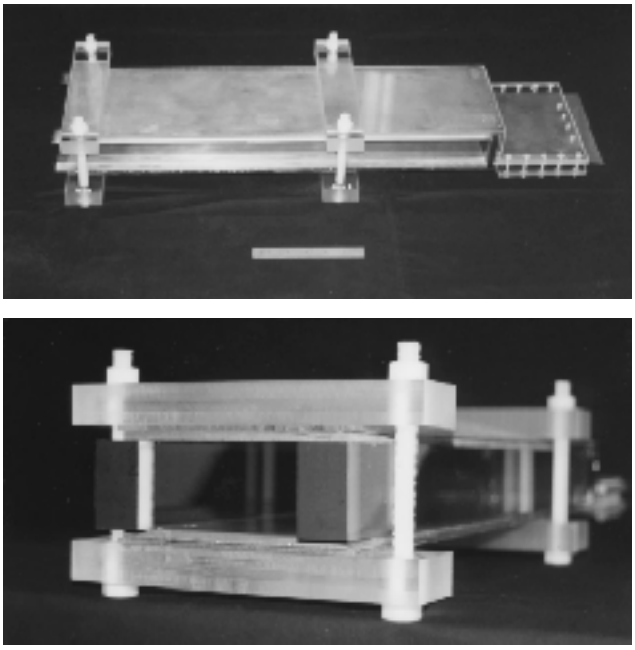


Рис. 1. Фотографии экспериментальной установки

Следующей фазой развития Т-слоя является фаза «снежного плуга», которая начинается, когда искривленная токовая ветвь соединяется с катодом. Непроницаемый для холодного газа Т-слой, подобно плугу, сгребает газ впереди себя. Основной плазменный канал, оторвавшийся от анода, движется к катоду и на стадии «снежного плуга» превращается в след, который тянется за токовым слоем. Более детально процессы, происходящие с токовым слоем в канале ускорителя, описаны в [4]. Нас же больше будет интересовать непосредственное влияние на плазменный сгусток эффекта Холла. Для изучения этого влияния обратимся к численному моделированию.

Математическая модель. Для численного моделирования описанного выше процесса решалась полная система двумерных уравнений магнитной газодинамики, которая, помимо законов сохранения массы, импульса и энергии, включала уравнение индукции магнитного поля с учетом эффекта Холла.

Уравнение неразрывности было следующим:

$$\frac{\partial \rho}{\partial t}+\frac{\partial}{\partial x}(\rho\cdot u)+\frac{\partial}{\partial y}(\rho\cdot v)=S(T), \qquad (1)$$

где $S(T)$ – источниковое слагаемое, отвечающее за увеличение массы газа в МГД-канале, связанное с интенсивной эрозией электродов. Значение этого источника находилось из эмпирического соотношения, а величины входящих в соотношение коэффициентов подобраны в результате методических расчетов:

$$S(T)=0{,}5\cdot e^{(-1{,}5/T)}. \qquad (2)$$

Закон сохранения импульса с учетом силы Лоренца представлен в виде

$$\frac{\partial}{\partial t}(\rho\cdot u)+\frac{\partial}{\partial x}(\rho\cdot u^2+P)+\frac{\partial}{\partial y}(\rho\cdot v\cdot u)=j_y\cdot B, \qquad (3)$$

$$\frac{\partial}{\partial t}(\rho\cdot v)+\frac{\partial}{\partial y}(\rho\cdot v^2+P)+\frac{\partial}{\partial x}(\rho\cdot v\cdot u)=-j_x\cdot B, \qquad (4)$$

а закон сохранения энергии с учетом джоулевой диссипации и радиационных потерь – в виде

$$\frac{\partial e}{\partial t}+\frac{\partial}{\partial x}(u(e+P))+\frac{\partial}{\partial y}(v(e+P))=\vec{J}\cdot\vec{E}-q_r, \qquad (5)$$

где e – полная удельная энергия плазмы; P – давление газа; u и v – компоненты вектора скорости потока; ρ – плотность газа.

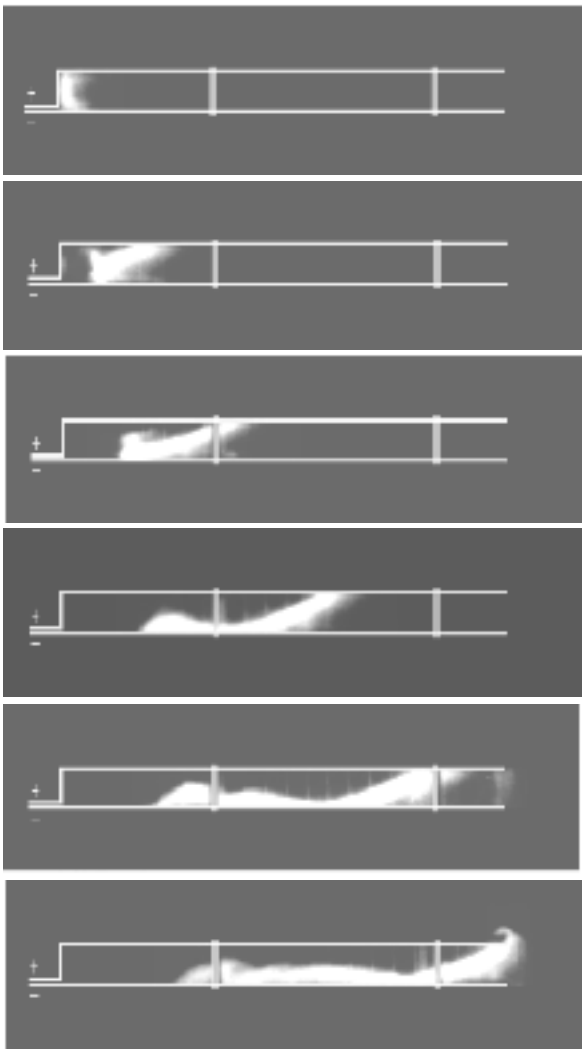


Рис. 2. Фотографии токового слоя через каждые 3 мкс [4]

В качестве уравнения состояния аргона использовалось уравнение идеального газа.

Радиационные потери энергии из объема плазмы, расчет которых даже в грубом приближении является сложной проблемой, в данной модели учитывались как величина, пропорциональная T^4. Коэффициент пропорциональности подбирался с таким расчетом, чтобы радиационные потери стабилизировали температуру плазмы в Т-слое на уровне $2\cdot10^4$ К [3]. Такой подход отражает экспериментальные данные о свойствах плазмы в условиях, близких к поставленной нами задаче. Таким образом, радиационные потери в единице объема плазмы брались в виде

$$q_r = q_0 \cdot T^4,\ q_0 = 10. \qquad (6)$$

Для инициирования токового слоя в начале канала создавалось локальное изобарическое возмущение температуры до максимального значения $T_{\max} = 10^4$ К.

В качестве граничных условий для газодинамических параметров на твердых стенках ставились условия скольжения и непротекания, на выходе из МГД-канала – условие сноса, т. е. равенства нулю производной по нормали к границе для всех величин.

Распределение электромагнитных величин находилось из уравнений Максвелла, дополненных дифференциальным законом Ома с учетом эффекта Холла:

$$\vec{J} = \sigma\left(\vec{E} + \vec{V}\times\vec{B}\right) - \frac{\vec{J}\times\vec{B}}{|B|}\beta,$$

$$\vec{J} = \frac{1}{\mu\cdot\mu_0}\nabla\times\vec{B},\ \nabla\times\vec{E} = -\frac{\partial\vec{B}}{\partial t},\ \nabla\cdot\vec{B} = 0. \qquad (7)$$

Объединив эти уравнения, получим уравнение индукции магнитного поля:

$$\frac{\partial B}{\partial t} = \nabla\left(\frac{1}{\mu\cdot\mu_0\cdot\sigma}\nabla B - B\left(\vec{V} - \frac{\vec{J}\cdot\beta}{B\cdot\sigma}\right)\right), \qquad (8)$$

где $\vec{B}$ – индукция магнитного поля; $\vec{J}$ – плотность электрического тока; β – параметр Холла; σ – электропроводность плазмы; $\vec{V}$ – скорость газового потока; $\vec{E}$ – напряженность электрического поля.

Для определения граничных условий в магнитном поле на левой границе расчетной области решалось электротехническое уравнение цепи с конденсатором и контуром возбуждения, который индуктивно связан с плазмой:

$$L\frac{dI(t)}{dt} + R\cdot I(t) - U(t) = -\frac{d}{dt}\Phi(t),$$

$$l_Z\cdot E = -\frac{d}{dt}\Phi(t),\ \frac{dU}{dt} = -\frac{I(t)}{C},$$

$$I(t) = \frac{B(0,t)}{h\cdot\mu_0},\ U(0) = 9\ \text{кВ},\ I(0) = 0\ \text{А},$$

$$C = 10\ \text{мкФ},\ L = 100\ \text{нГн}, \qquad (9)$$

где R – сопротивление цепи; U – напряжение на конденсаторе; Φ – магнитный поток; I – ток в цепи; L – индуктивность плазмы; C – емкость конденсатора; l_z – ширина электродов; h – шаг разностной сетки. На остальных границах задавались условия Неймана:

$$\frac{\partial B}{\partial x} = 0 \text{ при } x = l_x,\ \frac{\partial B}{\partial y} = 0 \text{ при } y = 0 \text{ и } y = l_x. \qquad (10)$$

В качестве модели плазмы была использована равновесная модель. Электропроводность газа рассчитывалась по эмпирической формуле, качественно верно отражающей поведение реальной плазмы:

$$\sigma = \frac{\sigma_L\sigma_S}{\sigma_L+\sigma_S},\ \sigma_S = \frac{1{,}53\cdot10^{-2}T^{3/2}}{\ln(\Lambda)},\ \sigma_L = \frac{n_e\cdot e^2}{m_e\cdot\sigma_{ea}^{tr}\cdot V_{ea}}, \qquad (11)$$

где σ_L – лоренцевская проводимость, обусловленная электрон-атомными столкновениями, которые преобладают в плазме при низких температурах; σ_S – спитцеровская проводимость, обусловленная кулоновскими электрон-ионными столкновениями, которые преобладают при более высоких температурах.

Концентрация электронов для равновесной плазмы аргона находилась из уравнения Саха:

$$n_e = -K_S + \sqrt{K_S^2 + \frac{P\cdot K_S}{k\cdot T}}, \qquad (12)$$

$$K_s = \frac{\left(2\pi m_e kT\right)^{3/2}}{h^3}\exp\left(-\frac{I}{kT}\right),$$

где I – потенциал ионизации атомов аргона; h – постоянная Планка; k – постоянная Больцмана; m_e – масса электрона.

Параметр Холла вычислялся следующим образом:

$$\beta = \frac{eB}{m_e\left(\nu_{ea}+\nu_{ei}\right)},$$

$$\nu_{ei} = 8{,}83\cdot10^{-6}\cdot n_e\cdot T^{-3/2},\ \nu_{ea} = n_a\cdot V_{ea}\cdot\sigma_{ea}^{tr},$$

где ν_{ei} – частота столкновений электронов с ионами; ν_{ea} – частота столкновений электронов с атомами.

Численная методика. Расчетная область представляет собой прямоугольник, ограниченный сверху и снизу электродными стенками канала, справа – диэлектрической стенкой, а слева – выходной границей. Простота геометрии задачи позволяет получать численное решение на однородной прямоугольной сетке. Представленные далее результаты расчетов получены на разностной сетке 300×60 узлов (размеры расчетной ячейки $2\times0{,}8$ мм).

Детально численная методика описана в [6], здесь же отметим лишь основные ее моменты.

Пожалуй, наибольшую сложность представляло решение уравнения магнитной индукции (8), характеризующегося сильной нелинейностью, вызванной наличием членов, связанных с эффектом Холла. Как известно, МГД-задачи с эффектом Холла являются неустойчивыми, и поэтому такие задачи обычно решаются через потенциал электрического поля в приближении постоянства магнитной индукции или же с использованием вектора-потенциала магнитного поля. Численная методики [6] позволяет решать уравнение магнитной индукции в той форме, в которой оно записано в уравнении (8). Стоит также отметить, что дифференциальное уравнение (8) по своей природе является задачей с сильно переменными коэффициентами и большими градиентами, что также наложило свои ограничения на выбор метода решения. Преодолеть все описанные выше трудности удалось благодаря использованию абсолютно устойчивой схемы с экспоненциальной подгонкой [7].

Взаимодействие подсистемы Эйлера с уравнениями Максвелла осуществлялось при помощи метода расщеп-

ления по физически процессам [8], суть которого состоит в следующем.

На первом этапе учитывались конвективные потоки и газодинамическая сила, что достигалось решением подсистемы Эйлера явной TVD-схемой Хартена:

$$\frac{\vec{U}^* - \vec{U}^n}{\tau} + \frac{\partial}{\partial x}\left(G(\vec{U})\right)^n + \frac{\partial}{\partial y}\left(H(\vec{U})\right)^n = 0\,, \qquad (13)$$

где $\vec{U}$ – вектор газодинамических величин; τ – шаг по времени, определяемый из условия Куранта; n – номер временного слоя; $\vec{U}^*$ – промежуточное распределение.

На втором этапе в результате решения уравнения магнитной индукции находились распределения электрического и магнитного полей:

$$\frac{B^k - B^n}{\tau} = \frac{\partial}{\partial x}\left(\Gamma^* \frac{\partial B}{\partial x} - B \cdot u^*\right)^k + \frac{\partial}{\partial y}\left(\Gamma^* \frac{\partial B}{\partial y} - B \cdot v^*\right)^k + \vec{F}^k. \qquad (14)$$

На третьем этапе учитывались МГД-эффекты (сила Лоренца, джоулева диссипация) и объемные радиационные потери энергии:

$$\rho^* \frac{u^{k+1} - u^*}{\tau} = j_y^k B^k\,,$$

$$\rho^* \frac{v^{k+1} - v^*}{\tau} = -j_x^k B^k\,,$$

$$\rho^* \frac{\varepsilon^{k+1} - \varepsilon^*}{\tau} = \frac{\left(\vec{j}^k\right)^2}{\sigma^k} - q_0\left(T^k\right)^4\,, \qquad (15)$$

где k – номер внутренней итерации; ε – внутренняя энергия газа.

Для увеличения устойчивости метода производилась корректировка $\bar{U}^{k+1}$ при помощи метода нижней релаксации:

$$\bar{U}^{k+1} = \alpha\left(\vec{U}\right)^{k+1} + (1-\alpha)\vec{U}^k\,, \qquad (16)$$

где α – параметр нижней релаксации, равный 0,2. После достижения сходимости этого итерационного процесса полученное решение $\bar{U}^{k+1}$ принималось за решение на новом временном слое.

Результаты моделирования. Все представленные в данной статье результаты приведены в безразмерных единицах, для перевода этих величин в СИ нужно умножить их на соответствующий размерный множитель: $T = 10^4$ К, $V = 10^3$ м/с, $P = 10^5$ Па, $J = 10^5$ А/м^2, $E = 10^3$ В/м, $B = 1$ Тл, $m = 10^{-1}$ кг, $t = 10^{-3}$ с.

Для отражения динамики нестационарного процесса приведем одномерное распределение всех параметров по длине канала для четырех последовательных моментов времени (рис. 3). Характер расчетных кривых говорит о том, что начальный плазменный сгусток формируется в токовый слой, температура которого стабилизируется на уровне $2 \cdot 10^4$ К. Толщина Т-слоя ≈ 2…3 см, что должно обеспечивать гидродинамическую устойчивость поршневой структуры по отношению к неустойчивости Релея–Тейлора. Сопоставление взаимного расположения скачков плотности и пиков температуры приводит к выводу, что максимум плотности опережает максимум температуры на толщину Т-слоя. Таков непосредственный результат воздействия плазменного поршня на газ. Анализ распределения магнитного поля в канале показывает, что образуется ступенчатая структура с резким падением магнитной индукции на Т-слое. Это явление объясняется тем, что Т-слой не полностью экранирует магнитное поле, которое сохраняет достаточное значение. Токовый слой, подобно поршню, увлекает за собой холодный газ, поэтому давление в волне разрежения за Т-слоем сильно падает по мере продвижения плазмы по каналу. Как и ожидалось, низкое давление плазмы в хвосте токового слоя приводит к тому, что параметр Холла в волне разряжения достигает значительной величины. Однако из-за высокой температуры плазмы в МГД-канале происходит непрерывная эрозия электродов, которая обеспечивает приток массы газа в волну разрежения, в связи с чем давление (а вместе с ним и параметр Холла) в хвосте Т-слоя постепенно стабилизируется.

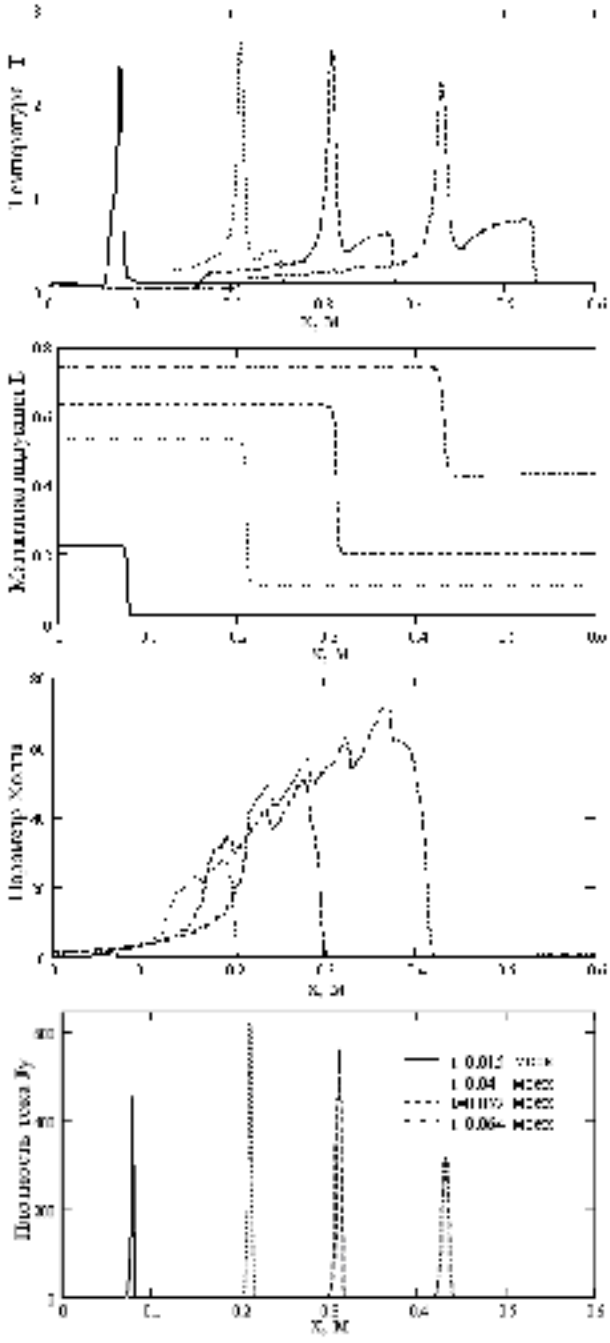
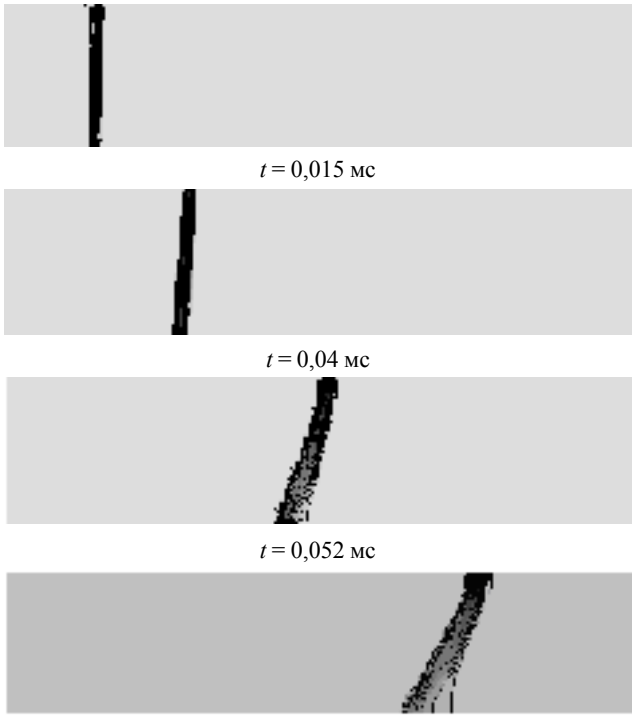


Рис. 3. Мгновенное распределение величин вдоль центральной линии МГД-канала

В используемой авторами численной методике приток массы от горящих электродов моделировался введением источника в уравнение неразрывности. Определение точного количества образующегося газа является весьма сложной задачей, но качественно можно считать, что интенсивность эрозии зависит от температуры по закону Аррениуса. Введение источника в уравнение неразрывности не только привело к уменьшению параметра Холла в волне разрежения до величин, соответствующих экспериментальным, но и в целом стабилизировало расчет.

Для большей наглядности приведем двумерное распределение плотности тока в расчетной области в виде изолинии (рис. 4). Поскольку параметр Холла в МГД-канале намного превышает единицу, то возникает достаточно большая холловская компонента силы тока, а вместе с ней и перпендикулярная потоку компонента силы Лоренца. Эта компонента приводит к тому, что токовый слой, оставаясь непроницаемым для холодного газа, отклоняется от ортогонального к электродам направления, т. е. имеет место ярко выраженное явление накренения плазменного сгустка.



t = 0,015 мс

t = 0,04 мс

t = 0,052 мс

t = 0,064 мс

Рис. 4. Изолинии плотности тока в диапазоне от 0 до 640 в различные моменты времени

Сопоставление расчетных данных с экспериментальными [2] (рис. 5) показывает, что численные результаты качественно верно описывают поведение Т-слоя в эксперименте.

Таким образом, разработан высокоэффективный численный алгоритм, позволяющий рассчитывать широкий класс двумерных нестационарных сильно неоднородных МГД-течений идеального газа, с большими значениями параметра Холла.

В результате применения разработанного алгоритма решена задача двумерного численного моделирования МГД-процесса эволюции плазменного сгустка в канале линейного ускорителя, что подтвердило существование наблюдаемого в экспериментах эффекта отклонения Т-слоя от направления, перпендикулярного электродам.

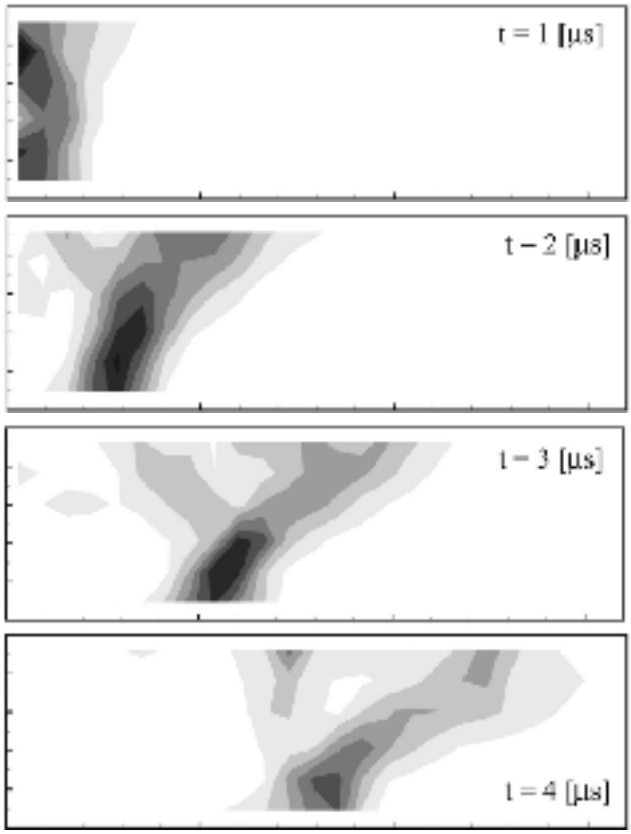


Рис. 5. Экспериментальные изолинии плотности тока в диапазоне от 0 до 400

Полученная система уравнений магнитной газодинамики в рассмотренной постановке хотя и не позволяет полностью описать начальную фазы развития токового слоя, тем не менее дает возможность качественно предсказать его поведение на более поздних этапах. Дальнейшее решение этой проблемы, по-видимому, потребует включения в обобщенный закон Ома слагаемого, связанного с градиентом давления, а также учета вязких сил и турбулентности.

В целом можно отметить, что наличие пространственных эффектов, существенно сказывающихся на работе МГД-устройства, в целом не отвергает идею создания эффективного МГД-ускорителя с неоднородным газоплазменным потоком.

Библиографический список

1. Славин, В. С. Диаграмма состояний стабилизированного токового слоя в канале МГД-генератора / В. С. Славин, Е. Н. Васильев, В. В. Овчинников // Докл. АН СССР. 1986. Т. 290, № 6. С. 1305–1309.

2. Гаврилов, А. А. Структура турбулентного неоднородного газоплазменного течения в канале магнитогидродинамического ускорителя / А. А. Гаврилов, В. С. Славин // Сб. докл. XXVI Сиб. теплофиз. семинара. Новосибирск, 2002.

3. Космическое применение магнитогидродинамических методов преобразования энергии с использованием

неоднородных газоплазменных потоков : монография / В. С. Славин, В. С. Соколов, К. А. Финников и др. ; под ред. В, С. Славина ; Краснояр. гос. техн. ун-т. Красноярск, 2004.

4. Marcusic, T. E. Phenomenological model of current sheet canting in pulsed electromagnetic accelerators / T. E. Marcusic, E. Y. Choueiri // 28th Intern. Electric Propulsion Conf. Toulouse, France, 2003. P. 0293.

5. Marcusic, T. E. Measurements of current sheet canting in pulsed electromagnetic accelerator / T. E. Marcusic, E. Y. Choueiri, J. W. Berkery // Physics of plasmas. 2004. Vol. 11. № 10.

6. Минаков, А. В. Численное моделирование нестационарных процессов, протекающих в канале рельсотрона : дисс. … магистра / А. В. Минаков ; Краснояр. гос. техн. ун-т. Красноярск, 2005.

7. Кузоватов, И. А. Анализ влияния эффекта Холла на структуру неравновесного плазменного слоя в канале МГД-генератора / И. А. Кузоватов, Т. А. Миловидова, В. С. Славин // Вычисл. технологии. Новосибирск, 2007. Т. 12, № 4. С. 73–84.

8. Марчук, Г. И. Методы расщепления / Г. И. Марчук. М. : Наука, 1988.

V. S. Slavin, I. A. Kuzovatov, A. V. Minakov

APPLICATION OF FINITE DIFFERENCE SCHEME WITH EXPONENTIAL FITTING FOR NUMERICAL SIMULATION OF UNSTEADY PROCESSES IN THE MHD CHANNEL

The highly effective numerical algorithm is developed and tested. It allows to solve a wide class of bidimentional non-stationary problems. Mathematical modeling of the non-stationary processes proceeding in the channel linear MHD – the accelerator is lead. In full statement the bidimentional problem of magnetic hydrodynamics in view of effect of the Hall is solved. In the result of modeling the deviation current effect of a layer from a direction, perpendicular to electrodes of the accelerator is found out. The results are will qualitatively coordinated with experimental data.

Keywords: exponential fitting, mathematical simulation of physical processes, computational meth-ods, computational hydrodynamics.

УДК 004.056.55

Т. А. Чалкин, К. М. Волощук

РАЗРАБОТКА АЛГОРИТМА ПОСТРОЕНИЯ УЗЛОВ ЗАМЕН АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147–89

Рассмотрены основные требования к проектированию узлов замен (S-блоков) блочных шифров и разработанный на их основе алгоритм построения узлов замен алгоритма шифрования ГОСТ 28147–89, обеспечивающий заданный уровень устойчивости шифра к линейному и дифференциальному криптоанализу.

Ключевые слова: шифрование, таблица замен, булева функция, криптостойкость, криптоанализ, алгоритм.

Отечественный стандарт алгоритма блочного симметричного шифрования – ГОСТ 28147–89 – [1] согласно действующему в Российской Федерации законодательству является обязательным к применению при криптографической защите секретных сведений любой степени секретности и рекомендуется к применению при защите конфиденциальных сведений, не составляющих государственную тайну, в частности при защите коммерческой тайны. При этом, помимо стандартной для всех симметричных шифров ключевой информации – последовательности бит фиксированной длины, называемой ключом шифрования (для ГОСТ 28147–89 длина ключа составляет 256 бит), этот стандарт в качестве элемента ключевой информации предусматривает использование таблицы замен, представляющей собой матрицу чисел размерности 8 × 16, которая содержит в своих ячейках числа от 0 до 15. Строки таблицы замен называются узлами замен. Назначение этой таблицы в целом аналогично назначению S-блоков алгоритма DES и подобных ему шифров, основанных на сети Фейстеля, – это перемешивание битов данных в ходе раунда шифрования путем замены отрезков блока данных по таблице, определяющей соответствие выходного значения входному.

Таблица замен является долговременным ключевым элементом, т. е. действует в течение гораздо более длительного срока, чем ключ шифрования. Предполагается, что она является общей для всех узлов шифрования в рамках одной криптосистемы. Также известно, что даже при нарушении секретности таблицы замен (когда она становится известной криптоаналитику) стойкость шифра остается достаточно высокой и не снижается ниже определенного предела [2].

Согласно действующему российскому законодательству, используемые при шифровании секретных сведе-