

Министерство науки и высшего образования РФ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Тверской государственный университет»

*Н.А. Семькина, И.А. Шаповалова*

# **МАТЕМАТИЧЕСКИЕ МОДЕЛИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Учебно-методическое пособие

Рекомендовано Ученым советом математического факультета федерального государственного бюджетного образовательного учреждения высшего образования «Тверской государственный университет» в качестве учебно-методического пособия для студентов, обучающихся по программе высшего образования по специальности 10.05.01 Компьютерная Безопасность

**Тверь 2020**

УДК 004.056(075.8)  
ББК 3972,52в631.0я73-1  
С30

Рецензент – доктор технических наук, профессор Д.С. Викторов

С30        **Семыкина, Н.А.** Математические модели в информационной безопасности: учебно-методическое пособие / Н.А. Семыкина, И.А. Шаповалова. – Тверь: Тверской государственный университет, 2020. – 126 с.

ISBN 978-5-7609-1573-3

В пособии представлены формализованные математические модели прикладных задач из области информационной безопасности. Приведена методика подхода к теоретическому и экспериментальному исследованию. Формулируются задачи, которые предлагается решить самостоятельно.

Пособие предназначено для студентов, обучающихся по специальности 10.05.01 Компьютерная Безопасность, а также для изучения курсов дисциплин: «Модели управляемых систем», «Управление нелинейными системами», «Математические методы оценки защищенности компьютерных сетей», «Анализ интеллектуальных систем».

ISBN 978-5-7609-1573-3

© Семыкина Н.А., Шаповалова И.А., 2020  
© Тверской государственный  
университет, 2020

## СОДЕРЖАНИЕ

<b>Введение</b>	5
<b>1. Этапы проведения исследования математических моделей</b>	6
<b>2. Математическая модель безопасного трафика компьютерной сети</b>	11
1.1. Постановка задачи	11
1.2. Дискретная аппроксимация непрерывной задачи	13
1.3. Исследование влияния параметров модели на решение задачи	15
<b>3. Математические модели распространения вредоносных программ</b>	20
3.1. Постановка задачи для модели MSEIRS	22
3.2. Применение принципа максимума Понтрягина для построения оптимального управления	24
3.3. Дискретная аппроксимация задачи	25
3.4. Анализ численных экспериментов	28
<b>4. Математическая модель информационного противоборства</b>	32
4.1. Классификация системно-динамических моделей информационного противоборства	33
4.2. Описание системно-динамической модели информационного противоборства	35
4.3. Постановка задачи	40
4.4. Применение необходимых условий оптимальности	41
4.5. Дискретная аппроксимация исходной задачи	42
4.6. Вычислительный эксперимент	43
<b>5. Математическая модель выбора оптимального набора средств защиты информации в корпоративной сети</b>	47
5.1. Постановка задачи	48
5.2. Исследование и анализ влияния параметров модели	50
<b>6. Математическая модель формирования защиты информации в распределенной сети</b>	54
6.1. Построение модели	56
6.2. Численная реализация и анализ результатов	58
<b>7. Математическая модель одновременного распространения легальных и контрафактных копий инновационного продукта</b>	64
7.1. Постановка задачи	64
7.2. Принцип максимума Понтрягина для случая протыкания траекторией поверхности переключения	65
7.3. Дискретная задача оптимального управления	69
7.4. Численное исследование модели	73
<b>8. Математическая модель распространения конкурирующей информации</b>	79
8.1. Построение модели	80
8.2. Необходимые условия оптимальности	83

8.3. Поиск численного решения задачи оптимального управления	85
8.4. Анализ зависимости численных решений от выбора параметров метода и модели	91
<b>9. Математическая модель обнаружение DDOS атак с помощью нечеткой нейронной сети</b>	101
9.1. Постановка задачи	103
9.2. Обучение нейронной сети	108
9.3. Программная реализация	114
<b>10. Задачи для самостоятельного исследования</b>	118
<b>Список использованных источников</b>	125

## ВВЕДЕНИЕ

Подготовка специалистов в области информационной безопасности является важным фактором в развитие кадрового потенциала для обеспечения информационной безопасности страны. Это отмечено в стратегических целях и основных направлениях доктрины информационной безопасности Российской Федерации. Учебно-методической компонентой системы подготовки кадров являются федеральные государственные образовательные стандарты высшего образования по специальностям, входящих в группу специальностей «Информационная безопасность». В настоящее время ведется работа по их актуализации с учетом профстандартов.

Согласно проекту федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность у выпускника должны быть сформированы установленные программой компетенции. Одна из общепрофессиональных компетенций (ОПК-3) – способность на основании совокупности существующих математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации.

Мощным подходом для решения и анализа задач информационной безопасности является аналитическое моделирование. Любая математическая модель представляет собой формальное описание цели, средств и результатов, а также способа связи средств с результатами. Преимуществом аналитического моделирования традиционно считается получение решения «в общем виде», а также высокая скорость моделирования конкретных сценариев для различных начальных условий. Кроме того, численные результаты, получаемые посредством таких моделей, позволяют анализировать поведение вирусов в сетях, состоящих из огромного числа элементов

На сегодняшний момент существует большое многообразие математических методов и моделей описания и нахождения оптимальных альтернатив решения в защите информации. В данном пособии представлены математические модели, которые формализованы как задачи оптимального управления.

В начале пособия представлена методика проведения исследования математических моделей. В отдельном разделе собраны примеры задач оптимального управления для самостоятельного исследования.

# 1. ЭТАПЫ ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ

Процесс исследования математической модели, которая формализуется как задача оптимального управления, можно разделить на несколько этапов. Рассмотрим эти этапы более подробно.

**1. Постановка задачи**, ее качественный анализ. Этот этап включает выделение важнейших черт и свойств моделируемого объекта и абстрагирование от второстепенных.

**2. Формализация модели**, выражение ее в виде конкретных математических зависимостей и отношений (функции, уравнения, неравенства и т.д.). В общем виде задачу оптимизации можно сформулировать следующим образом.

Требуется найти минимум функционала, определенного на заданном интервале  $[t_0, T]$ , состоящего из интегрального и терминального слагаемых

$$J(x(\cdot), u(\cdot)) = \int_{t_0}^T f_0(x(t), u(t)) dt + b(x(T)), \quad (1.1)$$

на множестве допустимых процессов  $\omega = (x(\cdot), u(\cdot))$ , удовлетворяющих следующей системе дифференциальных уравнений:

$$\dot{x}(t) = f(t, x(t), u(t)), \quad t \in [0, T], \quad (1.2)$$

с заданными начальными

$$x(t_0) \in \alpha, \quad \alpha \subset \mathbf{R}^n, \quad (1.3)$$

и граничными условиями

$$x(T) \in \beta, \quad \beta \subset \mathbf{R}^n. \quad (1.4)$$

В каждый момент времени  $t$  значение  $x(t)$  описывает данную систему. Назовем  $x$  - переменной состояния (или фазовой траекторией). Функция состояния  $x: [t_0, T] \rightarrow \mathbf{R}^n$  - абсолютно непрерывная вектор-функция. Функция  $u$  называется функцией управления. Управление

$u:[t_0, T] \rightarrow R^r$  является кусочно-непрерывной вектор-функцией и удовлетворяет ограничению

$$u(t) \in U \subseteq R^r, \text{ п. в. } t \in [t_0, T], \quad (1.5)$$

здесь  $U(t)$  фиксированное множество в  $\mathbf{R}^k$ , называемое управляемым множеством. Предполагаем, что все функции задачи непрерывно дифференцируемы по фазовой переменной и непрерывны по управлению.

Выписанную задачу оптимального управления можно рассматривать как задачу оптимизации функционала  $J(x, u)$ , при ограничениях (1.2) – (1.5). Характерным для ЗОУ является наличие дифференциальной связи (1.2) (уравнение процесса). Изменяя ограничения (1.3) – (1.5), можно получать различные ЗОУ для системы (1.2) и критерии качества (1.1).

Более сложные для анализа и исследования задачи содержат дополнительные условия: ограничения на переменные состояния

$$h(t, x(t)) \leq 0, \quad t \in [t_0, T],$$

где функция  $h$  непрерывна по  $t$  и непрерывно дифференцируема по  $x$ , смешанные ограничения

$$g(t, x(t), u(t)) \leq 0, \quad t \in [t_0, T],$$

где функция  $g$  непрерывно дифференцируема по совокупности аргументов.

**3. Анализ общих свойств модели.** Здесь применяются чисто математические приемы исследования. Наиболее важные моменты исследования – это доказательство существования и единственности решения. Задачи оптимального управления относятся к самым сложным экстремальным задачам. Наиболее эффективным методом исследования этих задач является принцип максимума Понтрягина, представляющий собой необходимое условие оптимальности.

Решение задач с помощью принципа максимума начинается с составления функции Понтрягина

$$H(t, x, u, \lambda_0, \lambda) = \lambda_0 f(t, x, u) + \lambda g(t, x, u).$$

Здесь вводится дополнительные функции  $(\lambda_0, \lambda) = (\lambda_0, \lambda_1, \dots, \lambda_n) : [t_0, T] \rightarrow \mathbf{R}^{n+1}$ , где  $\lambda_0$  - константа,  $\lambda$  - непрерывные функции. Назовем такие функции сопряженными вектор-функциями.

Если  $u^*$  является оптимальным управлением в задаче (1.1) – (1.5), а  $x^*$  - траектория, соответствующая оптимальному управлению. Тогда существует множитель  $(\lambda_0^*, \lambda^*) \neq (0, 0)$  и  $\forall \tau \in [t_0, t_1]$  имеем

$$H(\tau, x^*(\tau), u^*(\tau), \lambda_0^*, \lambda^*(\tau)) = \max_{v \in U} H(\tau, x^*(\tau), v, \lambda_0^*, \lambda^*(\tau));$$

при этом сопряженные вектор-функции удовлетворяют системе дифференциальных уравнений

$$\dot{\lambda}^* = - \frac{\partial H(t, x^*(t), u^*(t), \lambda_0^*, \lambda^*(t))}{\partial x}; \quad (1.6)$$

с условиями трансверсальности на правом конце

$$\lambda^*(T) = 0. \quad (1.7)$$

Принцип максимума позволяет трансформировать исходную задачу (1.1) – (1.5) к решению краевой задачи (1.2), (1.6), (1.3), (1.7), получение которого представляет значительную сложность и требует применения численных методов.

**4. Численное решение.** Этот этап включает разработку алгоритмов для численного решения задачи, написание программного кода и проведение расчетов. Трудности этого этапа осложняются целым рядом разнообразных причин: большой размерностью задач, наличие не дифференцируемых функционалов качества, возможностью появления многих экстремумов, наличие сложных ограничений.

Для построения численного решения аппроксимируем непрерывную модель к дискретной задаче заменой производных, например, по схеме Эйлера и интеграла – по правилу левых прямоугольников с шагом дискретизации  $\Delta t = Tq^{-1}$ . Ниже приведен алгоритм для решения задачи оптимального управления, используя метод проекции градиента.



**Алгоритм построения приближенного оптимального решения (метод проекции градиента)**

1. Зададим произвольный набор векторов управления  $(u^l)^{(0)}$ ,  $l = \overline{0, q-1}$ , здесь индекс в скобках означает номер итерации, в данном случае – нулевой.

2. Используя начальные значения  $(x^0)$  и набор  $(u^l)^{(0)}$ , вычислим  $x^l$ ,  $l = \overline{1, q}$ . В результате получим набор векторов  $x^1, \dots, x^q$ , соответствующий  $(u^l)^{(0)}$ , который обозначим  $(x^l)^{(0)}$ .

3. Вычислим значение целевого функционала  $J$ , используя  $(u^l)^{(0)}$  и  $(x^l)^{(0)}$ , и обозначим эту величину  $J^{(0)}$ . Здесь верхний индекс в скобках соответствует номеру итерации.

4. Определим сопряженные вектора  $(\lambda^{l+1})^{(0)}$  по рекуррентным формулам. Вычисление производится с конечного индекса  $q$  и заканчивая индексом 1.

5. Найдем управление  $u_i^l$ ,  $l = \overline{0, q-1}$ , соответствующее первой итерации  $(u^l)^{(1)}$ , по формуле (метод градиентного спуска)

$$(u_i^l)^{(k+1)} = (u_i^l)^{(k)} - \alpha^{(k)} \left( \frac{\partial L}{\partial u_i^l} \right)^{(k)},$$

где  $\alpha^{(k)} > 0$  – величина шага градиентного спуска,  $L(x, u, \lambda)$  – функция Лагранжа для данной задачи.

Для новых значений управления проверяем условия выполнения ограничений на управление. Если условие не выполняется, то строим проекцию управление на допустимое множество.

6. Аналогично строим  $(x^l)^{(1)}$ . Находим значение минимизируемой функционала  $J$ , используя  $(u^l)^{(1)}$  и  $(x^l)^{(1)}$ , и обозначим эту величину  $J^{(1)}$ . Вычислим приращение  $\Delta J^{(1)} = J^{(0)} - J^{(1)}$ .

7. Если  $\Delta J^{(1)} > 0$ , то заменим на втором шаге  $(u^l)^{(0)}$  на  $(u^l)^{(1)}$ ; если  $\Delta J^{(k)} \leq 0$ , то уменьшим шаг градиентного спуска  $\alpha^{(k)}$  в два раза и повторим процесс.

8. Итерационный процесс продолжим до тех пор, пока не выполнится одно из условий

$$\Delta J^{(k)} < \varepsilon; \quad \|u^{(k+1)} - u^{(k)}\| \leq \varepsilon; \quad \|x^{(k+1)} - x^{(k)}\| \leq \varepsilon,$$

где  $\varepsilon > 0$  - заданная точность.

Если разбиение шага  $\alpha^{(k)}$  не позволяет уменьшить минимизируемый функционал, то уменьшим  $\Delta t$  или переходим к другому методу.

**5. Анализ численных результатов.** На этом этапе встает вопрос о правильности и полноте результатов моделирования, о степени практической применимости последних. Анализ теоретических выводов и численных результатов, получаемых посредством модели, сопоставление их с имеющимися знаниями и фактами действительности позволяет обнаружить недостатки постановки задачи, сконструированной математической модели, ее информационного и математического обеспечения. В этом случае исходную постановку задачи и модель упрощают, снимают и объединяют условия, нелинейные соотношения заменяют линейными и т.д. Начав исследование с простой модели, можно быстро получить полезные результаты, а затем перейти к созданию более совершенной модели.

## **2. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ БЕЗОПАСНОГО ТРАФИКА КОМПЬЮТЕРНОЙ СЕТИ**

В современных условиях решение все более сложных задач управления различного рода системами и объектами, задач организационного управления основывается на широком использовании информационных технологий. Технической базой их практического применения являются корпоративные компьютерные сети (ККС). Именно они играют все возрастающую роль для обеспечения эффективности управления и успешного функционирования самых разных организаций. Практически в каждой такой сети наблюдается общая тенденция увеличения числа пользователей, объемов циркулирующей информации, интенсивности трафика и связанных с этими обстоятельствами ухудшения качества сетевых услуг.

Требования к повышению качества обслуживания сетей стимулировали развитие надежных систем с высокой устойчивостью к сбоям, что резко повысило интерес к исследованию свойств нагрузки в современных компьютерных системах. Анализ трафика является жизненно важным компонентом для понимания требований и возможностей сети.

Постоянный рост сетевого трафика вынуждает компании либо заменять маршрутизаторы, либо оптимизировать управление трафиком и топологию сети. Оптимальное использование имеющихся ресурсов является экономически более выгодными, а использование математического метода моделирования позволяет рассчитать необходимые характеристики оборудования.

### **2.1. Постановка задачи**

В качестве элементов вектора состояний  $\vec{x}(t)$  выступают величины  $x_{i,j}(t)$ , указывающие на интенсивность потока данных, находящегося в момент времени  $t$  на узле  $i$  и предназначенных узлу  $j$ . В качестве элементов  $u_{i,l}^j(t)$  вектора управления  $\vec{u}(t)$  выступают величины,

отображающие долю пропускной способности тракта  $(i, l)$ , выделенную в момент времени  $t$  потоку с адресом  $j$  из общей пропускной способности тракта передачи  $C_{i,l}$ . В роли возмущающего воздействия, приводящего к изменению переменных состояния, выступает мгновенная интенсивность абонентского потока  $y_{i,j}(t)$  с адресом  $j$ . [1-2] Тогда динамику информационного обмена в компьютерной сети может быть описана следующим уравнением:

$$\frac{dx_{i,j}(t)}{dt} = y_{i,j}(t) - \sum_{k \in E(i)} u_{k,i}^j(t) + \sum_{l \in I(i)} u_{i,l}^j(t), \quad (2.1)$$

где  $E(i)$  – множество трактов передачи, входящих в узел  $i$ ,  $I(i)$  – множество исходящих трактов,  $y_{i,j}(k) = \gamma_{i,j} \Delta t$  – объем нагрузки, поступающий в момент времени  $k$  на узел  $i$  и предназначенный узлу  $j$ , а  $\gamma$  – интенсивность поступающей нагрузки.

В соответствии с физическим смыслом на переменные следует наложить следующие ограничения:

$$0 \leq x_{i,j} \leq x_{i,j}^{max}, \quad 0 \leq u_{i,l}^j(t) \leq u_{i,l}^{j,max} \leq 1, \quad \sum_{n=1}^N u_{i,l}^n(t) \leq 1, \quad (2.2)$$

где  $x_{i,j}^{max}$  – максимальная длина очереди на  $i$ -ом узле для трафика с адресом  $j$ .

Теперь следует определить критерий оптимизации, т. е. какие именно значения нам следует минимизировать. С физической точки зрения это может быть либо суммарная задержка на маршрутизаторе

$$J1 = \int_0^T \sum_{i,j=1}^N d_{i,j} x_{i,j}(t) dt \rightarrow \min, \quad (2.3)$$

где  $d_{i,j}$  – коэффициенты приоритетов потоков.

Либо производительность системы

$$J2 = \sum_{k=0}^{q-1} \sum_{i=1}^n \sum_{\substack{j=1 \\ j \neq i}}^n b_{i,j}(k) u_{i,j}^j(k) \rightarrow \max.$$

Цель управления состоит в отыскании минимума функционала  $J$  с учетом ограничений на управление. В данной работе рассмотрим вариант с оптимизацией задержки (2.3).

Таким образом, задача детерминированного управления траффиком в рамках данной модели заключается в минимизации целевого функционала (2.3) по переменным  $u_{i,l}^j(t)$ , определяющих систему (2.1), при наличии приведенных ограничений (2.2). Полученный в результате вектор  $\vec{u}(t)$  и является искомым вектором оптимального управления.

Для построения решения применим методы теории оптимального управления и теории численных методов.

Используя метод штрафных функций, учтем ограничения (2.2) в минимизируемом функционале:

$$J = \int_0^T \sum_{i,j=1}^N d_{i,j} x_{i,j}(t) dt + A \int_0^T \sum_{i=1}^N \sum_{j=1}^N [\max\{-x_{ij}^l; 0\}]^2 dt + \\ + A \int_0^T \sum_{i=1}^N \sum_{j=1}^N [\max\{x_{ij}^l - x_{ij}^{max}; 0\}]^2 dt \rightarrow \min. \quad (2.4)$$

Здесь  $A$  – штрафной множитель, при этом  $A > 0$ .

Для решения задачи численным методом проекции градиента требуется привести имеющуюся задачу к дискретному виду.

## 2.2. Дискретная аппроксимация непрерывной задачи

Учитывая дискретный характер управления в компьютерной сети можно провести переход от записи в непрерывном виде к форме в дискретном времени с помощью метода Эйлера. Согласно методу Эйлера левая часть дифференциального уравнения (2.1) определяется в следующем виде

$$x'_{ij}(t_l) = \frac{x_{ij}^{l+1} - x_{ij}^l}{\Delta t}, \quad l = 0, 1, \dots, q - 1.$$

Перепишем формулу (2.1) с учетом этого равенства.

$$x_{i,j}^{l+1} = x_{i,j}^l - \sum_{l \in E(i)}^N C_{i,l} u_{i,j}^l \Delta t + \sum_{m \in I(i)}^N C_{m,i} u_{m,i}^l \Delta t + y_{i,j}^l.$$

Первая сумма описывает исходящий трафик, то есть все каналы, выходящие из узла  $i$ , вторая – входящий в узел  $i$  трафик.

В этом случае ограничения (2.2) будут иметь вид

$$0 \leq x_{i,j}^l \leq x_{i,j}^{max}, \quad 0 \leq u_{i,l}^j \leq u_{i,l}^{j,max} \leq 1, \quad \sum_{n=1}^N u_{i,l}^n \leq 1.$$

Для аппроксимации критерия оптимизации (1.3) воспользуемся методом левых прямоугольников. Проведя необходимые построения, в результате получим

$$\begin{aligned} I = & \sum_{l=0}^{q-1} \sum_{i=1}^N \sum_{j=1}^N d_{i,j} x_{i,j}^l \Delta t + A \sum_{l=0}^{q-1} \sum_{i=1}^N \sum_{j=1}^N [\max\{-x_{i,j}^l; 0\}]^2 \Delta t + \\ & + A \sum_{l=0}^{q-1} \sum_{i=1}^N \sum_{j=1}^N [\max\{x_{i,j}^l - x_{i,j}^{max}; 0\}]^2 \Delta t. \end{aligned}$$

Таким образом, получаем дискретную задачу оптимального управления, которую решим методом проекции градиента. Для этого запишем формулу Лагранжа для данной задачи.

$$\begin{aligned} L = & \lambda_0 \left( \sum_{l=0}^{q-1} \sum_{i=1}^N \sum_{j=1}^N d_{i,j} x_{i,j}^l \Delta t + A \sum_{l=0}^{q-1} \sum_{i=1}^N \sum_{j=1}^N [\max\{-x_{i,j}^l; 0\}]^2 \Delta t + \right. \\ & \left. + A \sum_{l=0}^{q-1} \sum_{i=1}^N \sum_{j=1}^N [\max\{x_{i,j}^l - x_{i,j}^{max}; 0\}]^2 \Delta t \right) + \\ & + \sum_{l=0}^{q-1} \sum_{i=1}^N \sum_{j=1}^N p_{i,j}^{l+1} (x_{i,j}^{l+1} - x_{i,j}^l + \sum_{\substack{k=1 \\ k \neq i}}^N b_{i,k}^l u_{i,k}^{j,l} - \sum_{\substack{m=1 \\ m \neq i,j}}^N b_{m,i}^l u_{m,i}^{j,l} - y_{i,j}^l). \end{aligned}$$

Продифференцируем функцию Лагранжа по фазовому вектору и управлению и запишем условия стационарности:

$$\frac{dL}{dx_{g,h}^c} = d_{g,h}\Delta t + 2A\Delta t \max\{-x_{gh}^c; 0\} + 2A\Delta t \max\{x_{gh}^c - x_{gh}^{max}; 0\} + p_{g,h}^c -$$

$$-p_{g,h}^{c+1} = 0, \quad g, h = 1, 2, \dots, N; c = 0, 1, \dots, q-1.$$

$$\frac{dL}{dx_{g,h}^q} = p_{g,h}^q = 0, \quad g, h = 1, 2, \dots, N.$$

$$\frac{dL}{du_{g,h}^{c,k}} = \begin{cases} 0, & g = h, g = c; \\ p_{g,c}^{k+1} b_{g,h}^k, & g \neq h, g = c; \\ p_{g,c}^{k+1} b_{g,h}^k - p_{h,c}^{k+1} b_{g,h}^k, & g \neq h, c. \end{cases}$$

$$g, h, c = 1, 2, \dots, N; k = 0, 1, \dots, q-1.$$

Будем рассматривать только регулярный случай ( $\lambda_0=1$ ), так как при  $\lambda_0=0$  задача не имеет смысла с физической точки зрения. Из условий стационарности выразим  $p_{g,h}^q$  и  $p_{g,h}^c$ ,  $c=0,1,\dots,q-1$ :

$$p_{g,h}^q = 0, \quad g, h = 0, 1, \dots, N,$$

$$p_{g,h}^c = p_{g,h}^{c+1} - d_{g,h}\Delta t + 2A\Delta t \max\{-x_{gh}^c; 0\} - 2A\Delta t \max\{x_{gh}^c - x_{gh}^{max}; 0\}.$$

Получены уравнения будем использовать для численного решения задачи методом проекции градиента.

### 2.3. Исследование влияния параметров модели на решение задачи

Для численного решения задачи рассмотрим компьютерную сеть [2], в которой требуется осуществить передачу информации между 5 узлами (рисунок 2.1).

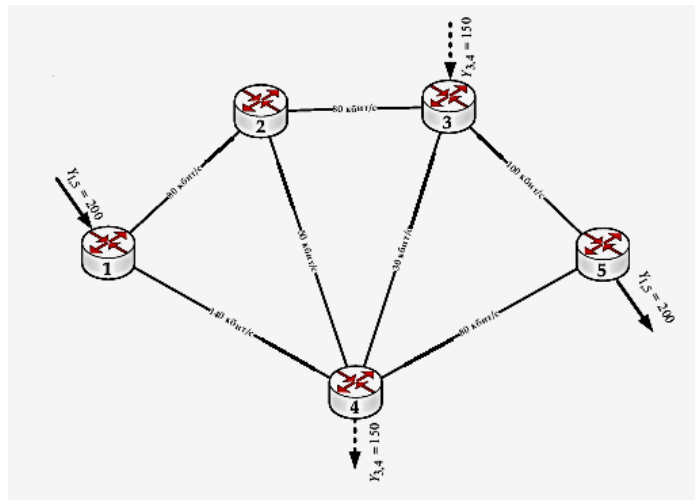


Рисунок 2.1. Пример исходной структуры телекоммуникационной сети

Определим следующие параметры метода: временной интервал прогноза  $[0, T]$ , где  $T = 15$ , точность вычислений  $= 0,0001$ ; штрафной коэффициент  $A = 1000$ .

В качестве начальных значений модели для анализа всех экспериментов примем следующие входные данные.

Начальные  $Y$

$Y$	1	2	3	4	5
1	0	0	0	0	200
2	0	0	0	0	0
3	0	0	0	150	0
4	0	0	0	0	0
	0	0	0	0	0

Топология сети

$C$	1	2	3	4	5
1	0	80	0	140	0
2	80	0	80	50	0
3	0	80	0	30	100
4	140	50	30	0	80
5	0	0	100	80	0

Максимальное значение  $X$

$X_{\max}$	1	2	3	4	5
1	0	80	0	80	0
2	80	0	80	80	0
3	0	80	0	80	80
4	80	80	80	0	80
5	0	0	80	80	0

Коэффициенты приоритетов

$d$	1	2	3	4	5
1	0	0	0	0	0,5
2	0	0	0	0	0
3	0	0	0	0,5	0
4	0	0	0	0	0
5	0	0	0	0	0

#### а) Влияние ограничений на управление на решение задачи

Выясним, как ограничение на пропускную способность тракта влияют на суммарную задержку на маршрутизаторе. Пусть максимальная доля пропускной способности тракта  $u_{i,l}^{j,\max}$  изменяется в следующем порядке: 1; 0.4; 0.1.

Таблица 2.1. Значения минимизируемой функции

Ограничение на управление $u_{i,l}^{j,\max}$	Количество итераций	Значение функции $J$
1	13930	5636729,5585
0,4	16063	23786347,5520
0,1	4188	118375299,3865



Заметим, что наличие ограничений приводит к значительному увеличению значений функции задержки. Ниже на рисунке 2.2 приведены значения задержки на линии 1 – 2 – 5 при разных значениях пропускной способности канала. Графики показывают, что ограничения увеличивают время, необходимое на уменьшение задержки.

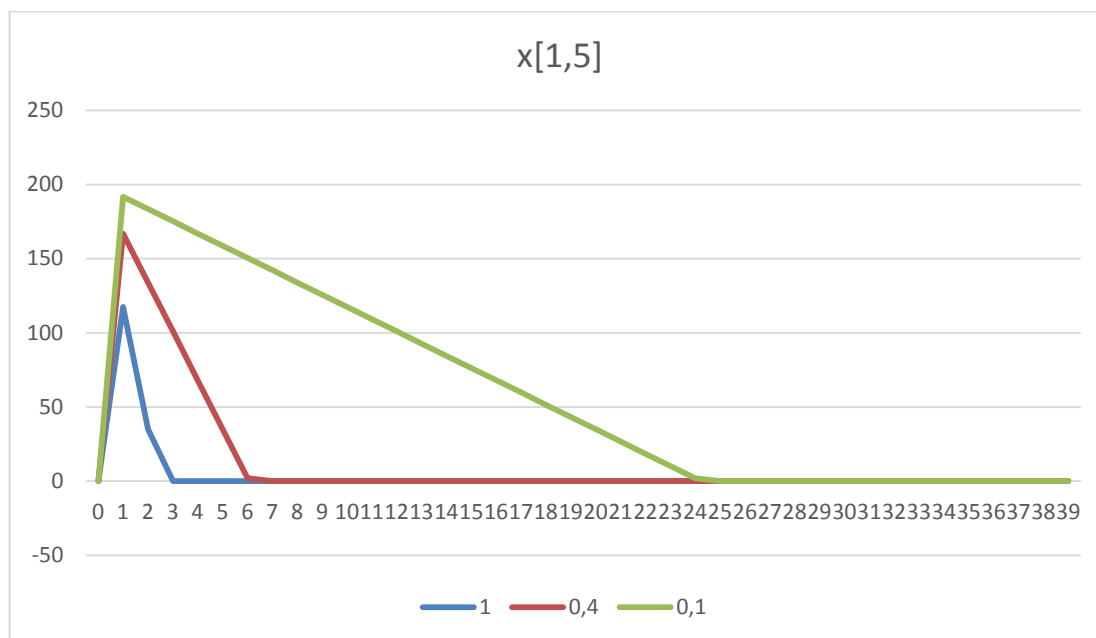


Рисунок 2.2. Динамика изменения средней межконцевой задержки пакетов

На рисунке 2.3 приведены графики функций управления, характеризующие пропускную способность тракта при соответствующих ограничениях для пути 1 – 2 – 5.

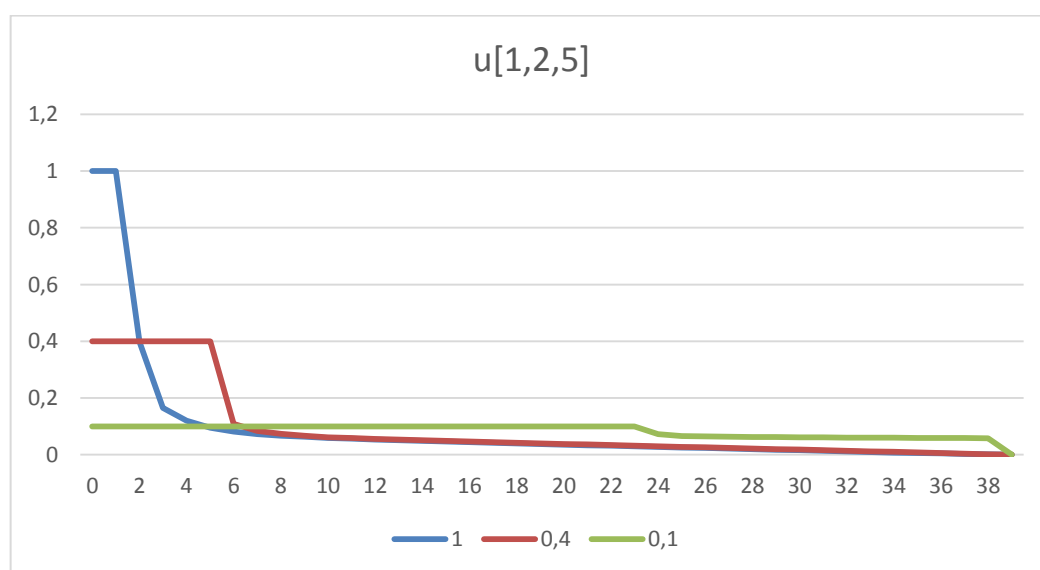


Рисунок 2.3. Динамика изменения пропускной способности канала

Наличие ограничений увеличивает время, необходимое для передачи данных по линии.

С точки зрения функции наличие ограничений на управление приводит к усложнению передачи данных. Но в реальной жизни иногда возникает необходимость резервирования части пропускной способности на случай непредвиденных обстоятельств.

*б) исследование влияния топологии на решение задачи*

Добавим в существующую сеть дополнительный канал 1 – 5 с пропускной способностью 140 кб/сек. В этом случае наличие дополнительного канала значительно – в 3,5 раза – уменьшает суммарную задержку сети, что демонстрирует таблица 2.2.

Таблица 2.2. Значение функции задержки

Дополнительный канал	Количество итераций	Значение функции J
0 кб/сек	13930	5636729,5585
140 кб/сек	13480	1584395,8778

Сравним графики динамики изменения задержки вдоль пути 1 – 5 напрямую и через второй маршрутизатор.

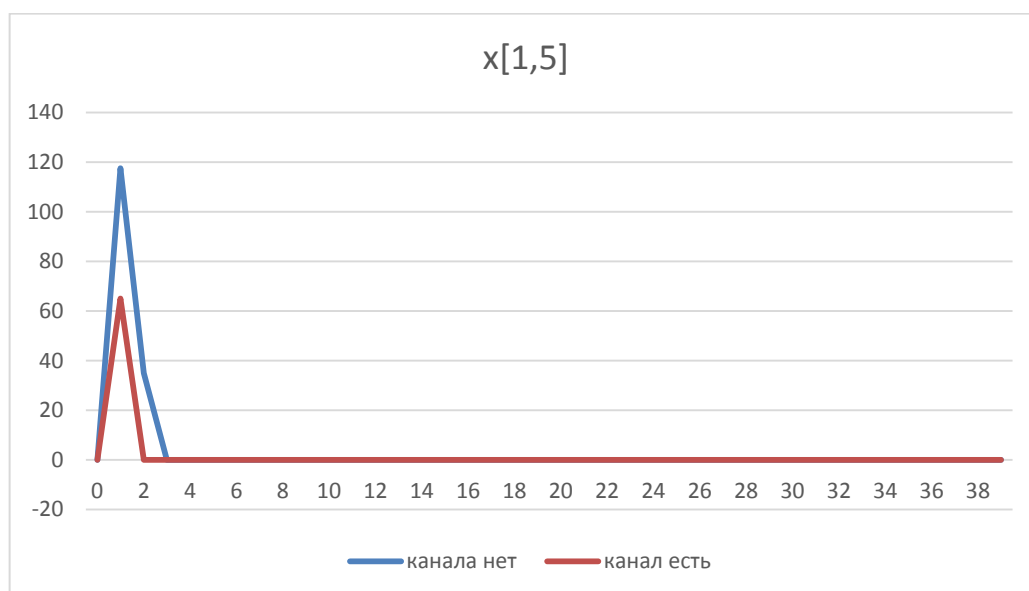


Рисунок 2.4. Динамика изменения средней межконцевой задержки пакетов

Из графиков видно, что дополнительный канал значительно уменьшил задержку на маршрутизаторе.

На рисунке 2.5 приведены графики динамики в пропускной способности канала.

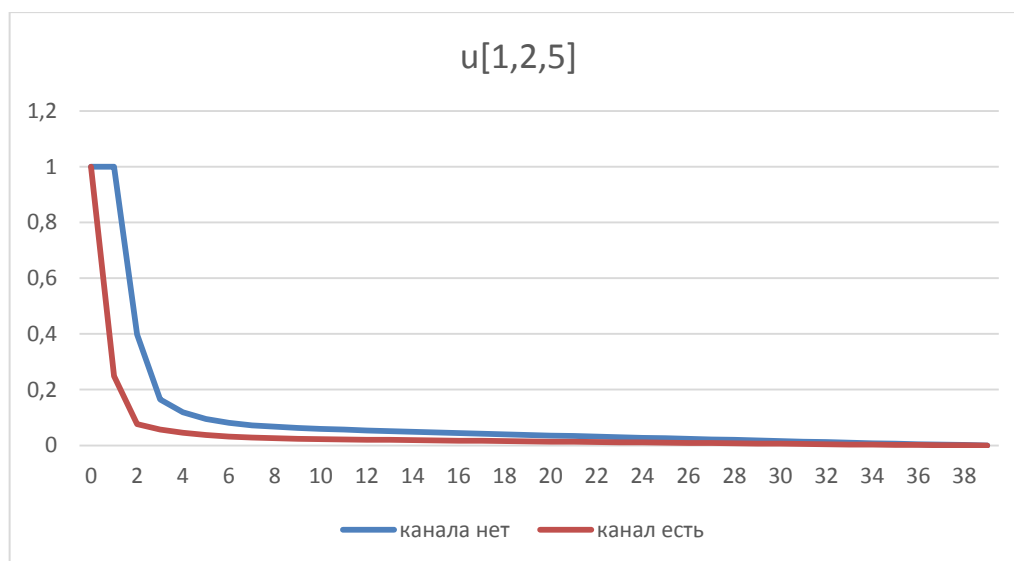


Рисунок 2.5. Динамика изменения пропускной способности канала

Наличие дополнительного канала приводит к равномерной разгрузке остальных, используемых для передачи данных от первого маршрутизатора к пятому.

Большее количество каналов позволяет быстрее передавать информацию от одного маршрутизатора к другому. Но не всегда возможно проложить эти каналы в здании корпорации. К тому же маршрутизаторы имеют физическое ограничение на количество подключаемых каналов. В случаи с пятью маршрутизаторами это ограничение можно не учитывать, но в больших корпорациях количество маршрутизаторов чаще всего достигает ста и более. К тому же дополнительные каналы хоть и уменьшает задержку передачи, но усложняет контроль над ней.

Данную модель можно использовать для создания шаблонов управления трафиком в корпоративной сети на основе реально существующих данных.

### 3. МАТЕМАТИЧЕСКИЕ МОДЕЛИ РАСПРОСТРАНЕНИЯ ВРЕДНОСНЫХ ПРОГРАММ

На сегодняшний день разработано множество математических моделей распространения вредоносных программ, большая часть которых базируется на стандартных моделях, описывающих поведение биологических вирусов. Многие встречающихся в литературе модели распространения червей представляют собой, так называемые, детерминированные модели эпидемий. Они пригодны для моделирования эпидемии в той фазе, когда число инфицированных хостов достигло больших значений. Рассмотрим несколько простых моделей, описывающих динамику распространения сетевых червей [3-4].

1) **SIS-модель** (простая эпидемическая модель, или «Susceptible – Infected – Susceptible model»)

Произвольный хост сети, состоящей из постоянного количества  $N$  хостов, может находиться в двух состояниях – уязвимом ( $S$ ) и инфицированном ( $I$ ), т.е.  $S + I = N$ .

При инфицировании хоста копия червя случайным образом выбирает в доступном адресном пространстве потенциальную жертву со средней постоянной скоростью  $\lambda$  хостов в секунду. На поиск и заражение одного хоста в среднем тратится  $1/\lambda$  секунд.

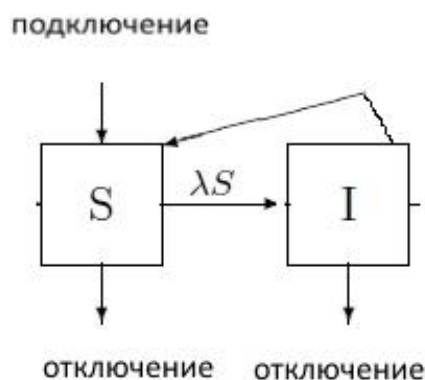


Рисунок 3.1. Схема модели SIS

В простейшем случае  $\lambda$  определяется средней скоростью сканирования червем сети ( $V$ ) и размером ее адресного пространства ( $N_{ip}$ ):

$$\lambda = V N / N_{ip},$$

где согласно спецификации протокола IP4  $N_{ip} = 2^{32}$ .

## 2) SIR-модель («Susceptible – Infected – Removed model»)

Для оценки факторов, обеспечивающих затухание сетевых эпидемий, можно использовать SIR-модель. В ней хосты существуют в трех состояниях: уязвимом ( $S$ ), зараженном ( $I$ ) и невосприимчивом ( $R$ ). Таким образом,  $S+I+R = N$ . Узлы оказываются неуязвимыми только после излечения от вредоносного кода.

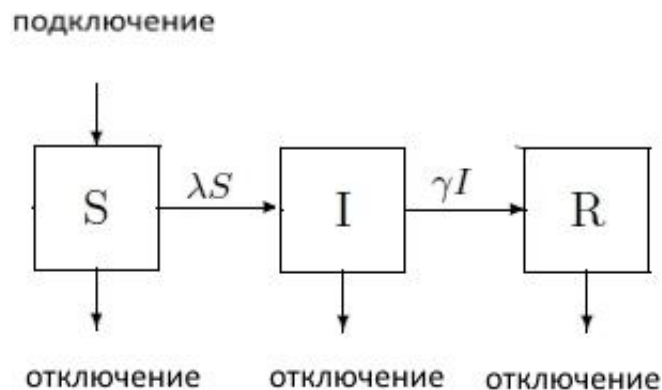


Рисунок 3.2. Схема модели SIR

Постоянная  $\gamma$ , характеризует среднюю скорость «иммунизации» в единицу времени.

## 3) SEIR-модель («Susceptible – Exposed – Infected – Removed model»)

В этой модели учитывается возможность того, что червь может иметь некий «инкубационный период», во время которого вирус не наносит какого-либо вреда инфицированному узлу. Обычно червь заражает уязвимый узел ( $S$ ) до входа в свою латентную стадию. В течение латентного периода ( $E$ , Exposed) узел считается зараженным, но не распространяет вирус. Через некоторое время он становится способным к заражению других хостов ( $I$ ) и далее становится «излеченным» ( $R$ ). В SEIR-модели требуется дополнительно вводить соотношение, характеризующее отношение между состояниями  $E$  и  $I$ .

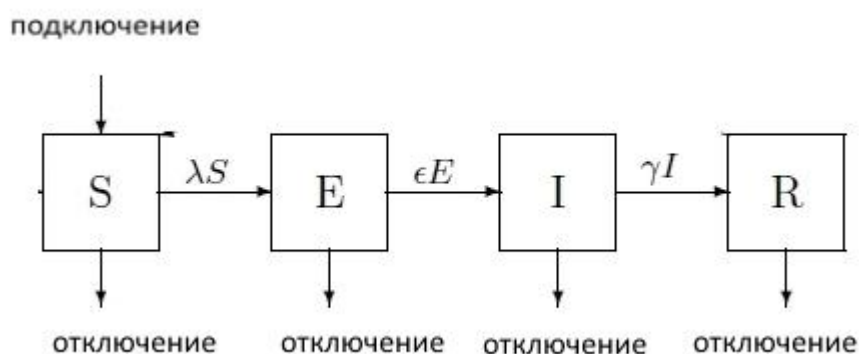


Рисунок 3.3. Схема модели SEIR

Коэффициент  $\epsilon$ , характеризует средний период, когда компьютер является зараженным, но сам вирус не активен.

Модели SIR, SIS, SEIR являются наиболее распространенными моделями в классической эпидемиологии. Данные модели предполагают, что каждая особь в популяции может находиться в одном из нескольких состояний и с течением времени переходить из одних состояний в другие. Модели базируются на составлении дифференциальных уравнений, описывающих зависимость количества зараженных особей от времени. Рассмотрим более подробно усовершенствованную модель MSEIRS.

### 3. 1. Постановка задачи для модели MSEIRS («Maternally derived immunity – Susceptible – Exposed – Infected – Removed model»)

Для оценки факторов, обеспечивающих затухание сетевых эпидемий, можно использовать MSEIRS-модель. В ней хосты (сетевые компьютеры) существуют в пяти состояниях: обладающие пассивным иммунитетом (M); уязвимые (S); зараженные, находящиеся в латентной стадии (E); зараженные, распространяющие заболевание (I); неподверженные заболеванию (R). Таким образом,  $M+S+E+I+R=N$ , где N – общее количество компьютеров в сети.

В реальных условиях «лечение» происходит за счет установки антивирусного программного обеспечения или межсетевых экранов. Скорость обновления антивирусных баз и их устаревание обозначим через константы  $\gamma$  и  $\delta$  соответственно.

Предположим, что со скоростью  $\mu$  компьютеры отключаются от сети, при этом отключение не связано с вирусной атакой, с частотой  $\theta$  осуществляется прирост новых компьютеров.

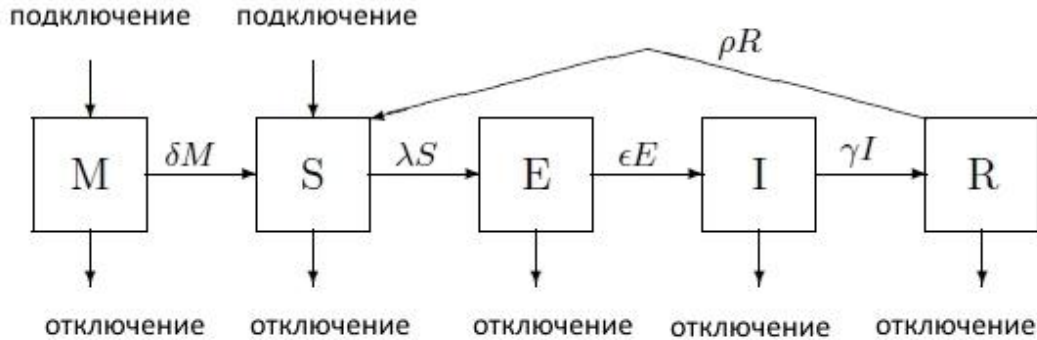


Рисунок 3.4. Схема модели MSEIR

Неподверженные заболеванию индивиды могут со временем терять иммунитет и переходить в группу уязвимых с интенсивностью  $\rho$ .

Как было сказано ранее, через  $\lambda$  обозначим среднюю скорость заражения, через константу  $\varepsilon$  – средний период, когда компьютер является зараженным, но сам вирус не активен.

Система дифференциальных уравнений, описывающая состояние компьютерной сети имеет следующий вид

$$\begin{aligned}
 \frac{dM}{dt} &= \theta (N - S) - (\delta + \mu)M + \rho R, \\
 \frac{dS}{dt} &= \theta N + \delta M - \frac{\lambda SI}{N} - \mu S, \\
 \frac{dE}{dt} &= \frac{\lambda SI}{N} - (\varepsilon + \mu)E, \\
 \frac{dI}{dt} &= \varepsilon E - (\gamma + \mu)I, \\
 \frac{dR}{dt} &= \gamma I - (\rho + \mu)R.
 \end{aligned} \tag{3.1}$$

Рассмотрим исходную модель в виде задачи оптимального управления. Для этого введем кусочно-непрерывную функцию управления  $\gamma(t)$ , характеризующую среднюю скорость установки антивирусного программного обеспечения для восприимчивых узлов. Функция управления  $\gamma(t)$  почти всюду на  $[0, T]$  удовлетворяет неравенству:

$$0 \leq \gamma(t) \leq Y_{max} \leq 1, t \in [0, T]. \quad (3.2)$$

Данное ограничение связано с техническими и экономическими возможностями. Здесь  $Y_{max}$  – максимальная норма управления.

Для оценки защищенности компьютерной сети будем использовать критерий, который учитывает требование, что в конечный момент времени рассматриваемого периода большинство компьютеров (более 80% ) являются невосприимчивым к заражению. В результате задача управления будет состоять в минимизации функционала

$$J(\cdot) = A \max\{(0,8 N(T) - R(T))^2, 0\}, \quad (3.3)$$

где  $A$  – масштабирующий множитель,  $R(T)$  и  $N(T)$  – значения в последний момент времени количество неподверженных заражению и общее количество компьютеров соответственно.

### 3.2. Применение принципа максимума Понтрягина для построения оптимального управления

Сформулируем необходимые условия оптимальности. Функция Понтрягина построенной задачи оптимального управления имеет вид

$$\begin{aligned} H(t, M, S, E, I, R, \gamma, p_M, p_S, p_E, p_I, p_R) = \\ = p_M(\theta(M + E + I + R) - (\delta + \mu)M - \rho R) + p_S\left(-\frac{\beta SI}{N} - \mu S - \theta N + \delta M\right) + \\ + p_E\left(\frac{\beta SI}{N} - (\varepsilon + \mu)E\right) + p_I(\varepsilon E - (\gamma(t) - \mu)I) + p_R(\gamma(t)I - (\rho + \mu)R). \end{aligned}$$

Сопряженные вектор-функции  $p_M, p_S, p_E, p_I, p_R$  являются кусочно-непрерывно дифференцируемыми функциями.

Согласно необходимым условиям оптимальности локально оптимальный процесс  $[\bar{M}(t), \bar{S}(t), \bar{E}(t), \bar{I}(t), \bar{R}(t), \bar{\gamma}(t)]$  в задаче (3.1) – (3.3) удовлетворяет принципу максимума Понтрягина в точках непрерывности

$$\begin{aligned} \max_{0 \leq \gamma(t) \leq Y_{max}} H(t, M, S, E, I, R, \gamma, p_M, p_S, p_E, p_I, p_R) = \\ = H(t, \bar{M}, \bar{S}, \bar{E}, \bar{I}, \bar{R}, \bar{\gamma}, \bar{p}_M, \bar{p}_S, \bar{p}_E, \bar{p}_I, \bar{p}_R) \end{aligned}$$

и уравнениям Эйлера с условиями трансверсальности на правом конце траектории:



$$\left\{ \begin{array}{l} \frac{d\bar{p}_m}{dt} = -\left(\theta p_M + (\delta + \mu)p_M + \theta p_S - \beta(p_S - p_E) \frac{SI}{N^2} + \delta p_M\right), \\ \frac{d\bar{p}_S}{dt} = -\left(\mu p_S - \theta p_S + \beta(p_S - p_E) \frac{I(M+E+I+R)}{N^2}\right), \\ \frac{d\bar{p}_E}{dt} = -\left(\varepsilon p_E - \mu p_E - \varepsilon p_I - \theta p_S - \beta(p_S - p_E) \frac{SI}{N^2} + \theta p_M\right), \\ \frac{d\bar{p}_I}{dt} = -\left(\gamma p_I - \mu p_I + \gamma p_R - \theta p_S + \beta(p_S - p_E) \frac{S(M+E+S+R)}{N^2} + \theta p_M\right), \\ \frac{d\bar{p}_R}{dt} = -(\mu p_R - \theta p_S - \beta(p_S - p_E) \frac{SI}{N^2} + \theta p_M + \rho p_M - \rho p_R). \end{array} \right. \quad (3.4)$$

$$\begin{aligned} p_M(T) &= -1,6A \max\{0,8 N(T) - R(T); 0\}, \\ p_S(T) &= -1,6A \max\{0,8 N(T) - R(T); 0\}, \\ p_E(T) &= -1,6A \max\{0,8 N(T) - R(T); 0\}, \\ p_I(T) &= -1,6A \max\{0,8 N(T) - R(T); 0\}, \\ p_R(T) &= 0,4A \max\{0,8 N(T) - R(T); 0\}. \end{aligned} \quad (3.5)$$

Так как функции управления входят линейно в функцию Понтрягина, то можно выписать функцию переключения

$$\varphi(t) = -p_I I + p_R I.$$

Согласно принципу максимума, оптимальное управление определяется из следующих условий:

$$\gamma(t) = \begin{cases} Y_{max} & \text{если } \varphi(t) > 0 \\ 0 & \text{если } \varphi(t) < 0 \\ \gamma \in [0, Y_{max}] & \text{если } \varphi(t) = 0 \end{cases} \quad (3.6)$$

В результате получаем краевую задачу принципа максимума Понтрягина, состоящую из системы дифференциальных уравнений (3.1), (3.4) с краевыми условиями (3.5), где оптимальное управление определяется формулой (3.6).

### 3.3. Дискретная аппроксимация задачи

Для численного решения задачи построим дискретную аппроксимацию, используя численные методы. На отрезке  $[0, T]$  введем равномерную сетку  $\{t_i = \Delta t \cdot i, 0 \leq i \leq N\}$  с шагом  $\Delta t = T/N$ . Обозначим значения фазовых функций и функций управления в точках разбиения:  $M(t_i) = M^i, S(t_i) = S^i, E(t_i) = E^i, R(t_i) = R^i, I(t_i) = I^i, \gamma(t_i) = \gamma^i$ . Используя явную разностную схему и квадратурную формулу

прямоугольников, получаем следующую дискретную задачу оптимального управления:

$$\left\{ \begin{array}{l} M_{i+1} = M_i + \Delta t (\theta (n - S_i) - (\mu + \delta)M_i + \rho R_i), M^0 = M_0; \\ S_{i+1} = S_i + \Delta t \left( \theta n + \delta M_i - \frac{\lambda S_i I_i}{n} - \mu S_i \right), S^0 = S_0; \\ E_{i+1} = E_i + \Delta t \left( \frac{\lambda S_i I_i}{n} - (\varepsilon + \mu)E_i \right), E^0 = E_0; \\ I_{i+1} = I_i + \Delta t (\varepsilon E_i - (\gamma + \mu)I_i), I^0 = I_0; \\ R_{i+1} = R_i + \Delta t (\gamma I_i - (\rho + \mu)R_i), R^0 = R_0. \end{array} \right. \quad (3.7)$$

Ограничения на управление (2.2) запишутся в виде

$$0 < \gamma^i \leq Y_{max} \leq 1.$$

Требуется минимизировать функционал

$$J = A \max\{0, 8 N_i^q - R_i^q; 0\} \rightarrow \inf.$$

Применим для построенной дискретной задачи метод множителей Лагранжа. Функция Лагранжа для задачи будет иметь вид

$$\begin{aligned} L = & A(\max\{0, 8 N_i^q - R_i^q; 0\})^2 + \\ & + \sum_{k=0}^{q-1} p m_i^{k+1} \left( M_i^{k+1} - M_i^k - \Delta t (\theta (M_i^k + E_i^k + I_i^k + R_i^k) - (\delta + \mu)M_i^k - \rho R_i^k) \right) \\ & + \sum_{k=0}^{q-1} p s_i^{k+1} \left( S_i^{k+1} - S_i^k - \Delta t \left( \theta N_i^k - \frac{\lambda S_i^k I_i^k}{N_i^k} - \mu S_i^k + \delta M_i^k \right) \right) + \\ & + \sum_{k=0}^{q-1} p e_i^{k+1} \left( E_i^{k+1} - E_i^k - \Delta t \left( \frac{\lambda S_i^k I_i^k}{N_i^k} - \mu E_i^k - \varepsilon E_i^k \right) \right) + \\ & + \sum_{k=0}^{q-1} p i_i^{k+1} \left( I_i^{k+1} - I_i^k - \Delta t (\varepsilon E_i^k - \gamma_i^k I_i^k - \mu I_i^k) \right) + \\ & + \sum_{k=0}^{q-1} p r_i^{k+1} \left( R_i^{k+1} - R_i^k - \Delta t (\gamma_i^k I_i^k - \mu R_i^k - \rho R_i^k) \right). \end{aligned}$$

Для построенной функции Лагранжа выпишем условия стационарности.

а) по фазовым переменным

$$\frac{dL}{dM_i^k} = p m_i^k - p m_i^{k+1} - \Delta t (\theta p m_i^{k+1} + (\delta + \mu) p m_i^{k+1} + \theta p s_i^{k+1} -$$

$$\begin{aligned}
& -\lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k I_i^k}{(N_i^k)^2} + \delta pm_i^{k+1}) = 0, \\
\frac{dL}{dS_i^k} &= ps_i^k - ps_i^{k+1} - \Delta t(\mu ps_i^{k+1} - \theta ps_i^{k+1} + \\
& + \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{I_i^k(M_i^k + I_i^k + E_i^k + R_i^k)}{(N_i^k)^2}) = 0, \\
\frac{dL}{dE_i^k} &= pe_i^k - pe_i^{k+1} - \Delta t(\epsilon pe_i^{k+1} - \mu pe_i^{k+1} - \epsilon pi_i^{k+1} - \theta ps_i^{k+1} - \\
& - \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k I_i^k}{(N_i^k)^2} + \theta pm_i^{k+1}) = 0, \\
\frac{dL}{dI_i^k} &= pi_i^k - pi_i^{k+1} - \Delta t(\gamma_i^k pi_i^{k+1} - \mu pi_i^{k+1} + \gamma_i^k pr_i^{k+1} - \theta ps_i^{k+1} + \\
& + \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k(M_i^k + S_i^k + E_i^k + R_i^k)}{(N_i^k)^2} + \theta pm_i^{k+1}) = 0, \\
\frac{dL}{dR_i^k} &= pr_i^k - pr_i^{k+1} - \Delta t(\mu pr_i^{k+1} - \theta ps_i^{k+1} - \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k I_i^k}{(N_i^k)^2} + \\
& + \theta pm_i^{k+1} + \rho pm_i^{k+1} - \rho pr_i^{k+1}) = 0, \\
\frac{dL}{dM_i^q} &= pm_i^q + 1,6A \max\{0,8 N_i^q - R_i^q; 0\} = 0, \\
\frac{dL}{dS_i^q} &= ps_i^q + 1,6A \max\{0,8 N_i^q - R_i^q; 0\} = 0, \\
\frac{dL}{dE_i^q} &= pe_i^q + 1,6A \max\{0,8 N_i^q - R_i^q; 0\} = 0, \\
\frac{dL}{dI_i^q} &= pi_i^q + 1,6A \max\{0,8 N_i^q - R_i^q; 0\} = 0, \\
\frac{dL}{dR_i^q} &= pr_i^q - 0,4 \max\{0,8 N_i^q - R_i^q; 0\} = 0.
\end{aligned}$$

b) По переменным управления

$$\frac{dL}{d\gamma_{i-1}^k} = \Delta t I_{i-1}^k (pi_{i-1}^{k+1} - pr_{i-1}^{k+1}) = 0.$$

Из данных условий получаем выражения для вычисления импульсов:

$$\begin{aligned}
pm_i^k &= pm_i^{k+1} + \Delta t(\theta pm_i^{k+1} + (\delta + \mu) pm_i^{k+1} + \theta ps_i^{k+1} - \\
& - \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k I_i^k}{(N_i^k)^2} + \delta pm_i^{k+1}), \\
ps_i^k &= ps_i^{k+1} + \Delta t(\mu ps_i^{k+1} - \theta ps_i^{k+1} + \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{I_i^k(M_i^k + I_i^k + E_i^k + R_i^k)}{(N_i^k)^2}) \\
pe_i^k &= pe_i^{k+1} + \Delta t(\epsilon pe_i^{k+1} - \mu pe_i^{k+1} - \epsilon pi_i^{k+1} - \theta ps_i^{k+1} - \\
& - \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k I_i^k}{(N_i^k)^2} + \theta pm_i^{k+1}) \\
pi_i^k &= pi_i^{k+1} + \Delta t(\gamma_i^k pe_i^{k+1} - \mu pi_i^{k+1} + \gamma_i^k pr_i^{k+1} - \theta ps_i^{k+1} +
\end{aligned}$$

$$\begin{aligned}
& +\lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k(M_i^k + S_i^k + E_i^k + R_i^k)}{(N_i^k)^2}, \\
pr_i^k &= pr_i^{k+1} + \Delta t(\mu pr_i^{k+1} - \theta ps_i^{k+1} - \lambda(ps_i^{k+1} - pe_i^{k+1}) \frac{S_i^k I_i^k}{(N_i^k)^2} + \\
& + \theta pm_i^{k+1} + \rho pm_i^{k+1} - \rho pr_i^{k+1}), \\
pm_i^q &= -1,6A \max\{0,8 N_i^q - R_i^q; 0\}, \quad ps_i^q = -1,6A \max\{0,8 N_i^q - R_i^q; 0\}, \\
pe_i^q &= -1,6A \max\{0,8 N_i^q - R_i^q; 0\}, \quad pi_i^q = -1,6A \max\{0,8 N_i^q - R_i^q; 0\}, \\
pr_i^q &= 0,4 \max\{0,8 N_i^q - R_i^q; 0\}.
\end{aligned}$$

Перечисленные выше формулы можно использовать для численных экспериментов, с помощью которых проанализировать зависимость решения задачи от параметров модели.

### 3.4. Анализ численных экспериментов

Для построения приближенного оптимального решения воспользуемся методом проекции градиента.

Рассмотрим случай, когда число узлов, восприимчивых к вредоносному коду, очень большое,  $S(0) = 75000$ , антивирус для данного вида вируса не обновлен. В начальный период количество зараженных компьютеров  $I(0) = 101$ , неподверженных вирусу узлов  $R(0) = 500$ , а компьютеров, находящихся в латентном состоянии,  $E(0) = 302$ .

Пусть антивирусные базы обновляются со скоростью  $\gamma = 0,01$ ; скорость заражения  $\lambda = 0,06$ ; частота отключения и подключения компьютеров  $\mu = \theta = 0,0001$ ; компьютеры переходят из латентное состояние со скоростью  $\varepsilon = 0,016$ ; средний период действия антивирусных баз  $\rho = 0,01$ . Т. е. антивирусные базы обновляются с такой же скоростью, как и устаревают.

Ниже на рисунке 3.5 приведены траектории динамики функций, характеризующие количество компьютеров разных типов. Из приведенных графиков можно заметить, что при большой скорости распространения вредоносного кода за рассматриваемый период удастся погасить

эпидемию. При этом выполнено требование, что в конечный момент времени рассматриваемого периода количество невосприимчивых компьютеров  $R(t)$  составляет более 80% (а именно 89,9%).

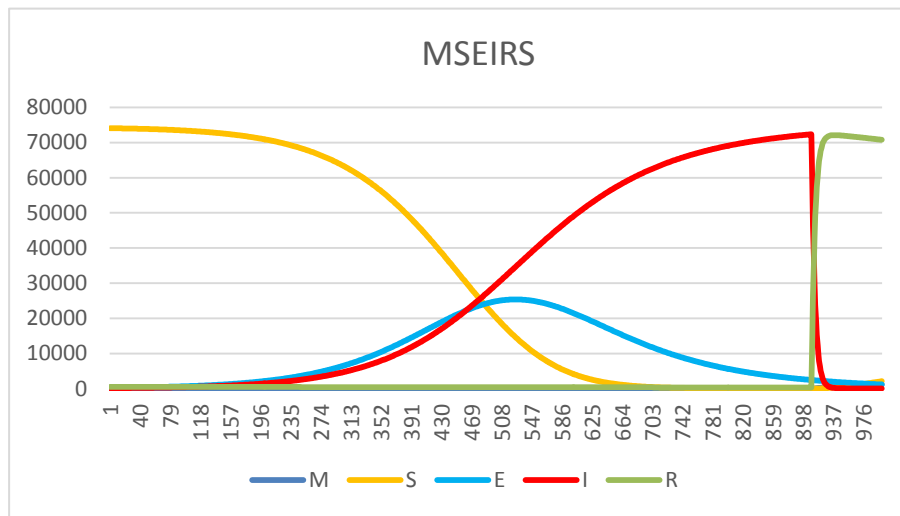


Рисунок 3.5. Графики функций, характеризующие состояние сети

Исследуем, как начальные значения функций влияют на решение задачи и отражаются на зараженности компьютеров в целом.

Пусть компьютеров с активной антивирусной программой по-прежнему нет, подверженных заражению  $S(0) = 6500$ , в латентном состоянии и зараженных одинаковое количество  $E(0) = I(0) = 33900$ , неподверженных заражению  $R(0) = 775$ . В этом случае мы получаем схожий результат, представленный на рисунке 3.6.

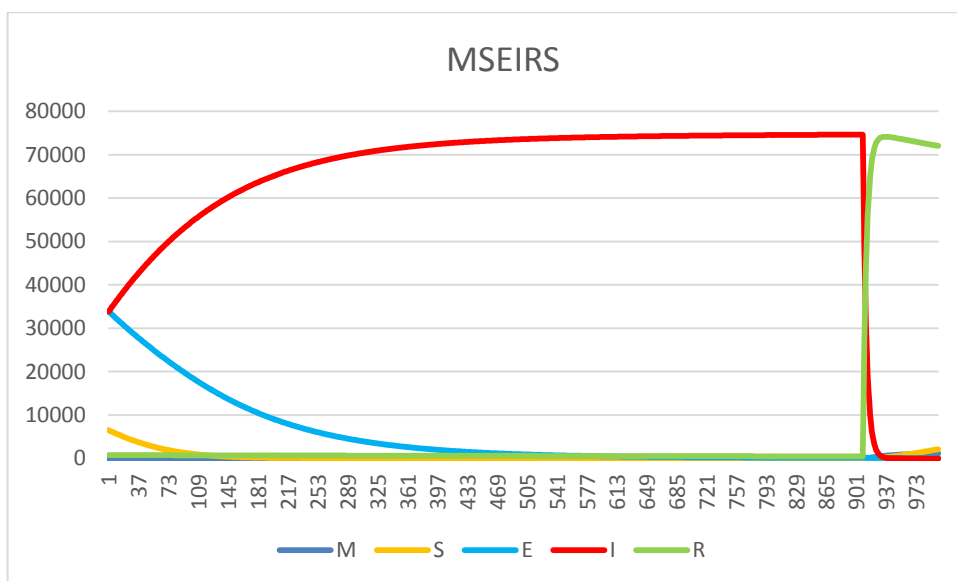


Рисунок 3.6. Графики функций, характеризующие состояние сети

В конечный момент времени рассматриваемого периода количество зараженных близко к 0, а неподверженных вирусом близко к максимуму.

Рассмотрим нештатную ситуацию, когда в начальный период зараженных компьютеров большое число,  $I(0) = 74001$ , антивирусы по-прежнему с неактуальными базами данных, подверженных заражению  $S(0) = 197$ , в латентном состоянии  $E(0) = 302$ , а неподверженных  $R(0) = 500$ .

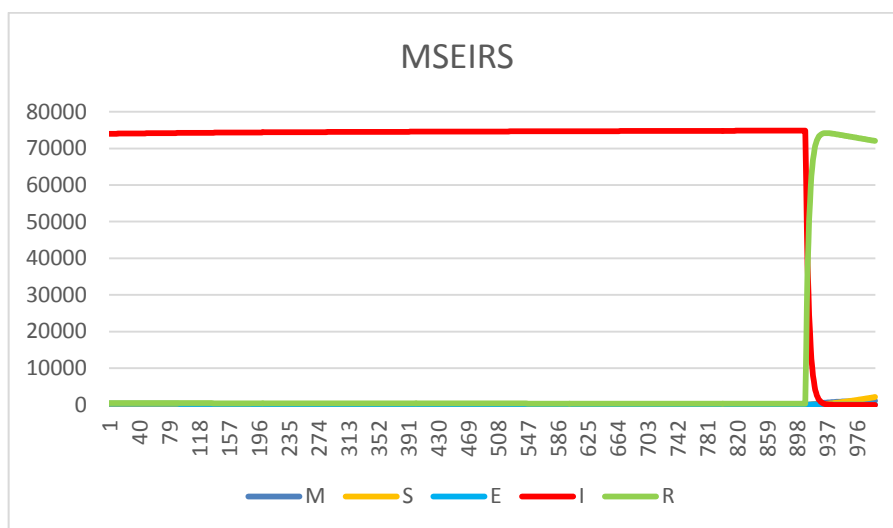


Рисунок 3.7. Графики функций, характеризующие состояние сети

Получается, что эпидемию удалось погасить. И на конец периода прогноза число инфицированных узлов в системе равно нулю.

Исследуем зависимость решения задачи от среднего период действия антивирусных баз  $\delta$ . Пусть начальные данные остаются прежними. Предположим, что средний период действия антивирусных баз сократился в десять раз и стал равен 0,0001, скорость потери «иммунитета»  $\rho = 0,001$ , а вирус поражает компьютеры со скоростью  $\lambda = 0,86$ . Т. е. антивирусные базы не будут успевать обновляться, и вирус будет быстро проникать на другие компьютеры. Скорость обновления антивирусных баз  $\gamma = 0,51$ .

Из графиков на рисунке 3.8 можно заметить, что эпидемию практически удается погасить. Остается буквально 8% зараженных компьютеров за такой короткий промежуток времени - эпидемия погашена. Стоит отметить, что при этом скорость обновления крайне низкая.

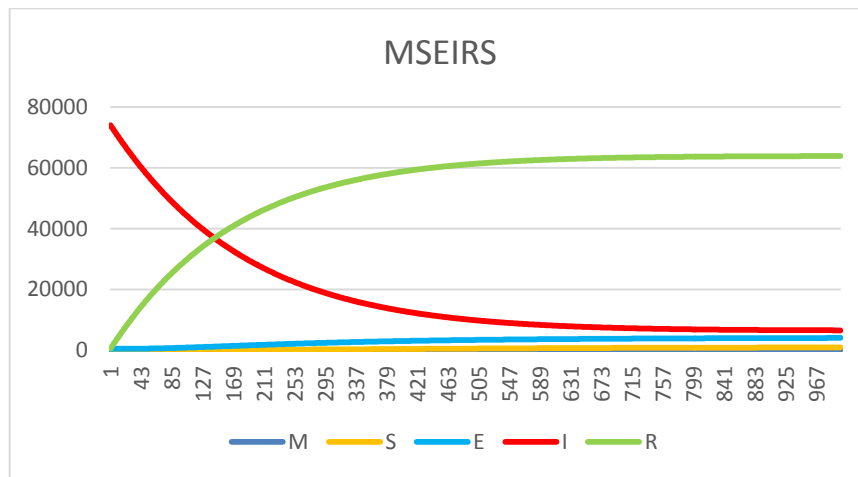


Рисунок 3.8. Графики функций, характеризующие состояние сети

Если мы будем чаще обновлять антивирусные базы ( $\gamma = 0,8$ ), то при тех же параметрах модели получим ликвидацию эпидемии за меньший период времени (рисунок 3.9).

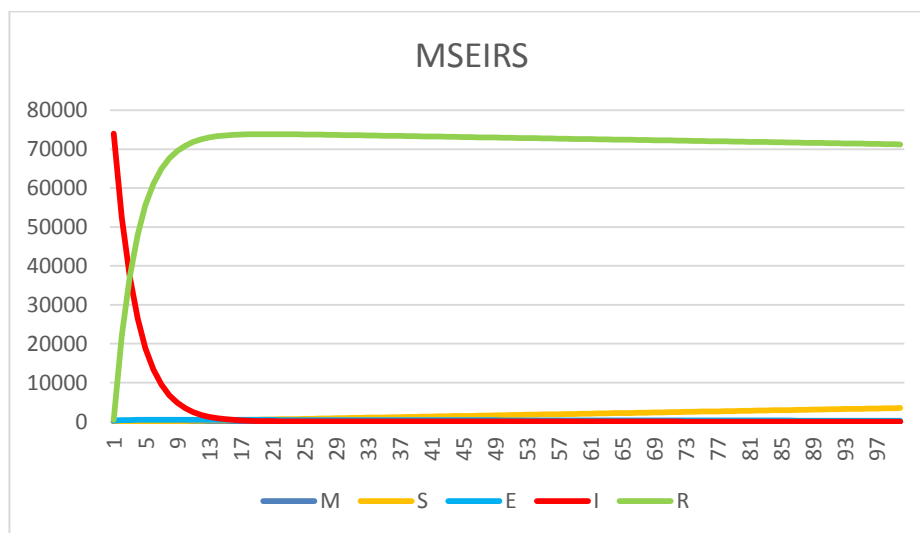


Рисунок 3.9. Графики функций, характеризующие состояние сети

Можно сделать вывод, что рассмотренная модель управления защитой компьютерной сети от атак вредоносного кода является разносторонней и всеобщей, так как она учитывает многие факторы, влияющие на состояние сети: временные параметры заражения для конкретных вирусов и лечения сети с помощью антивируса, средняя скорость иммунизации и произвольное отключение компьютеров от сети. Это позволяет грамотно оценить защищенность сети и при необходимости применить эффективные методы борьбы с вредоносным кодом.

#### **4. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА**

В указе Президента Российской Федерации "О Стратегии национальной безопасности Российской Федерации" особое внимание уделяется усиливающемуся противоборство в глобальном информационном пространстве и оказывающим негативное влияние на международную обстановку и техносферу.

Информационное противоборство представляет собой борьбу в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру противоборствующей стороны с одновременной защитой собственной информации, информационных систем и информационной инфраструктуры от подобного воздействия. Конечной целью информационного противоборства является завоевание и удержание информационного превосходства над противоборствующей стороной [5].

Учитывая высокую важность задачи выявления информационных воздействий противоборствующей стороны, ослабления их влияния и выработки эффективных ответных мер, подходы к решению таких задач должны основываться на выверенных математических моделях. Создание математических моделей информационного противоборства служит основой для решения задач выявления, прогнозирования и управления информационными воздействиями.

К сегодняшнему дню проведён значительный объём научных исследований в области информационного противоборства. На современном этапе основными задачами являются: систематизация накопленного опыта создания математических моделей информационного противоборства, уточнение их классификации и развитие в направлении



имитационного моделирования явлений и процессов, определяющих информационное противоборство.

#### 4.1. Классификация системно-динамических моделей информационного противоборства

Приведём граф, отражающий классификацию системно-динамических моделей информационного противоборства (рис. 3.1). Введённая классификация моделей информационного противоборства включает 16 моделей: SXY-модель, SXYR-модель, SLXY-модель, SLXYR-модель, OSXY-модель, SXYS-модель, OSXYS-модель, OSLXY-модель, SLXYS-модель, OSLXYS-модель, OSXYR-модель, SXYRS-модель, OSXYRS-модель, OSLXYR-модель, SLXYRS-модель, OSLXYRS-модель.

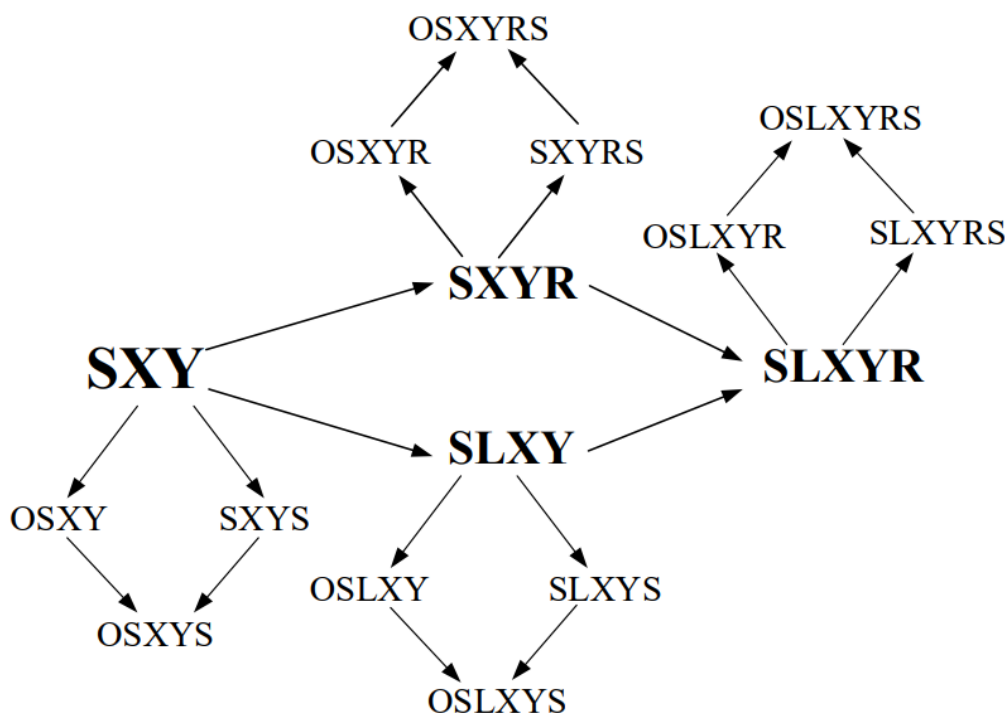


Рисунок 4.1. Граф классификаций моделей информационного противоборства

Отправной точкой классификации является базовая системно-динамическая модель информационного противоборства, которую назовём SXY-модель по заглавным буквам её основных состояний. Данная модель имеет три состояния: S – количество лиц, подверженных информационному воздействию, X – количество лиц, принявших

негативную идею информационного воздействия,  $Y$  – количество лиц, принявших идею информационного воздействия от противоборствующей стороны (позитивную идею). На основе SXY-модели разрабатываются SXYR-модель, SLXY-модель и SLXYR-модель, в которых добавляются новые состояния:  $R$  – количество лиц, отказавшихся от негативной идеи информационного воздействия навсегда,  $L$  – количество лиц, находящихся в латентной стадии информационного воздействия, то есть данные лица приняли одну из двух идей информационного воздействия, но пока ещё её не распространяют.

Далее можно трансформировать SXY-модель, SXYR-модель, SLXY-модель и SLXYR-модель путём отражения в них изменений размеров и составов социума, подвергающегося влиянию (добавляется первый символ "O" в название модели), и возможности забывания негативной идеи информационного воздействия и перехода лица, принявшего негативную идею информационного воздействия, обратно во множество лиц, подверженных информационному воздействию (добавляется последний символ "S" в название модели).

Каждая из приведенных моделей может быть двух типов. В моделях первого типа предполагается, что лицо, принявшее негативную идею информационного воздействия, не может поменять свою точку зрения и напрямую перейти во множество лиц, принявших позитивную идею информационного воздействия (от противоборствующей стороны), и наоборот. Предусматривается только возможность забывания информации и переход лица, принявшего позитивную или негативную идею информационного воздействия, обратно во множество лиц, подверженных информационному воздействию. После этого лицо может вновь принять как позитивную, так и негативную идею информационного воздействия. Модели второго типа являются усложненными модификациями моделей первого типа и подразумевают прямой переход лица, принявшего первую (негативную) идею информационного воздействия, во множество лиц,

принявших вторую (позитивную) идею информационного воздействия, и наоборот.

## 4.2. Описание системно-динамической модели информационного противоборства

Построим системно-динамическую SXY-модель информационного противоборства (рис. 3.2).

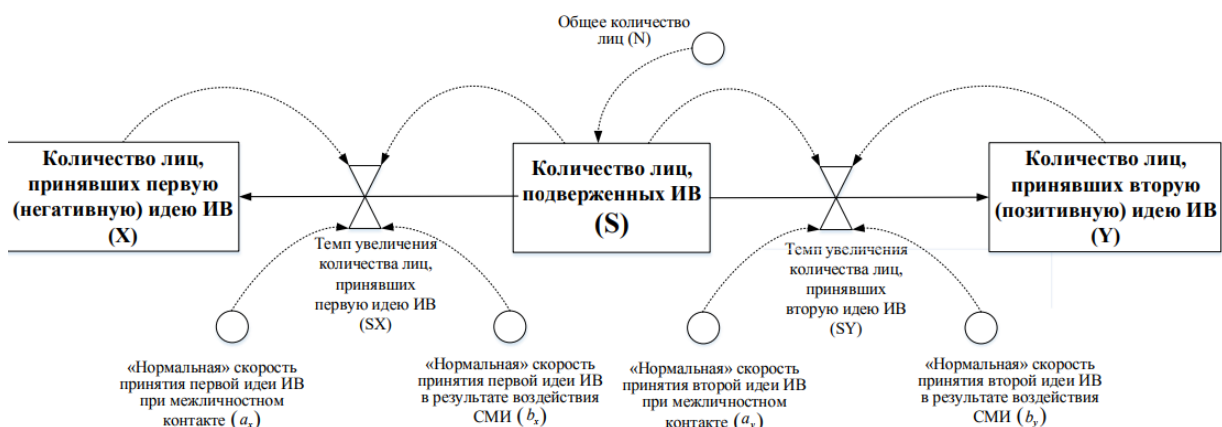


Рисунок 4.2. Системно-динамическая SXY-модель информационного противоборства.

Приведём расшифровку условных обозначений, используемых в модели (таблица 4.1).

Таблица 4.1. Условные обозначения

Условное обозначение элемента	Название элемента
$X$	Количество лиц, принявших первую (негативную) идею ИВ
$Y$	Количество лиц, принявших вторую (позитивную) идею ИВ
$S$	Количество лиц, подверженных ИВ
$N$	Общее количество лиц в социуме
$SX$	Темп изменения количества лиц, принявших первую (негативную) идею ИВ
$SY$	Темп изменения количества лиц, принявших вторую (позитивную) идею ИВ
$a_x$	"Нормальная" скорость принятия первой (негативной) идеи ИВ при межличностном контакте
$b_x$	"Нормальная" скорость принятия первой (негативной) идеи ИВ в результате воздействия СМИ
$a_y$	"Нормальная" скорость принятия второй (позитивной) идеи ИВ при межличностном контакте
$b_y$	"Нормальная" скорость принятия второй (позитивной) идеи ИВ в результате воздействия СМИ

Понятие "нормальной" скорости введено Дж. Форрестером [6] и, с учётом рассматриваемой проблематики, представляет собой отношение числа лиц в день, принявших идею информационного воздействия при

межличностном контакте или в результате воздействия СМИ, к общему количеству лиц, подверженных информационному воздействию.

Как показано на рисунке 4.2, на темп распространения идеи информационного воздействия влияют два параметра:

- "Нормальная" скорость принятия идеи информационного воздействия при межличностном контакте;
- "Нормальная" скорость принятия идеи информационного воздействия в результате воздействия СМИ.

Построенная системно-динамическая SXY-модель описывается следующей системой уравнений:

$$\left\{ \begin{array}{l} \frac{dS}{dt} = -SX(t) - SY(t); \\ \frac{dX}{dt} = SX(t); \\ \frac{dY}{dt} = SY(t); \\ SX(t) = SX1(t) + SX2(t); \\ SY(t) = SY1(t) + SY2(t); \\ SX1(t) = b_x \cdot S(t); \\ SX2(t) = \frac{a_x \cdot S(t) \cdot X(t)}{S(t) + X(t)}; \\ SY1(t) = b_y \cdot S(t); \\ SY2(t) = \frac{a_y \cdot S(t) \cdot Y(t)}{S(t) + Y(t)}. \end{array} \right.$$

Первое уравнение системы определяет скорость изменения количества лиц, подверженных информационному воздействию.

Второе и третье уравнения системы определяют скорость изменений количества лиц, принявших первую (негативную) и вторую (позитивную) идею информационного воздействия соответственно.

Четвёртое уравнение системы определяет темп увеличения количества лиц, принявших первую (негативную) идею информационного

воздействия ( $SX$ ), и складывается из темпа увеличения количества лиц, принявших первую (негативную) идею информационного воздействия в результате воздействия СМИ ( $SX1$ ), и темпа увеличения количества лиц, принявших первую (негативную) идею информационного воздействия после межличностного контакта ( $SX2$ ).

Пятое уравнение системы определяет темп увеличения количества лиц, принявших вторую (позитивную) идею информационного воздействия ( $SY$ ), и складывается из темпа увеличения количества лиц, принявших вторую (позитивную) идею информационного воздействия в результате воздействия СМИ ( $SY1$ ), и темпа увеличения количества лиц, принявших вторую (позитивную) идею информационного воздействия после межличностного контакта ( $SY2$ ).

Шестое и седьмое уравнения системы определяют темпы увеличения количества лиц, принявших первую (негативную) и вторую (позитивную) идею информационного воздействия в результате воздействия СМИ.

Восьмое и девятое уравнения системы определяют темпы увеличения количества лиц, принявших первую (негативную) и вторую (позитивную) идею информационного воздействия в результате межличностного взаимодействия. Данные темпы прямо пропорциональны произведению количества лиц, подверженных идее информационного воздействия и количества лиц, принявших идею информационного воздействия, и, учитывая принятую размерность темпов, обратно пропорциональны сумме данных лиц.

Приведём временные графики (рисунок 4.3а) и временную диаграмму с накоплением (рисунок 4.3б), отражающие динамику количества лиц, подверженных информационному воздействию ( $S$ ) и принявших первую (негативную) и вторую (позитивную) идею информационного воздействия ( $X$  и  $Y$  соответственно).

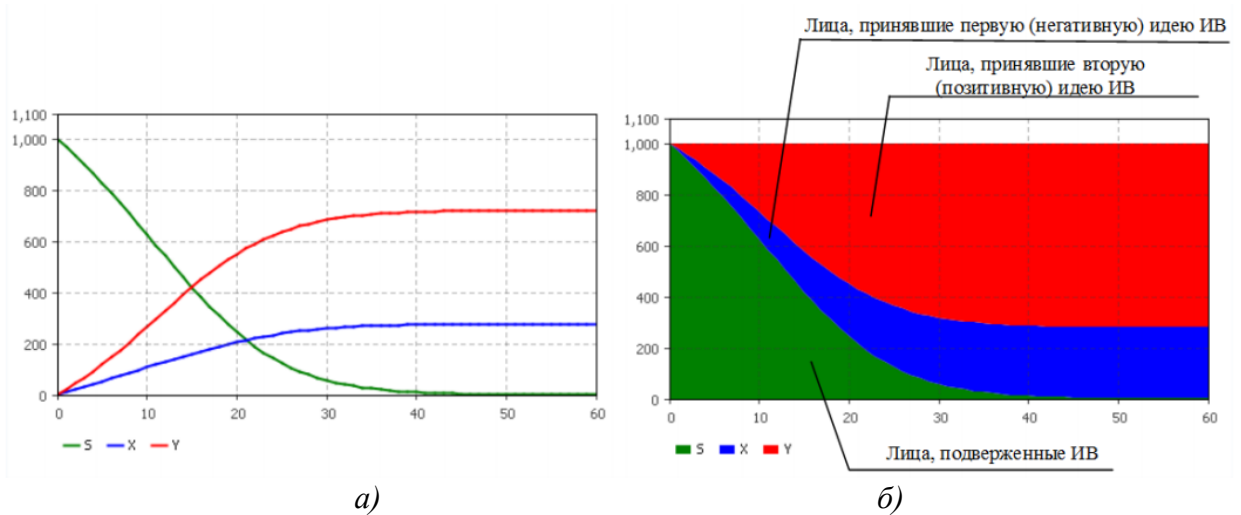


Рисунок 4.3. Динамика количества лиц, подверженных информационному воздействию и принявших первую (негативную) и вторую (позитивную) идею

На рисунке 4.4 представлены временные графики темпа принятия первой (негативной) и второй (позитивной) идеи информационного воздействия при следующих начальных условиях:  $S(0) = N = 1000$ ;  $X(0) = Y(0) = 1$ ;  $a_x = 0,05$ ;  $b_x = 0,01$ ;  $a_y = 0,1$ ;  $b_y = 0,02$ .

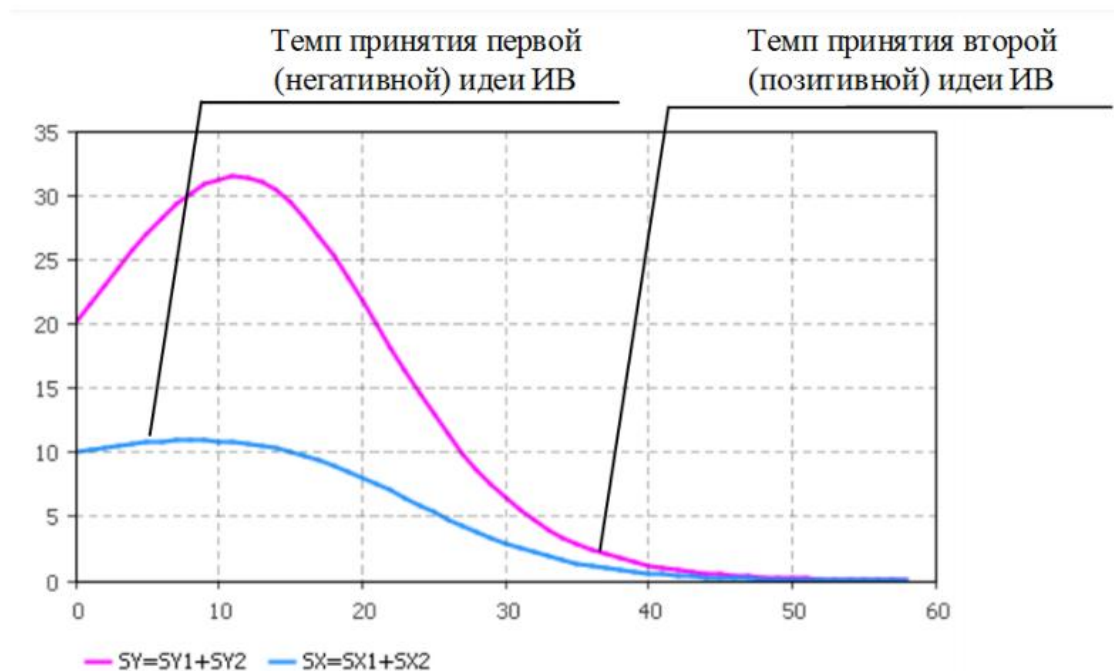


Рисунок 4.4. Временные графики темпа принятия первой (негативной) и второй (позитивной) идеи информационного воздействия

На рисунке 4.5 изображены временные диаграммы с накоплением темпа принятия первой (негативной) и второй (позитивной) идеи информационного воздействия.

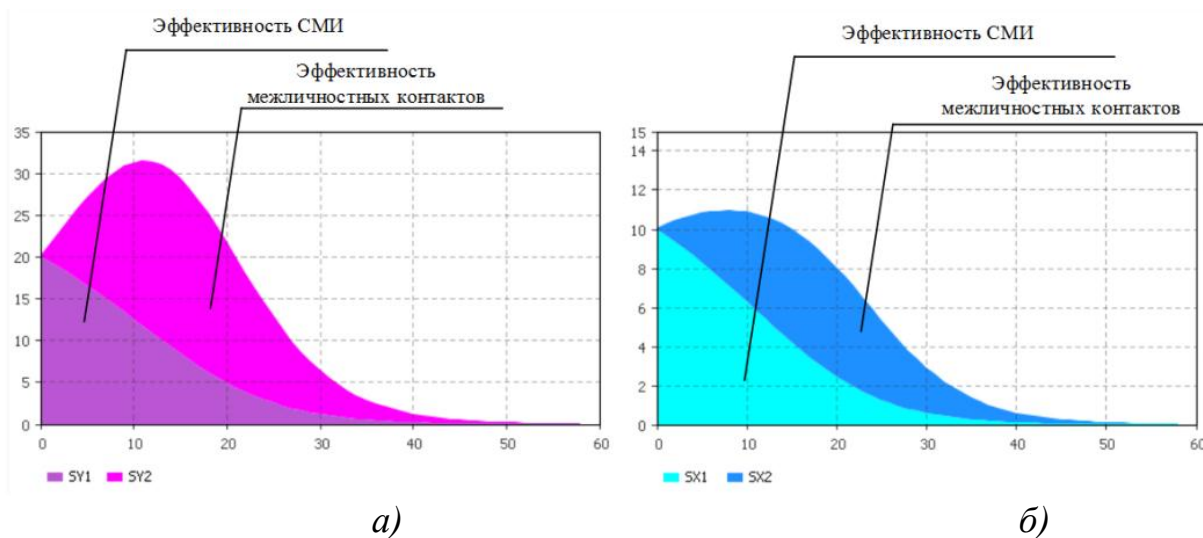


Рисунок 4.5. Временная диаграмма с накоплением темпа принятия первой (негативной) (а) и второй (позитивной) (б) идеи информационного воздействия

Таким образом, при заданных начальных условиях, первая (негативная) и вторая (позитивная) идеи информационного воздействия распространятся по всему рассматриваемому социуму за 50 дней. При этом количество лиц, принявших первую (негативную) идею информационного воздействия, составит 279 человек, а количество лиц, принявших вторую (позитивную) идею информационного воздействия, составит 723 человека.

Накопленный опыт исследований по моделированию информационного противоборства позволяет провести его систематизацию и предложить классификацию моделей информационного противоборства, а также продвинутся в построении имитационных моделей, дающих возможность воспроизвести сложный спектр факторов, включая линию деятельности МЧС России. Метод системной динамики выбран в качестве наиболее эффективного метода для моделирования информационного противоборства и позволяет делать более обоснованные оценки и прогнозы влияния информационного противоборства в зависимости от динамики различных факторов.

Предлагаемая базовая системно-динамическая модель информационного противоборства является основой для построения всех других модификаций моделей информационного противоборства, учитывающих возможность изменения социума, забывания информации, неполный охват социума СМИ, замещение информации и др.

#### **4.3. Постановка задачи**

Рассмотрим некоторую социальную группу с численностью  $N^*$ , члены которой подвержены информационному воздействию в ходе антитеррористической пропаганды, осуществляемой через СМИ по информационным каналам, которые важны для данной группы [7].

Пусть  $x(t)$  – количество лиц, воспринявших к моменту времени  $t$  распространяемую источником информацию, принявших передаваемые идеи, нормы и т.д. Полагаем, что в начальный момент  $t = t_0$   $x(t_0) = x_0$ .

Предположим, что распространение информации происходит по двум каналам: внешнему и внутреннему.

Внешний по отношению к группе канал характеризуется величиной  $u(t) \geq 0$  – количеством (интенсивностью) равноценных информационных актов передачи информации в единицу времени.

Внутренний канал определяется межличностным общением членов социальной группы, при этом для характеристики его интенсивности вводится параметр  $\alpha \geq 0$  (положительная константа). В результате такого общения члены группы, уже воспринявшие информацию, оказывая влияние на ещё не подверженных информационному воздействию членов, вносят свой собственный вклад в процесс распространения информации.

В этом случае скорость изменения числа членов группы, принявших прививаемые нормы, есть сумма скоростей внешнего и внутреннего воздействий. Данная зависимость выражается уравнением, при  $t \in [0, T]$ :



$$\dot{x}(t) = (u(t) + \alpha x(t))(N^* - x(t)), \quad x(t_0) = x_0. \quad (4.1)$$

Полагаем, что ресурс управляющего воздействия ограничен на исследуемом промежутке времени  $[0, T]$ . Ограничение заданы двойным неравенством:

$$0 \leq u(t) \leq u_{\max}. \quad (4.2)$$

В качестве критерия оптимальности рассматриваем максимизацию числа членов группы, воспринявших информацию при минимизации затрат на эти цели на фиксированном промежутке времени. В этом случае целевая функция примет вид

$$J(u) = \int_0^T (x(t) - ku(t))^2 dt \rightarrow \max, \quad (4.3)$$

где  $k$  - коэффициент стоимости внешнего воздействия.

В результате приходим к задаче оптимального управления, состоящей из критерия качества (4.3), дифференциального уравнения с начальным условием (4.1) и ограничений на функцию управления (4.2).

#### 4.4. Применение необходимых условий оптимальности

Для построения оптимального решения применим принцип максимума Понтрягина. Функция Понтрягина задачи имеет вид:

$$H(t, x, u, p) = -(x(t) - ku(t))^2 + p(t)((u(t) + \alpha x(t))(N^* - x(t))),$$

где

$$\dot{p}(t) = -\frac{\partial H}{\partial x(t)} = (\alpha N^* - 2x(t)\alpha - u(t))p(t) - 2k\alpha + 2x(t),$$

$$p(T) = -\frac{\partial H}{\partial x(T)} = 0.$$

Определим функцию переключения.

$$\psi(t) = \frac{2x(t)k - p(t)(N^* - x(t))}{2k^2} - \frac{u_{\max}}{2}.$$

Тогда, согласно принципу максимума, оптимальное управление  $\bar{u}(t)$  удовлетворяет условию почти всюду на  $[0, T]$ :

$$\bar{u}(t) = \begin{cases} u_{\max}, \psi(t) \leq 0, \\ 0, \psi(t) > 0. \end{cases} \quad (4.4)$$

Краевая задача принципа максимума имеет вид:

$$\begin{cases} \dot{x}(t) = (\bar{u}(t) + \alpha x(t))(N^* - x(t)), \\ \dot{p}(t) = -\frac{\partial H}{\partial x(t)} = (\alpha N^* - 2x(t)\alpha - \bar{u}(t))p(t) - 2k\alpha + 2x(t) \\ x(t_0) = x_0, \\ p(T) = 0, \end{cases} \quad (4.5)$$

Таким образом, решение задачи оптимального управления (4.1)-(4.3) может быть найдено как решение системы дифференциальных уравнений (4.5) с условием (4.4).

В ряде случаев система вида (4.5) может быть решена аналитически. Однако, в рассматриваемой задаче аналитическое решение достаточно трудоёмко, к тому же даже самая незначительная модификация модели (например, ввод дополнительных ограничений на фазовую переменную  $x(t)$ ) делает решение только аналитическим методом затруднительным. В то же время численные методы решения (метод проекции градиента, сопряженных направлений, Ньютона и др.) демонстрируют высокую эффективность при решении рассматриваемого класса задач.

Аппроксимируем рассматриваемую задачу (4.1) - (4.3) задачей нелинейного программирования и построим алгоритм её численного решения методом проекции градиента.

#### 4.5. Дискретная аппроксимация исходной задачи

Разобьём отрезок  $[0, T]$ ,  $q-1$ -й точкой на  $q$  частичных интервалов длины  $\Delta t = T/q$ , положим  $t^i = i\Delta t$ ,  $x(t^i) = x^i$ ,  $u(t^i) = u^i$ ,  $i = \overline{0, q-1}$ .

Для аппроксимации производных используем формулу Эйлера 1-го порядка точности. Вычисляем целевой функционал с использованием

формулы левых прямоугольников. Задача, аппроксимирующая исходную задачу оптимального управления с точностью  $O(\Delta t)$ , имеет вид

$$I(u) = \sum_{i=0}^{q-1} (x^i - ku^i)^2 \Delta t.$$

$$x^{i+1} = x^i + (u^i + \alpha x^i)(N^* - x^i)\Delta t, \quad x^0 = x_0,$$

$$0 \leq u^i \leq u_{\max}, i = \overline{0, q-1}.$$

Выпишем функцию Лагранжа построенной задачи

$$L(x, c, u, p) = - \sum_{i=0}^{q-1} (x^i - ku^i)^2 \Delta t + \sum_{i=0}^{q-1} p^{i+1} (x^{i+1} - x^i - (u^i + \alpha x^i)(N^* - x^i)\Delta t).$$

Из условий стационарности:  $\frac{\partial L}{\partial x^i}(x, c, u, p) = 0, i = \overline{0, q}$ , получаем рекуррентные соотношения

$$p^i = p^{i+1} - ((\alpha N^* - 2x^i\alpha - u^i)p^i + 2k\alpha + 2x^i)\Delta t, \quad i = \overline{0, q-1},$$

с условиями трансверсальности на правом конце траектории

$$p_1^q = 0.$$

Вычисляем производные по направлению.

$$\frac{\partial L}{\partial u^i} = \frac{2x^i k \Delta t - p^i (N^* - x^i) \Delta t}{2k^2} - \frac{u_{\max}}{2} \Delta t, \quad i = \overline{0, q-1}.$$

С учетом полученных формул может быть разработан алгоритм численного решения.

#### 4.6. Вычислительный эксперимент

Исследуем, как на решение задачи влияет величина стоимости внешнего воздействия  $k$ . Для всех экспериментов определим следующие параметры метода и модели:  $N^* = 100$ ,  $u_{\max} = 0,1$ ,  $\alpha = 0,001$ ,  $b = 0,8$ ,  $T=10$ ,  $q=1000$ ,  $\varepsilon = 10^{-5}$ .

1) Пусть  $k=1$ . Тогда получаем следующие результаты работы программы, представленные на рисунках 4.6 – 4.7.

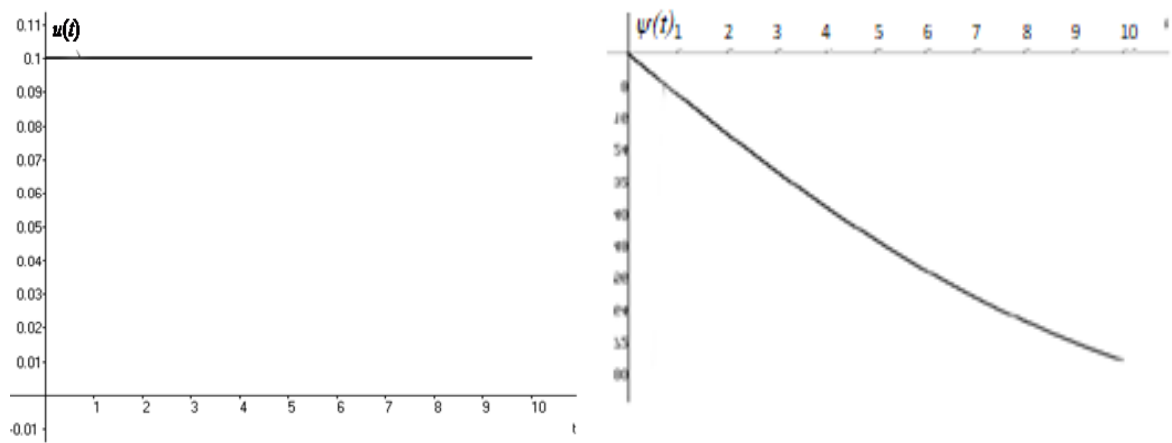


Рисунок 4.6. Графики функции управления  $\bar{u}(t)$  и функции переключения  $\bar{\psi}(t)$  при  $k=1$

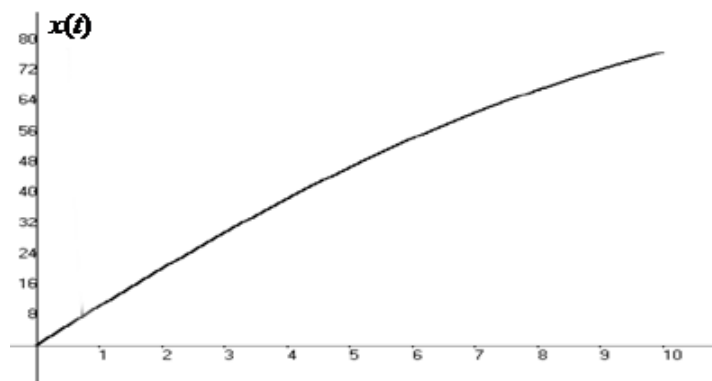


Рисунок 4.7. График функции  $\bar{x}(t)$  при  $k=1$

2) Если  $k=100$ . Получено решение, представленное на рисунках 4.8 – 4.9.

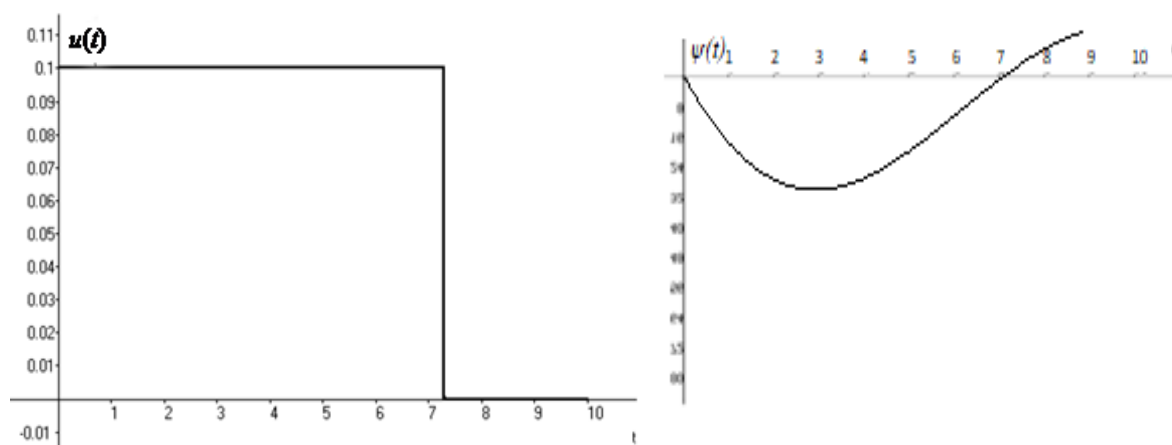


Рисунок 4.8. Графики функций управления  $\bar{u}(t)$  и переключения  $\bar{\psi}(t)$  при  $k=100$

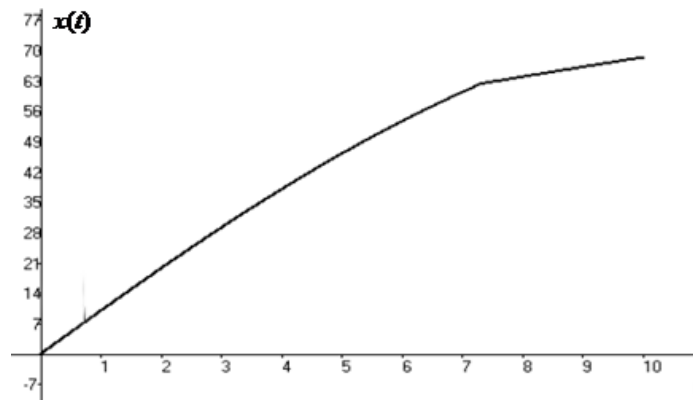


Рисунок 4.9. График функции  $\bar{x}(t)$  при  $k=100$

2) Если  $k=500$ . На рисунках 4.10 – 4.11 приведено решение задачи

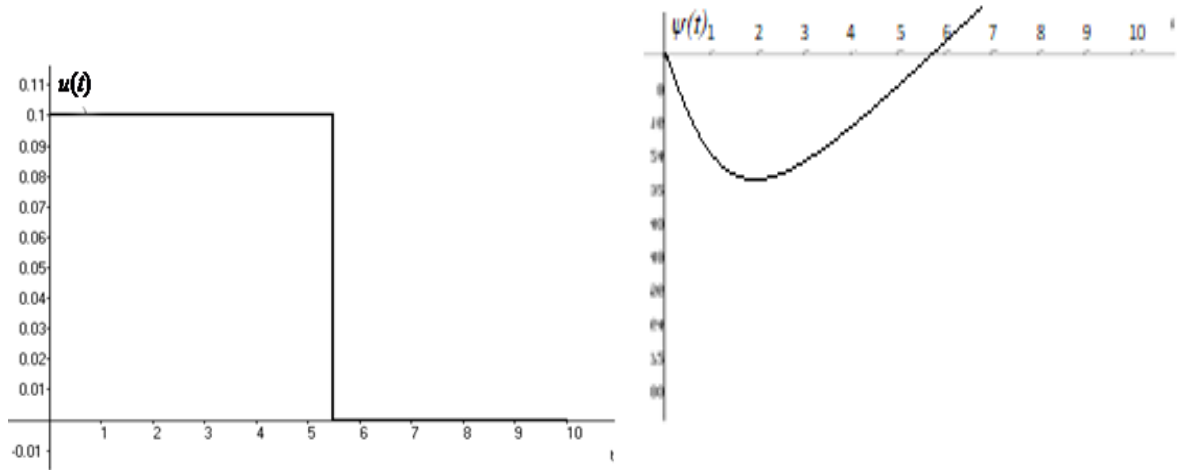


Рисунок 4.10. Графики функций управления  $\bar{u}(t)$  и переключения  $\bar{\psi}(t)$  при  $k=500$

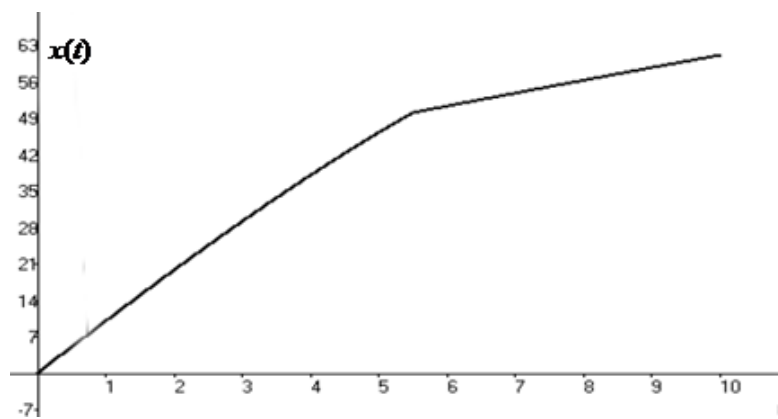


Рисунок 4.11. График функции  $\bar{x}(t)$  при  $k=500$

Из анализа графиков можно сделать вывод, что при увеличении платы за размещение информации в СМИ в некоторый момент времени управление, отвечающее за распространение по внешнему каналу, отключается и распространение продолжается только за счет личных коммуникаций внутри группы. Отключение внешнего канала происходит тем раньше, чем выше стоимость. Установленные факты вполне согласуются со здравым смыслом, что подчеркивает адекватность модели рассматриваемой ситуации.

Таким образом, при незначительных затратах на размещение информации в СМИ оптимальной является стратегии с максимальной интенсивностью внешнего воздействия. При увеличении стоимость размещения внешнее воздействие изначально максимально, а затем отключается. При этом сохраняется активность внутреннего канала передачи информации между членами социальной группы. Полученные численно результаты решения задачи демонстрируют высокую эффективность применяемых вычислительных методов, которые сохраняют свою актуальность при различных модификациях модели (например, при вводе дополнительных параметров, выражающих забывание переданной информации, неоднородность социальной группы и т.п.) В связи с этим особенный практический интерес представляет уточнение модели, а также анализ производительности численных методов при решении рассматриваемой задачи.

## **5. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЫБОРА ОПТИМАЛЬНОГО НАБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ**

Глобальное использование средств вычислительной техники приводит к использованию новых возможностей несанкционированного доступа к информации и к ее высокой уязвимости. В связи с этим, защита информации в компьютерных системах и сетях является одним из ведущих направлений развития информационных технологий. Наибольшей эффективности защиты информационных систем от различных угроз можно достичь лишь в том случае, когда степень защиты информации будет соответствовать ее ценности.

Задача определения мер и средств защиты информации на предприятии зачастую формулируется как оптимизационная задача выбора при заданных ограничениях, например минимизация стоимости при требуемой эффективности мер защиты или максимизация эффективности мер защиты при ограничении на стоимость средств.

Между тем, нормативными документами ФСТЭК строго определен порядок построения эффективной защиты — выявление всех возможных угроз безопасности информации, оценка их актуальности, вероятности реализации, определения класса защищенности АС, и установление по этим данным определенного набора мер соответствия введенному классу защищенности (уровню защиты), то есть покрытия множества требований РД множеством мер и способов защиты.

Процесс поиска, изучения, анализа и выбора средств достаточно сложен и продолжителен, зависим от уровня знаний специалиста, при этом надо учитывать множество влияющих факторов. Поэтому возможно появление ошибок в силу различных причин, которые могут привести к выбору не лучшего варианта, что может затем сказаться на бюджете и безопасности. Поэтому задача выбора оптимального состава комплекта СрЗИ является актуальной.

Решать эту задачу можно применив систему поддержки принятия решения, основанную на математической модели многокритериальной оптимизации. Задача выбора оптимальной структуры системы из составляющих ее объектов может быть следующим образом [8].

### 5.1. Постановка задачи

Пусть определено множество требований  $R = \{r_1, r_2, \dots, r_m\}$  и множество объектов (элементов оборудования)  $S = \{S_1, S_2, \dots, S_n\}$ , таких, что каждый  $S_j$  ассоциирован с подмножеством  $R_j \in R$ , где  $j \in N = \{1, \dots, n\}$ , при этом  $S_j$  удовлетворяет требованиям из  $R_j$ , либо выполняет функцию из  $R_j$ . Совокупность  $\{R_j\}$ ,  $j \in J$ ,  $J \in N$  называется покрытием множества  $R$ , если  $\cup R_j = R$ ,  $j \in J$ .

Каждому элементу оборудования  $S_j$  соответствует своя стоимость, которая обозначена  $C_j > 0$ . Требуется найти набор объектов, имеющий минимальный суммарный вес.

Приведем соответствующую модель целочисленного линейного программирования (ЦЛП). Введем переменные:  $x_j = 1$ , если множество  $R_j$  входит в покрытие, иначе  $x_j = 0$ ,  $j \in N$ . Определим матрицу  $A = (a_{ij})$ :

$$a_{ij} = \begin{cases} 1, \text{ если элемент } r_i \text{ входит в подмножество} \\ \text{требований к } j \text{ объекту,} \\ 0, \text{ иначе.} \end{cases}$$

Тогда задача определения оптимального набора средств защиты  $S = \{S_1, S_2, \dots, S_n\}$ , при реализации полного набора функций (требований)  $R = \{r_1, r_2, \dots, r_m\}$  примет вид задачи целочисленного линейного программирования:

$$F_1(x) = \sum_{j=1}^n (C_j x_j) \rightarrow \min \quad (5.1)$$

при условиях:

$$\sum_{j=1}^n (a_{ij} x_j) \geq 1, \text{ где } i \in \overline{1, m}, j \in \overline{1, n}, \quad (5.2)$$

$$x_j \in \{0, 1\}, \text{ где } j \in \overline{1, n}. \quad (5.3)$$



Обозначим через  $B_j$  эффективность элементов средств защиты, тогда целевая функция (5.4) будет определять максимальную эффективность набора средств защиты для системы, которая удовлетворяет заданным требованиям.

$$F_2(x) = \sum_{j=1}^n (B_j x_j) \rightarrow \max \quad (5.4)$$

при ограничениях:

$$\sum_{j=1}^n (a_{ij} x_j) \geq 1, \text{ где } i \in \overline{1, m}, j \in \overline{1, n},$$

$$x_j \in \{0, 1\}, \quad \text{где } j \in \overline{1, n}.$$

Поскольку для защиты корпоративной сети в каждой организации критерии могут иметь различную значимость, решать задачу выбора оптимального состава комплекта СрЗИ целесообразно с использованием коэффициентов, характеризующих важность каждого критерия. Поэтому воспользуемся методом аддитивной свертки. В этом случае задача будет приведена к следующему виду

Пусть  $\alpha = \{\alpha_1, \alpha_2\}$  - вектор весовых коэффициентов, характеризующий важность критериев  $F_1$  и  $F_2$  соответственно.

При этом  $\alpha_1, \alpha_2 \geq 0, \alpha_1 + \alpha_2 = 1$

Преобразуем критерий  $F_2 = -\sum_{j=1}^n (B_j x_j)$ .

Тогда можно построить новую целевую функцию

$$F = \alpha_1 F_1(x) - \alpha_2 F_2(x)$$

и задача примет вид:

$$F = \alpha_1 \sum_{j=1}^n (C_j x_j) - \alpha_2 \sum_{j=1}^n (B_j x_j) \rightarrow \min$$

при условиях:

$$\sum_{j=1}^n (a_{ij} x_j) - 1 \geq 0, \text{ где } i \in \overline{1, m}, \quad j \in \overline{1, n},$$

$$x_j \in (0, 1), \text{ где } j \in \overline{1, n}.$$

Данная задача является задачей целочисленного линейного программирования. Для построения алгоритма и численного решения будем использовать циклический алгоритм Гомори.

## 5.2. Исследование и анализ влияния параметров модели

Построенная программа была использована для численных экспериментов. Ниже приведены результаты исследования влияния определенных параметров модели на решение поставленной задачи.

### 1. Исследование влияния важности критериев на решение задачи.

Первый эксперимент – исследование зависимости решения от значений коэффициентов важности критериев. Были введены следующие параметры модели, которые являются одинаковыми для всех экспериментов в данном исследовании:

- количество ограничений  $m = 3$ ,
- количество средств защиты  $n = 4$ ,
- стоимость средств защиты  $C_j = (10, 20, 30, 40)$ ,
- эффективность средств защиты  $B_j = (20, 40, 10, 30)$ ,
- матрица выполнения требований  $A$ :

1	1	1	1
1	0	1	0
0	1	0	1

В таблице 5.1 представлены результаты численных экспериментов.

Таблица 5.1 Зависимость решения от значений весовых коэффициентов

Важность 1 критерия	Важность 2 критерия	Решение задачи
0,5	0,5	$X=(1, 1, 0, 0)$
0,1	0,9	$X=(1, 1, 1, 1)$
0,9	0,1	$X=(1, 1, 0, 0)$
0,3	0,7	$X=(1, 1, 0, 1)$

Поясним полученные результаты.

а) При равнозначной важности критериев, оптимальный набор средств защиты информации будет состоять из средств минимальных по стоимости и в то же время наиболее эффективных.

б) Если критерий эффективности намного важнее критерия стоимости, то оптимальный набор будет включать в себя все средства, независимо от стоимости.

в) В обратном случае, если критерий стоимости важнее критерия эффективности, в набор будут включены только объекты с минимальной стоимостью;

г) В случае, когда значимость эффективности немного больше важности стоимости, в наборе будут все объекты, за исключением средства с наименьшей эффективностью.

*2. Исследование влияния стоимости средств защиты на решение задачи.*

Второй эксперимент – исследование зависимости решения от стоимости средств защиты (остальные параметры остаются без изменения). Для данного исследования были использованы следующие параметры модели, которые оставались неизменными для всех экспериментов в данном исследовании:

- количество ограничений  $m = 3$ ;
- количество средств защиты  $n = 4$ ;
- эффективность средств защиты  $B_j = (20, 40, 10, 30)$ ;
- матрица выполнения требований  $A$ :

1	1	1	1
1	0	1	0
0	1	0	1

- коэффициент важности критерия стоимости средств защиты  $\alpha_1=0,5$ ;
- коэффициент важности критерия эффективности средств защиты  $\alpha_2=0,5$ .

В таблице 6.2 представлены результаты эксперимента.

Таблица 5.2 Зависимость решения от стоимости средств защиты

Стоимость средств защиты	Решение задачи
(10, 10, 10, 10)	$X=(1, 1, 0, 1)$
(100, 100, 10, 15)	$X=(0, 0, 1, 1)$
(10, 20, 5, 15)	$X=(1, 1, 1, 1)$

Как можно заметить из представленной таблицы, решение задачи подчиняется следующим правилам:

- а) Если стоимость одинаково небольшая, то в наборе будут все средства за исключением минимального по эффективности;
- б) Если разница в стоимости средств большая, то оптимальным будет набор из объектов с наименьшей стоимостью.
- в) Если значения стоимости всех средств меньше значений эффективности, то в набор будут входить все средства.

3. *Исследование влияния эффективности средств защиты на решение задачи.*

Третий эксперимент – исследование зависимости решения от значений эффективности средств защиты. В этом исследовании использовались следующие параметры модели, которые во всех экспериментах были одинаковы:

- количество ограничений  $m = 3$ ;
- количество средств защиты  $n = 4$ ;
- стоимость средств защиты  $C_j = (10, 20, 30, 40)$ ;
- матрица выполнения требований  $A$ :

1	1	1	1
1	0	1	0
0	1	0	1

- коэффициент важности критерия стоимости средств защиты  $\alpha_1=0,5$ ;

- коэффициент важности критерия эффективности средств защиты  $\alpha_2=0,5$ .

Таблица 5.3 Зависимость решения от эффективности средств защиты

Эффективность средств защиты	Решение задачи
(10, 10, 10, 10)	$X=(1, 1, 0, 0)$
(100, 100, 100, 100)	$X=(1, 1, 1, 1)$
(10, 10, 100, 100)	$X=(0, 0, 1, 1)$

Анализируя результаты, представленные в таблице 6.3 можно сделать следующие выводы:

а) В случае, если значения эффективности одинаково небольшие, то в наборе будут средства с наименьшей стоимостью;

б) Если эффективность каждого средства максимальная, то оптимальным будет набор из всех средств;

в) Если разница в эффективности средств большая, то в набор войдут средства с наибольшей эффективностью.

Из представленного анализа можно сделать вывод, что результаты экспериментов соответствуют реальности.

## 6. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ФОРМИРОВАНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ СЕТИ

В данном разделе рассмотрим математическую модель формирования защиты информации в распределенной сети, которая формализована как целочисленная задача линейного программирования.

На рисунке 6.1 представлена примерная схема распределенной компьютерной сети, которая состоит из трех глобальных компонентов:

- сервер;
- автоматизированное рабочее место;
- сетевая инфраструктура.

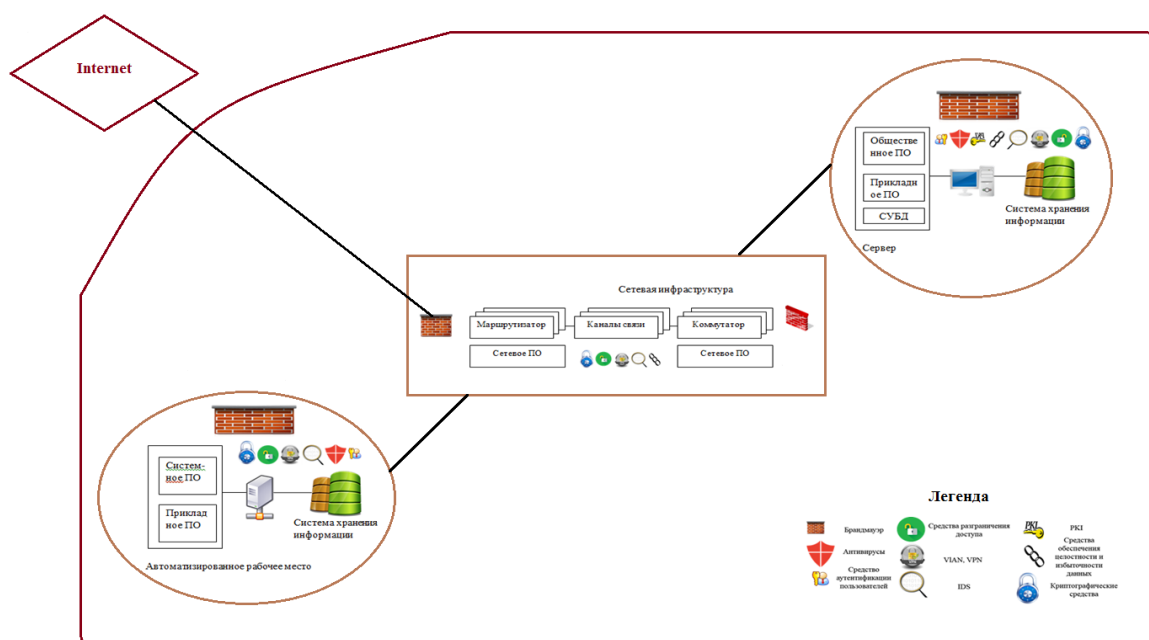


Рисунок 6.1. Схема распределенной сети

Модель приближена к реальности, так как у каждой компоненты (точек, хостов) компьютерной сети разная ресурсоемкость, на каждую выделяется различный бюджет и, как следствие, для них предусмотрены различные средства защиты информации.

Есть множество разновидностей точек, каждый из которых имеет уже отведенный на его обеспечения бюджет, в который входит не только закупка тех самых средств, но ресурсоемкость данных средств.

Задачу формирования средств информационной защиты можно представить как задачу о рюкзаке. Наиболее подходящими разновидностями задач о рюкзаке для решения поставленной задачи формирования информационной защиты являются задача о рюкзаке с мультिवыбором и задача о мультипликативном рюкзаке [9].

Суть задачи о рюкзаке с мультिवыбором заключается в том, что все предметы разделены на  $k$  классов  $N_1, \dots, N_k$ , объединяющих в себе эквивалентные предметы, схожие по своему назначению. Обязательным является условие выбора предмета из каждого класса. Для каждого  $j$ -го груза, принадлежащего  $i$ -му классу, определён вес  $w_{ij}$  и ценность  $p_{ij}$ ,  $j = 1, \dots, n$ . Необходимо найти количество  $x_{ij}$  предмета  $j$ , принадлежащего классу  $i$ .

Математически можно сформулировать следующим образом. Требуется найти максимум целевой функции

$$\sum_{i=1}^k \sum_{l \in N_i} p_{il} x_{il} \rightarrow \max,$$

так, чтобы выполнялись следующие условия:

$$\begin{aligned} \sum_{i=1}^k \sum_{l \in N_i} w_{il} x_{il} &\leq C, \\ \sum_{l \in N_i} x_{il} &= 1, \quad i = 1, \dots, k, \\ x_{il} &\in \{0, 1\}, i = 1, \dots, k; l \in N_i. \end{aligned}$$

Задача о мультипликативном рюкзаке (или задача о нескольких рюкзаках) имеет следующую постановку: пусть есть  $n$  предметов и  $m$  рюкзаков. У каждого предмета, как и раньше, есть ценность  $p_j > 0$  и вес  $w_j$ . У каждого рюкзака есть своя вместимость  $c_i$ ,  $i = 1, \dots, m$ . Необходимо найти количество  $x_{ij}$  предмета  $j$ , укладываемого в рюкзак  $i$ .

Математически можно сформулировать следующим образом:

$$\sum_{i=1}^m \sum_{l=1}^n p_i x_{il} \rightarrow \max$$

так, чтобы выполнялись следующие условия:

$$\sum_{l=1}^n w_i x_{il} \leq c_i, \quad i = 1, \dots, m,$$

$$\sum x_{il} \leq 1, \quad i = 1, \dots, m, \quad l = 1, \dots, n$$

$$x_{il} \in \{0,1\}, \quad i = 1, \dots, m, \quad l = 1, \dots, n$$

### 6.1. Построение модели

Имеется  $m$  точек, на которых могут быть размещены средства информационной защиты. Каждая точка принадлежит одному из  $z$  классов. В качестве данных точек могут выступать серверы, рабочие станции и другие элементы распределённой сети. На данных точках необходимо разместить средства информационной защиты. Всего имеется  $n$  средств информационной защиты. Каждое средство принадлежит какому-либо классу. Всего имеется  $k$  классов  $N_1, \dots, N_k$ . Класс объединяет в себе эквивалентные средства защиты, одно из которых должно обязательно присутствовать в системе. Каждое средство имеет стоимость  $w_j$  и ресурсозатратность  $q_j$ . Предлагается составить таблицу эффективности  $E$ , которая будет показывать эффективность  $e_{ijl}$  конкретного средства защиты  $l$ , принадлежащего классу  $j$ , относительно размещения на  $i$ -том классе точек. Цена не должна превышать фиксированную сумму  $C$ , а ресурсозатратность - значение  $Q$ . Необходимо найти оптимальное количество  $x_{ijl}$  каждого средства защиты  $l$  из класса  $j$ , размещаемого на точке  $i$ .

Таким образом, задачу оптимизации средств размещения информационной защиты можно сформулировать следующим образом. Требуется найти максимум целевой функции



$$\sum_{i=1}^z \sum_{j=1}^k \sum_{l \in N_i} e_{ijl} x_{ijl} \rightarrow \max,$$

так, чтобы выполнялись следующие условия:

$$\begin{aligned} \sum_{i=1}^k \sum_{j \in N_i} \sum_{l \in N_{li}} w_{ijl} x_{ijl} &\leq C, \\ \sum_{i=1}^z \sum_{j \in N_i} \sum_{l \in N_i} q_{ijl} x_{ijl} &\leq Q, \\ \sum_{j \in N_i} \sum_{l \in N_i} x_{ijl} &\geq 1, \end{aligned}$$

где введены следующие обозначения

- $x_i$  – средство информационно защиты;
- $e_i$  – эффективность средства информационной защиты;
- $q_i$  – ресурсозатратность средства информационной защиты;
- $w_i$  – стоимость средства информационной защиты;
- $Q$  – общая ресурсозатратность;
- $W$  – общая стоимость.

### Классификация средств информационной защиты

Почти каждое средство является сертифицированным средством информационной защиты. Данная информация представлена на сайте Федеральной службы по техническому и экспортному контролю [10].

Таблица 6.1. Классы средств защиты информации и их характеристика

Класс	Средства ИЗ	Цена	Ресурсоемкость	Эффективность
Антивирус	Kaspersky	2000	1	93
	Dr.Web Enterprise Security Suite версия 6.0	1300	1	80
	Norton	1600	1	91
	Windows Defender	0	1	62
Брэндмауэр	Mikrotik RouterOS	14250	2	80

	Ideco Internet Control Server	20000	2	81
	Cisco PIX-515E	37276	2	90
Средство аутентификации и пользователя	SecurID	0	1	40
	Mobile ID	7000	2	55
	Smart ID	16000	2	64
	Биометрия	23000	2	81
Средства разграничения доступа	Diamond ACS	37000	2	91
	HiPath 4000	26000	2	85
	OpenScape 4000	20000	2	76
VLAN, VPN	Cisco AnyConnect Secure Mobility Client	1000	1	87
	ZyXEL ZyWALL VPN Client	900	1	86
IDS	Stonegate IPS версии 5.2.7	215000	3	91
	Cisco IPS версии 7.2	456000	3	97
	Рубикон	115000	2	85
PKI	Public-Key Infrastructure (X.509)	0	1	90
Криптографические средства	Континент TLS VPN Сервер	6900	1	84
	СКЗИ Континент-АП 3.6	7120	2	85
	Континент-АП 3.7	7780	2	91
Средства обеспечения целостности и избыточности данных	ФИКС-UNIX 1.0	2080	1	90

## 6.2. Численная реализация и анализ результатов

Для численной реализации представленной модели был использован ниже представленный алгоритм, основанный на методе динамического программирования.

## Алгоритм

### 1. Вводим параметры модели:

- количество точек;
- количество классов точек;
- количество средств информационной защиты;
- количество классов средств;
- фиксированная сумма системы;
- ресурсозатратность системы.

Отдельно для каждого средства информационной защиты прописываем его характеристики: цену, ресурсозатратность и эффективность.

### 2. По формулам вычисляем оптимальное значение по эффективности и заносим данные в промежуточную таблицу.

$$j = 1, \quad f_1(\gamma) = e_1 * \left[ \frac{\gamma}{q_1 + w_1} \right], \quad \text{где } \gamma = \overline{1, Q + W};$$
$$j > 1, f_j(\gamma) = \max\{f_{j-1}(\gamma), f_j(\gamma - q_j + w_j) + e_j\}$$

### 3. Строим таблицу F размера $n \times b$ . В j-ой строке и $\gamma$ -ом столбце этой таблицы записывается значение $f_j(\gamma)$ .

### 4. Строим таблицу I, размера $n \times b$ и заполняем ее следующим образом. В j-ой строке и $\gamma$ -ом столбце этой таблицы записывается максимальной номер $i(j, \gamma)$ ненулевой компоненты оптимального вектора задачи, т.е.

$$\gamma(1, \gamma) = \begin{cases} 0, & \text{если } f_1(\gamma) = 0, \\ 1, & \text{если } f_1(\gamma) \neq 0. \end{cases}$$
$$\gamma(j, \gamma) = \begin{cases} i(j-1, \gamma), & \text{если } f_{j-1}(\gamma) > f_j(\gamma - q_j - w_j) + e_j, \\ j, & \text{если } f_{j-1}(\gamma) \leq f_j(\gamma - q_j - w_j) + e_j. \end{cases}$$

Используя таблицу 7.1, находим необходимое решение, которое выражается в качестве вектора.

Этот алгоритм описывает нахождение оптимального решения для средств информационной защиты одного класса. Соответственно, для

нахождения полного решения модели, необходимо пройти по этому алгоритму для каждого класса средств информационной защиты, после чего проделать все выше действия уже исходя из точки, для которой рассматривается наполнение.

#### *Анализ влияния параметров модели на решение задачи*

Данный алгоритм была использован для численных экспериментов. Ниже приведены результаты исследования влияния определенных параметров модели на решение поставленной задачи.

Т.к. для каждой точки модели программа находит решение отдельно, то для наглядности можно рассмотреть частное решение для одного хоста.

Для данных, представленных в таблице 6.1, оптимальным набором является следующее множество средств защиты информации для первой точки: Kaspersky, Microsoft, Mikrotik RouterOS, Ideco Internet Control Server, SecurID, Mobile ID, Smart ID, HiPath 4000, ZyXEL ZyWALL VPN Client, Stone gate IPS версии 5.2.7, Рубикон, Континент-АП 3.7.

Общая стоимость точки для такого набора средств равна 425530.

#### *1) Исследование влияния стоимости средств на решение задачи*

Эксперимент заключается в том, чтобы исследовать зависимость решения от стоимости средств защиты. В таблице приведены результаты работы программы, исходя из входных данных о стоимости средств защиты информации.

(1500, 21000, 13000, 25000, 900, 300000, 7100)	Kaspersky Norton Cisco PIX-515E Биометрия Diamond ACS Cisco AnyConnect Secure Mobility Client Cisco IPS версии 7.2 СКЗИ Континент-АП 3.6
(1500-15000, 21000-51000, 13000-39000, 25000-255000, 900-1000, 300000-500000, 7100-9000)	Dr.Web Microsoft Defender Ideco Internet Control Server

	Mobile ID HiPath 4000 ZyXEL ZyWALL VPN Client Stonegate IPS версии 5.2.7 СКЗИ Континент-АП 3.6
(0-1300, 10900-16000, 0-11900, 7000-15000, 400-600, 15900-23000, 2690-3500)	Kaspersky Dr.Web Microsoft Defender Norton Mikrotik RouterOS Ideco Internet Control Server Cisco PIX-515E SecurID Mobile ID Smart ID Diamond ACS HiPath 4000 OpenScape 4000 Cisco AnyConnect Secure Mobility Client Stonegate IPS версии 5.2.7 Cisco IPS версии 7.2 Рубикон Континент TLS VPN Сервер СКЗИ Континент-АП 3.6 Континент-АП 3.7

Данные о стоимости представлены для конкретного класса средств защиты информации.

Проанализировав данные из таблицы, можно сделать следующие выводы:

- если стоимость одинаковая для всех средств защиты, то в наборе будут все средства за исключением минимальных по эффективности, которые будут удовлетворять требованиям по стоимости и ресурсозатратности;
- если разница в стоимости средств большая, то оптимальным набором будет тот, который состоит из объектов с наименьшей стоимостью, но в тоже время является наиболее эффективным из них.

- если в разнице в стоимости незначительная, а требования позволяют приобрести все средства, то в набор войдут все средства защиты информации.

## 2) Исследование влияния эффективности средств на решение задачи

Эксперимент заключается в том, чтобы исследовать зависимость решения от эффективности средств защиты. В таблице приведены результаты работы программы, исходя из входных данных о эффективности средств защиты информации.

(50, 50, 50, 50, 50, 50, 50)	Dr. Web Microsoft Defender Mikrotik RouterOS SecurID Mobile ID Smart ID OpenScape 4000 ZyXEL ZyWALL VPN Client Stonegate IPS версии 5.2.7 Рубикон Континент TLS VPN Сервер
(100, 100, 100, 100, 100, 100, 100)	KASPERSKY MICROSOFT Cisco PIX-515E SecurID Mobile ID Smart ID Diamond ACS Cisco AnyConnect Secure Mobility Client Stonegate IPS версии 5.2.7 Рубикон Континент TLS VPN Сервер
(50-100, 50-100, 50-100, 50-100, 50-100, 50-100, 50-100)	MICROSOFT NORTON Ideco Internet Control Server SecurID Mobile ID Smart ID HiPath 4000

	ZyXEL ZyWALL VPN Client Stonegate IPS версии 5.2.7 Рубикон СКЗИ Континент-АП 3.6
--	---

Данные о эффективности представлены для конкретного класса средств защиты информации.

Проанализировав данные из таблицы, можно сделать следующие выводы:

- если значения эффективности одинаково небольшое для всех средств, то в набор войдут средства с наименьшей стоимостью, исходя их ограничения по стоимости и ресурсозатратности;
- если значения эффективности одинаково большое для всех средств защиты, то в набор войдут все средства, которые удовлетворяют условия модели в части стоимости и ресурсозатратности;
- если значения эффективности между средствами большая, то в набор войдут средства с наибольшей эффективностью.

## **7. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОДНОВРЕМЕННОГО РАСПРОСТРАНЕНИЯ ЛЕГАЛЬНЫХ И КОНТРАФАКТНЫХ КОПИЙ ИННОВАЦИОННОГО ПРОДУКТА**

Борьба с нелегальным копированием осуществляется различными способами: начиная с полицейских операций по пресечению деятельности пиратов и заканчивая современными системами защиты программ от копирования. Из всех известных на сегодняшний день методов борьбы с виртуальным пиратством рассмотрим пропаганду. Её целью является убедительная демонстрация преимуществ лицензионной продукции на фоне недостатков пиратских копий. Одним из эффективных методов такой пропаганды является организация рекламных кампаний в средствах массовой информации, акцентирующих внимание на проблемах кражи интеллектуальной собственности путем незаконного копирования, скачивания и пользования из сети Интернет. Математическое моделирование может существенно помочь в оценке эффективности антипиратских мероприятий, разработке и анализе стратегий борьбы против нелегального использования инновационных продуктов.

В качестве базовой модели рассматривается модель, представленная в статье [11], где основное внимание уделено исследованию численности легальных и контрафактных пользователей в любой момент времени, а также рассмотрен вопрос о стойкости защиты от взлома для обеспечения большей доли легальных пользователей.

В силу того, что защита от копирования данных продуктов может сопротивляться взлому лишь некоторый конечный интервал времени, по истечению которого на рынке будут присутствовать и контрафактные копии, рассматриваемая в данном разделе, модель сформулирована в терминах разрывной задачи оптимального управления. В качестве управляющего параметра выбрана пропаганда использования легального продукта.



Изучаемый процесс может быть описан следующим образом. В момент времени  $t = 0$  издатель выпускает на рынок новый инновационный продукт, оснащенный защитой от копирования. Представители теневой индустрии ищут способы обойти эту защиту. На практике защита способна противостоять взлому в течение конечного интервала времени  $0 \leq t < \tau$ , как правило – порядка нескольких недель. Продолжительность этого интервала  $\tau$  мы будем называть стойкостью защиты, а момент времени  $t = \tau$  моментом взлома. При  $0 \leq t < \tau$  пользователи приобретают только легальную продукцию, а после взлома становятся доступными также контрафактные копии. Таким образом, при  $t \geq \tau$  имеет место конкуренция между легальным производителем и теневой индустрией.

Применительно ко многим инновационным продуктам, в том числе компьютерным играм, практика показывает, что большая часть пользователей стремится приобрести новый продукт вскоре после его выпуска и основная масса продаж приходится обычно на несколько первых недель. Таким образом, защита от копирования является оправданной, если она способна противостоять взлому в течение этого срока.

### **7.1 Постановка задачи**

Будем считать, что рекламная кампания легального производителя по продвижению инновационного продукта на рынок начинается вместе со стартом продаж.

Введем следующие обозначения:

$N_0$  – количество потенциальных пользователей инновационного продукта, за которых конкурируют производители легальных и контрафактных копий.

$X(t)$  – количество легальных пользователей в момент времени  $t$ .

$Y(t)$  – количество контрафактных пользователей в момент времени  $t$ .

$t = 0$  – начало продаж легальных копий и начало рекламы.

В течение времени  $0 \leq t < \tau$  на рынке присутствуют только легальные копии инновационного продукта.

В момент времени  $t = \tau$  происходит взлом защиты и начало рекламной кампании по продвижению контрафактной продукции.

Во время  $\tau \leq t \leq T$  на рынке одновременно присутствуют легальные и контрафактные копии инновационного продукта.

Функция  $u(t) \geq 0$  называется функцией интенсивности распространения легальной информации с помощью рекламы; слагаемое  $\beta_1 X$  отвечает за интенсивность распространения легальной информации путем межличностной коммуникации ( $\beta_1 > 0$ ); параметр  $\alpha_2 > 0$  характеризует интенсивность распространения контрафактной информации с помощью рекламы; слагаемое  $\beta_2 X$  отвечает за интенсивность распространения контрафактной информации путем межличностной коммуникации ( $\beta_2 > 0$ ); параметр  $\alpha_1$  характеризует стоимость рекламы легальной продукции.

Динамика процесса описывается системой дифференциальных уравнений с разрывной правой частью.

$$\frac{dX(t)}{dt} = \begin{cases} (u(t) + \beta_1 X(t))(N_0 - X(t)), & 0 \leq t < \tau, \\ (u(t) + \beta_1 X(t))(N_0 - X(t) - Y(t)), & \tau \leq t \leq T, \end{cases} \quad (7.1)$$

$$\frac{dY(t)}{dt} = \begin{cases} 0, & 0 \leq t < \tau, \\ (\alpha_2 + \beta_2 Y(t))(N_0 - X(t) - Y(t)), & \tau \leq t \leq T. \end{cases}$$

В начальный момент времени количество пользователей легальных и контрафактных копий инновационного продукта можно считать нулевым

$$\begin{aligned} X(0) &= 0, \\ Y(0) &= 0. \end{aligned} \quad (7.2)$$

Функция интенсивности распространения легальной информации является управляющей функцией и удовлетворяет ограничениям, которые можно представить в виде двойного неравенства:

$$0 \leq u(t) \leq A. \quad (7.3)$$

Целью управления является максимально возможное увеличение числа легальных пользователей инновационного продукта с минимальными затратами на рекламу. Эту цель можно представить в виде функционала, состоящего из интегрального и терминального слагаемых с соответствующими весовыми коэффициентами.

$$I = -A_1 X(T) + A_2 \int_0^T u(t) c dt \rightarrow \inf. \quad (7.4)$$

Задача (7.1) – (7.4) сформулирована в терминах задачи оптимального управления с разрывной правой частью и функцией переключения

$$S(t, x, y) = t - \tau. \quad (7.5)$$

Вид функции переключения означает, что из всех возможных вариантов поведения фазовой траектории на поверхности переключения в данном случае возможно лишь протыкание траекторией поверхности переключения.

## **7.2. Принцип максимума Понтрягина для случая протыкания траекторией поверхности переключения**

Построим функцию Понтрягина:

$$\begin{aligned} H_1 &= -(A_2 u(t) c) + p_1(t) (u(t) + \beta_1 X(t)) (N_0 - X(t)); \\ H_2 &= -(A_2 u(t) c) + p_2(t) (u(t) + \beta_1 X(t)) (N_0 - X(t) - Y(t)) + \\ &+ g_2(t) (\alpha_2 + \beta_2 Y(t)) (N_0 - X(t) - Y(t)). \end{aligned}$$

Заметим, что здесь и далее рассматривается только регулярный случай  $\lambda_0 = 1$ .

Запишем систему дифференциальных уравнений для сопряженных функций (7.6):

при  $0 \leq t < \tau$

$$\dot{p}_1(t) = -\frac{\partial H_1}{\partial x} = p_1(t) (u(t) - \beta_1 N_0 + 2\beta_1 X(t)),$$

при  $\tau \leq t \leq T$

$$\dot{p}_2(t) = -\frac{\partial H_2}{\partial x} = p_2(t)(u(t) - \beta_1 N_0 + 2\beta_1 X(t) + \beta_1 Y(t)) + g_2(t)(\alpha_2 + \beta_2 Y(t)); \quad (7.6)$$

при  $\tau \leq t < T$

$$\dot{g}_2(t) = -\frac{\partial H_2}{\partial y} = p_2(t)(u(t) + \beta_1 X(t)) + g_2(t)(\alpha_2 - \beta_2 N_0 + \beta_2 X(t) + 2\beta_2 Y(t)).$$

Условия трансверсальности имеют вид:

$$\begin{aligned} \dot{p}_2(T) &= -\frac{\partial \Phi}{\partial x} = A_1; \\ \dot{g}_2(T) &= -\frac{\partial \Phi}{\partial y} = 0. \end{aligned} \quad (7.7)$$

Оптимальное управление  $\bar{u}(t)$  определяется из условия максимума функции Понтрягина на отрезках времени  $0 \leq t < \tau$  и  $\tau \leq t \leq T$ .

$$\begin{aligned} \bar{H}_1 &= \max_{0 \leq u(t) \leq A} [u(t)(-A_2 c + p_1(t)N_0 - p_1(t)X(t))] + \\ &\quad + p_1(t)\beta_1 X(t)N_0 - p_1(t)\beta_1 X^2(t); \\ \bar{H}_2 &= \max_{0 \leq u(t) \leq A} [u(t)(-A_2 c + p_2(t)N_0 - p_2(t)X(t) - p_2(t)Y(t))] + \\ &\quad + p_2(t)\beta_1 X(t)N_0 - p_2(t)\beta_1 X^2(t) - p_2(t)\beta_1 X(t)Y(t) + \\ &\quad + g_2(t)(\alpha_2 + \beta_2 Y(t))(N_0 - X(t) - Y(t)). \end{aligned}$$

На отрезке времени  $0 \leq t < \tau$  оптимальное управление определяется знаком функции переключения  $\varphi_1(t) = -c + p_1(t)N_0 - p_1(t)X(t)$ , то есть

$$\bar{u}(t) = \begin{cases} 0, & \text{если } \varphi_1(t) < 0, \\ A, & \text{если } \varphi_1(t) > 0, \\ [0, A], & \text{если } \varphi_1(t) = 0. \end{cases} \quad (7.8)$$

Если  $\tau \leq t \leq T$ , то оптимальное управление определяется знаком функции  $\varphi_2(t) = -c + p_2(t)N_0 - p_2(t)X(t) - p_2(t)Y(t)$ , то есть:

$$\bar{u}(t) = \begin{cases} 0, & \text{если } \varphi_2(t) < 0, \\ A, & \text{если } \varphi_2(t) > 0, \\ [0, A], & \text{если } \varphi_2(t) = 0. \end{cases} \quad (7.9)$$

Для функции переключения  $S(t, x, y) = t - \tau$  в точке протыкания траекторией поверхности переключения у сопряженных вектор-функций скачек отсутствует, так как

$$\frac{\partial S(\tau, \bar{x}(\tau), \bar{y}(\tau))}{\partial x} = 0 \quad \text{и} \quad \frac{\partial S(\tau, \bar{x}(\tau), \bar{y}(\tau))}{\partial y} = 0,$$

$$\begin{aligned} \text{то} \quad & p_1(\tau - 0) = p_2(\tau + 0), \\ & g_1(\tau - 0) = g_2(\tau + 0). \end{aligned} \quad (7.10)$$

Согласно теореме о необходимых условиях оптимальности, функция Понтрягина имеет скачек в точке протыкания  $H_1(\tau - 0) = \lambda + H_1(\tau + 0)$ . Величина скачка  $\lambda$  определяется выражением:

$$\begin{aligned} \lambda &= \frac{(f_2(\tau, x(\tau), \bar{u}(\tau+0)) - f_1(\tau, x(\tau), \bar{u}(\tau-0)), p_2(\tau))}{\frac{\partial S}{\partial t}(\tau) + \left(\frac{\partial S}{\partial x}(\tau), f_1(\tau, x(\tau), \bar{u}(\tau-0))\right)} = \\ &= [\bar{u}(\tau + 0) - \bar{u}(\tau - 0) - \beta_1 X(\tau)Y(\tau)]p_2(\tau) + \\ &+ [(\alpha_2 + \beta_2 Y(\tau))(N_0 - X(\tau) - Y(\tau))]g_2(\tau). \end{aligned} \quad (7.11)$$

Краевая задача принципа максимума включает в себя системы дифференциальных уравнений (1), (6) с граничными условиями (7.2), (7.7) при условии, что оптимальное управление находится согласно принципу максимума (7.8) – (7.9).

### 7.3. Дискретная задача оптимального управления

Разобьём отрезок  $[0, T]$  точками  $\tau_i, i = \overline{0, q}, 0 = \tau_0, T = \tau_q$ . Обозначим через  $\Delta\tau_i = \tau_{i+1} - \tau_i, x^i = x(\tau_i), u^i = u(\tau_i), y^i = y(\tau_i), i = \overline{0, q}$ .

Аппроксимируем производную в уравнениях (7.1) по схеме Эйлера, а интегральное слагаемое в минимизируемом функционале (7.4) – по правилу левых прямоугольников. Предположим, что точка протыкания  $\tau$  находится на отрезке  $[\tau_j, \tau_{j+1}]$ , тогда в точках  $\tau_0, \dots, \tau_j$  выполняется условие  $S(\tau_i, x^i, y^i) < 0, i = \overline{0, j}$ , и динамика системы до точки  $\tau_j$  определяется рекуррентными соотношениями

$$\begin{aligned} x^{i+1} &= x^i + \Delta\tau_i \left( (u^i + \beta_1 x^i)(N_0 - x^i) \right), i = \overline{0, j-1}, \\ y^{i+1} &= y^i, i = \overline{0, j-1}. \end{aligned} \quad (7.12)$$

После пересечения траекторией поверхности переключения  $S(\tau_i, x^i, y^i) > 0, i = \overline{j+1, q}$  поведение системы описывается рекуррентными соотношениями

$$\begin{aligned} x^{i+1} &= x^i + \Delta\tau_i(u^i + \beta_1 x^i)(N_0 - x^i - y^i), \quad i = \overline{j+1, q}, \\ y^{i+1} &= y^i + \Delta\tau_i(\alpha_2 + \beta_2 y^i)(N_0 - x^i - y^i), \quad i = \overline{j+1, q}. \end{aligned} \quad (7.13)$$

На рисунке 7.1 приведено схематичное изображение дискретной фазовой траектории  $x^i$ , акцент сделан на точке переключения.

Введем обозначения:

$$\begin{aligned} \alpha &:= (\tau_\alpha - \tau_j), & x^\alpha &:= x(\tau_\alpha), \\ y^\alpha &:= y(\tau_\alpha), & u^\alpha &:= u(\tau_\alpha + 0). \end{aligned}$$

Рассмотрим переход из точки  $x^j$  в точку  $x^{j+1}$ , используя метод касательных. Заметим, что до точки протыкания имеют место следующие равенства:

$$\begin{aligned} x^\alpha &= x^j + \alpha(u^j + \beta_1 x^j)(N_0 - x^j), \\ x^{j+1} &= x^\alpha + (\tau_{j+1} - \tau_\alpha)(u^\alpha + \beta_1 x^\alpha)(N_0 - x^\alpha - y^\alpha), \\ y^\alpha &= y^j, \\ y^{j+1} &= y^\alpha + (\tau_{j+1} - \tau_\alpha)(\alpha_2 + \beta_2 y^\alpha)(N_0 - x^\alpha - y^\alpha). \end{aligned}$$

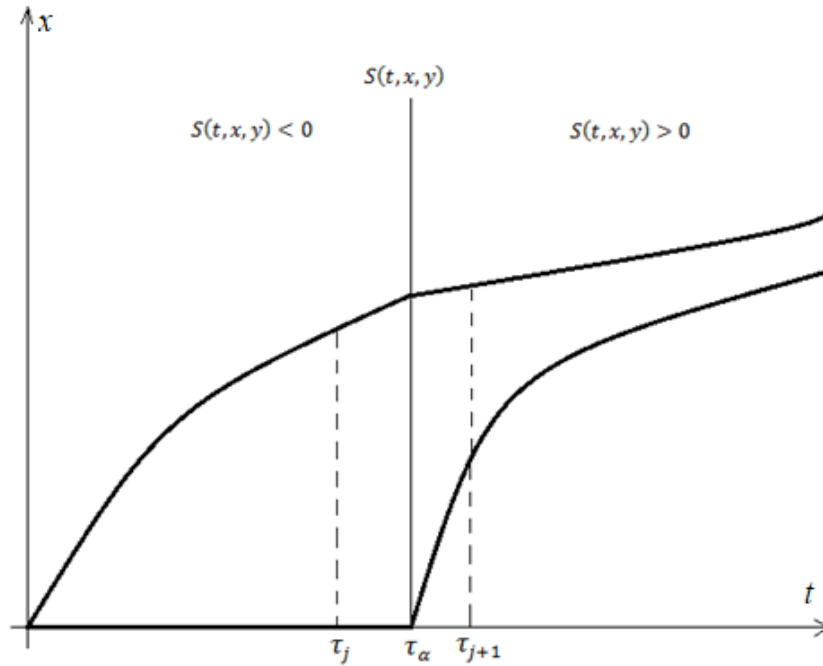


Рисунок 7.1. Дискретная фазовая траектория  $x$

Тогда формулы для вычисления  $x^{j+1}$  и  $y^{j+1}$  примут вид с учетом возможности скачкообразного изменения управления в точке  $\tau_\alpha$ .

$$\begin{aligned} x^{j+1} &= x^j + \alpha(u^j + \beta_1 x^j)(N_0 - x^j) + (\Delta\tau_j - \alpha)(u^\alpha + \beta_1 x^\alpha)(N_0 - x^\alpha - y^\alpha) \\ y^{j+1} &= y^j + (\Delta\tau_j - \alpha)(\alpha_2 + \beta_2 y^\alpha)(N_0 - x^\alpha - y^\alpha). \end{aligned}$$

Дискретная задача оптимального управления состоит в нахождении минимума функции

$$I = -A_1 x^q + A_2 \sum_{i=0}^{q-1} (u^i c) \Delta \tau_i \rightarrow \inf$$

при ограничениях

$$x^{i+1} = \begin{cases} x^i + \Delta \tau_i \left( (u^i + \beta_1 x^i)(N_0 - x^i) \right), i = \overline{0, J-1} \\ x^j + \alpha(u^j + \beta_1 x^j)(N_0 - x^j) + (\Delta \tau_j - \alpha)(u^\alpha + \beta_1 x^\alpha)(N_0 - x^\alpha - y^\alpha), \\ x^i + \Delta \tau_i (u^i + \beta_1 x^i)(N_0 - x^i - y^i), i = \overline{j+1, q} \end{cases}$$

$$y^{i+1} = \begin{cases} y^{i+1} = y^i, i = \overline{0, J-1} \\ y^j + (\Delta \tau_j - \alpha)(\alpha_2 + \beta_2 y^\alpha)(N_0 - x^\alpha - y^\alpha), \\ y^i + \Delta \tau_i (\alpha_2 + \beta_2 y^i)(N_0 - x^i - y^i), i = \overline{j+1, q} \end{cases}$$

где

$$\alpha(\tau_j, x^j, y^j) = -S(\tau_j, x^j, y^j) \left[ \frac{dS}{dt}(\tau_j) \right]^{-1} = \tau - \tau_j;$$

$$x^0 = 0,$$

$$y^0 = 0,$$

$$0 \leq u^i \leq A,$$

$$i = \overline{0, q-1}.$$

Для решения дискретной задачи воспользуемся методом множителей Лагранжа. Составим функцию Лагранжа:

$$L = -A_1 x^q + A_2 \sum_{i=0}^{q-1} (u^i c) \Delta \tau_i +$$

$$+ \sum_{i=0}^{j-1} p^{i+1} \left( x^{i+1} - x^i - \Delta \tau_i \left( (u^i + \beta_1 x^i)(N_0 - x^i) \right) \right) +$$

$$+ p^{j+1} (x^{j+1} - x^j - \alpha(u^j + \beta_1 x^j)(N_0 - x^j) -$$

$$- (\Delta \tau_j - \alpha)(u^\alpha + \beta_1 x^\alpha)(N_0 - x^\alpha - y^\alpha)) +$$

$$+ \sum_{i=j+1}^{q-1} p^{i+1} \left( x^{i+1} - x^i - \Delta \tau_i (u^i + \beta_1 x^i)(N_0 - x^i - y^i) \right) +$$

$$\begin{aligned}
& + \sum_{i=0}^{j-1} g^{i+1}(y^{i+1} - y^i) + \\
& + g^{j+1} \left( y^{j+1} - y^j - (\Delta\tau_j - \alpha)(\alpha_2 + \beta_2 y^\alpha)(N_0 - x^\alpha - y^\alpha) \right) + \\
& + \sum_{i=j+1}^{q-1} g^{i+1} \left( y^{i+1} - y^i - \Delta\tau_i(\alpha_2 + \beta_2 y^i)(N_0 - x^i - y^i) \right).
\end{aligned}$$

Запишем условие стационарности.

$$\frac{\partial L}{\partial x^i} = p^i - p^{i+1} - p^{i+1} \Delta\tau_i (\beta_1 N_0 - u^i - 2\beta_1 x^i) = 0, \quad i = \overline{1, J-1};$$

$$\begin{aligned}
\frac{\partial L}{\partial x^j} = & p^j - p^{j+1} - \alpha p^{j+1} (-u^j + \beta_1 N_0 - 2\beta_1 x^j) - \\
& - p^{j+1} (\Delta\tau_j - \alpha) \left[ \beta_1 \left( 1 + \alpha (\beta_1 (N_0 - x^j) - (u^j + \beta_1 x^j)) \right) (N_0 - x^\alpha - y^\alpha) - \right. \\
& \left. - (u^\alpha + \beta_1 x^\alpha) \left( 1 + \alpha (\beta_1 (N_0 - x^j) - (u^j + \beta_1 x^j)) \right) \right] - g^{j+1} \left( 1 + \alpha (\beta_1 (N_0 - \right. \\
& \left. x^j) - (u^j + \beta_1 x^j)) \right) (\Delta\tau_j - \alpha)(\alpha_2 + \beta_2 y^\alpha) = 0;
\end{aligned}$$

$$\begin{aligned}
\frac{\partial L}{\partial x^i} = & p^i - p^{i+1} - p^{i+1} \Delta\tau_i (-u^i + \beta_1 N_0 - 2\beta_1 x^i - \beta_1 y^i) + g^{i+1} \Delta\tau_i (\alpha_2 + \beta_2 y^i) = 0, \\
& i = \overline{J+1, q-1};
\end{aligned}$$

$$\frac{\partial L}{\partial y^i} = g^i - g^{i+1} = 0, \quad i = \overline{1, J-1};$$

$$\begin{aligned}
\frac{\partial L}{\partial y^j} = & g^j - g^{j+1} + p^{j+1} (\Delta\tau_j - \alpha)(u^\alpha + \beta_1 x^\alpha) + \\
& + g^{j+1} (\Delta\tau_j - \alpha)(-N_0 + x^\alpha + y^\alpha + \alpha_2 + \beta_2 y^\alpha) = 0;
\end{aligned}$$

$$\begin{aligned}
\frac{\partial L}{\partial y^i} = & g^i - g^{i+1} - g^{i+1} \Delta\tau_i (-\alpha_2 + \beta_2 N_0 - \beta_2 x^i - 2\beta_2 y^i) + p^{i+1} \Delta\tau_i (u^i + \beta_1 x^i) = 0, \\
& i = \overline{J+1, q-1}.
\end{aligned}$$

В конечной точке  $\tau_q$  условие стационарности запишется следующим образом:

$$\frac{\partial L}{\partial x^q} = -A_1 + p^q = 0; \quad \frac{\partial L}{\partial y^q} = g^q = 0.$$

Запишем производные по управлению:

$$\frac{\partial L}{\partial u^i} = -\Delta\tau_i p^{i+1} (N_0 - x^i) + A_2 c \Delta\tau_i, \quad i = \overline{0, J-1};$$

$$\frac{\partial L}{\partial u^i} = -\Delta\tau_i p^{i+1} (N_0 - x^i - y^i) + A_2 c \Delta\tau_i, \quad i = \overline{J+1, q-1};$$



$$\frac{\partial L}{\partial u^j} = p^{j+1}(\Delta\tau_j - \alpha)\alpha(N_0 - x^j)(\beta_1(N_0 - x^\alpha - y^\alpha) - (u^\alpha + \beta_1 x^\alpha));$$

$$\frac{\partial L}{\partial u^\alpha} = p^{j+1}(\alpha - \Delta\tau_j)(N_0 - x^\alpha - y^\alpha).$$

Используя полученные соотношения, выпишем рекуррентные формулы для вычисления импульсов  $p^i, g^i, i = \overline{1, q}$ :

$$p^q = A_1;$$

$$p^i = p^{i+1} + p^{i+1}\Delta\tau_i(\beta_1 N_0 - u^i - 2\beta_1 x^i), \quad i = \overline{1, J-1};$$

$$p^j = p^{j+1} + \alpha p^{j+1}(-u^j + \beta_1 N_0 - 2\beta_1 x^j) + \\ + p^{j+1}(\Delta\tau_j - \alpha) \left[ \beta_1 \left( 1 + \alpha \left( \beta_1(N_0 - x^j) - (u^j + \beta_1 x^j) \right) \right) (N_0 - x^\alpha - y^\alpha) - \right. \\ \left. - (u^\alpha + \beta_1 x^\alpha) \left( 1 + \alpha \left( \beta_1(N_0 - x^j) - (u^j + \beta_1 x^j) \right) \right) \right] + g^{j+1} \left( 1 + \alpha \left( \beta_1(N_0 - \right. \right. \\ \left. \left. x^j) - (u^j + \beta_1 x^j) \right) \right) (\Delta\tau_j - \alpha)(\alpha_2 + \beta_2 y^\alpha);$$

$$p^i = p^{i+1} + p^{i+1}\Delta\tau_i(-u^i + \beta_1 N_0 - 2\beta_1 x^i - \beta_1 y^i) - g^{i+1}\Delta\tau_i(\alpha_2 + \beta_2 y^i),$$

$$i = \overline{j+1, q-1};$$

$$g^q = 0;$$

$$g^i = g^{i+1}, \quad i = \overline{j+1, q-1};$$

$$g^j = g^{j+1} - p^{j+1}(\Delta\tau_j - \alpha)(u^\alpha + \beta_1 x^\alpha) - \\ - g^{j+1}(\Delta\tau_j - \alpha)(-N_0 + x^\alpha + y^\alpha + \alpha_2 + \beta_2 y^\alpha);$$

$$g^i = g^{i+1} + g^{i+1}\Delta\tau_i(-\alpha_2 + \beta_2 N_0 - \beta_2 x^i - 2\beta_2 y^i) - p^{i+1}\Delta\tau_i(u^i + \beta_1 x^i),$$

$$i = \overline{1, j-1}.$$

Полученные формулы можно использовать для построения численного решения.

#### 7.4. Численное исследование модели

Проанализируем динамику распространения легальных и контрафактных копий инновационного продукта. Для построения графиков и анализа зависимости решения от параметров используем метод проекции градиента.

### *Анализ параметров метода*

К параметрам метода относятся: шаг градиентного спуска  $\alpha$ ; количество слоёв  $q$ ; набор начальных управлений  $[u]^{(0)}$ ; точность вычисления (ограничение)  $\varepsilon$ .

Зависимость значений целевой функции ( $I_{opt}$ ), числа легальных пользователей в конечный момент времени ( $x^q$ ) и количества итераций ( $k$ ) от различных параметров метода будем рассматривать при следующих параметрах модели:  $N_0 = 30000$ ,  $\tau = 0,6$ ,  $T = 10$ ,  $\alpha_2 = 0,1$ ,  $\beta_1 = 0,00001$ ,  $\beta_2 = 0,000001$ ,  $A_1 = 10$ ,  $A_2 = 100$ ,  $c = 500$ ,  $A = 0,4$ .

#### *Влияние точности вычислений на оптимальное решение*

Результаты численных экспериментов представлены в Таблице 7.1.

Таблица 7.1. Влияние изменения точности вычисления  $\varepsilon$

$\varepsilon$	$I_{opt}$	$x^q$	$k$
0,1	-155462,546282371	19619,955193168	13
0,01	-155462,622136468	19619,5213410159	17
0,001	-155462,649510215	19619,8060111296	28
0,0001	-155462,653412353	19618,665538614	61
0,00001	-155462,654533299	19618,2683017995	74
0,000001	-155462,654533299	19618,2654533298	75
0,0000001	-155462,654533299	19618,2654533298	75
0,00000001	-155462,654533299	19618,2654533298	75
0,000000001	-155462,654533299	19618,2654533298	75

Заметим, что при увеличении точности вычислений более 0,000001 результат не меняется. Следовательно, рекомендуемая точность вычислений – 0,000001.

#### *Влияние шага градиентного спуска на оптимальное решение*

Таблица 7.2. Влияние изменения шага градиентного спуска  $\alpha$

$\alpha$	$I_{opt}$	$x^q$	$k$
10	-155462,654533299	19618,2654533298	39
5	-155462,654533299	19618,2654533298	36
1	-155462,654533299	19618,2654533298	32
0,1	-155462,654533299	19618,2654533298	75
0,01	-155462,654533299	19618,2654533298	647
0,001	-155462,654533299	19618,2654533298	6451

При изменении шага градиентного спуска результат вычислений не меняется. В целях экономии времени рекомендуемый шаг градиентного спуска равен 1.

#### *Влияние количества слоёв на оптимальное решение*

Таблица 7.3. Влияние изменения количества слоёв  $q$

$q$	$I_{opt}$	$x^q$	$k$
1000	-155552,851765533	19629,0698001266	75
2000	-155496,541203663	19619,6541203663	22
3000	-155477,719905161	19621,1053238495	23
4000	-155468,296575654	19621,8296575654	88
5000	-155462,654533299	19618,2654533298	75

Из таблицы 7.3 можно заметить, что увеличение количества слоёв дает более точный результат вычислений, при этом число итераций остается приемлемо. Поэтому, для дальнейших исследований рекомендуемое количество слоёв – 5000.

#### *Влияние набора начальных управлений на оптимальное решение*

Таблица 7.4. Влияние изменения набора начальных управлений  $u_i^0$

$u_i^0, \forall i = \overline{0, q-1}$	$I_{opt}$	$x^q$	$k$
0,05	-155462,654533299	19618,2654533298	77
0,1	-155462,654533299	19618,2654533298	75
0,15	-155462,654533299	19618,2654533298	73
0,2	-155462,654533299	19618,2654533298	71
0,25	-155462,654533299	19618,2654533298	63
0,3	-155462,654533299	19618,2654533298	72
0,35	-155462,654533299	19618,2654533298	73

Заметим, что выбор начального управления не влияет на выбор численного оптимального решения. В целях экономии времени рекомендуемый набор начальных управлений  $u_i^0 = 0,25, \forall i = \overline{0, q-1}$ .

Выполненный анализ позволяет предположить, что в качестве параметров метода можно выбрать следующий набор параметров:

$$\varepsilon = 0,000001, \alpha = 1, q = 5000, u_i^0 = 0,25, \forall i = \overline{0, q-1}.$$

### *Анализ параметров модели*

Проанализируем силу влияния параметров модели на динамику процесса.

Параметрами модели в данной задаче, являются следующие величины: количество потенциальных пользователей  $N_0$ ; время взлома  $\tau$ ; время реализации  $T$ ; интенсивность  $\alpha_2$ ; интенсивность распространения легальной информации  $\beta_1$ ; интенсивность распространения контрафактной информации  $\beta_2$ ; параметр важности первого критерия  $A_1$ ; параметр важности второго критерия  $A_2$ ; стоимость рекламной кампании для распространения легальной информации  $c$ ; максимальная интенсивность рекламных акций  $A$ .

#### *Влияние изменения времени взлома на оптимальное решение*

Таблица 7.5. Влияние изменения времени взлома  $\tau$

$\tau$	$x^q$	$y^q$	$I_{opt}$	$k$	Точка переключения управления
0,1	16918,97	13081,03	-130309,71	22	1,942
0,3	18067,73	11932,27	-141117,25	15	1,978
0,6	19618,27	10381,73	-155462,65	13	2,036
1,1	21772,16	8227,85	-174721,55	10	2,148
1,6	23440,98	6559,02	-188849,84	38	2,278
2,1	24709,12	5290,88	-198731,23	21	2,418
2,6	25581,21	4418,79	-205252,13	646	2,528
3,1	25787,10	4212,90	-210476,59	4940	2,37
3,6	25988,91	4011,09	-215449,09	2154	2,222
4,1	26186,85	3813,15	-220157,78	2428	2,088
4,6	26378,65	3621,35	-224590,44	6307	1,96
5,1	26561,39	3438,61	-228733,91	5165	1,844
5,6	26733,37	3266,63	-232573,69	3807	1,738

При повышении стойкости защиты (увеличении значения  $\tau$ ) растет число пользователей легальной продукции и, соответственно, уменьшается число людей, использующих не легальные копии инновационного продукта.

*Влияние изменения параметра, характеризующего интенсивность распространения легальной информации путем межличностной коммуникации на оптимальное решение*

Таблица 7.6. Влияние изменения интенсивности  $\beta_1$

$\beta_1$	$x^q$	$y^q$	$I_{opt}$	$k$	Переключение управления
0,001	29999,84	0,16	-299996,77	11609	0,002
0,0001	27553,04	2446,96	-265978,75	26	0,478
0,00001	19618,27	10381,73	-155462,65	13	2,036
0,000001	17269,82	12730,18	-118498,23	56	2,71
0,0000001	17003,41	12996,59	-114194,07	187	2,792
0,00000001	16975,80	13024,20	-113758,02	116	2,8
0,000000001	16971,44	13028,56	-113714,36	92	2,8

Параметр  $\beta_1$  отвечает за интенсивность распространения легального продукта путем межличностных коммуникаций, поэтому с уменьшением данной величины до 0,00000001 уменьшается количество пользователей легального продукта. При дальнейшем уменьшении параметр практически не оказывает влияния на число пользователей легальных копий продукта. Уменьшение интенсивности межличностной коммуникации среди пользователей легального продукта ведет к необходимости более длительного проведения рекламной компании легального продукта.

*Влияние изменения параметра, характеризующего интенсивность распространения контрафактной информации путем межличностной коммуникации на оптимальное решение*

Таблица 7.7. Влияние изменения интенсивности  $\beta_2$

$\beta_2$	$x^q$	$y^q$	$I_{opt}$	$k$	Переключение управления
0,001	8868,40	21131,60	-71764,02	5	0,846
0,0001	14892,88	15107,12	-114648,82	5	1,714
0,00001	19067,53	10932,47	-149435,26	16	2,062
0,000001	19618,27	10381,73	-155462,65	13	2,036
0,0000001	19674,16	10325,84	-156101,60	13	2,032
0,00000001	19680,59	10319,41	-156165,86	12	2,032

Из Таблицы 7.7 можно сделать следующие выводы. Параметр  $\beta_2$  отвечает за интенсивность распространения контрафактного продукта путем межличностных коммуникаций, поэтому с уменьшением данной величины до 0,000001 увеличивается количество пользователей легального

продукта. При дальнейшем уменьшении параметр практически не оказывает влияния на число пользователей легальных копий продукта.

*Влияние изменения параметров, характеризующих приоритетные цели оптимизации*

Данные параметры имеет смысл рассматривать только совместно, потому что каждый из них указывает важность соответствующего критерия оптимизации.

Таблица 7.8. Влияние изменения параметров  $A_1$  и  $A_2$

$A_1$	$A_2$	$x^q$	$y^q$	$I_{opt}$	$k$	Переключение управления
1	10	19618,27	10381,73	-15546,27	63	2,036
10	10	21443,92	8556,08	-205589,26	24	4,426
100	10	21643,38	8356,62	-2150326,45	95	7,006
10	100	19618,27	10381,73	-155462,65	13	2,036
1	100	6889,56	23110,44	-1695,78	1483	0,26
100	1	21665,27	8334,73	-2164547,78	233	9,896

Параметр  $A_1$  отвечает за максимальное количество пользователей легального продукта, параметр  $A_2$  за то, чтобы максимальное количество легальных пользователей достигалось при минимальных затратах, поэтому при увеличении  $A_1$  относительно  $A_2$  растет число пользователей легального продукта и увеличивается время проведения рекламной кампании легального продукта.

## **8. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ РАСПРОСТРАНЕНИЯ КОНКУРИРУЮЩЕЙ ИНФОРМАЦИИ**

Современные подходы к изучению гуманитарных проблем информационной безопасности могут быть существенно обогащены точными методами. К ним относится, прежде всего, использование соответствующих математических моделей, опирающихся на социологическое знание, в том числе на последние достижения в области социальной психологии. К сожалению, проблемы информационной безопасности сводятся, в основном, либо к её защите от несанкционированного доступа, либо к вопросам подавления распространения нежелательной информации техническими или силовыми способами. С развитием технологий распространения информации экстремистские сообщества, террористические организации и недружественные государства получили возможность пропагандировать свои интересы и реализовывать цели в наиболее важных областях жизни не только человека, но и всего общества. В связи с этим перед информационной безопасностью ставится задача поиска методов реагирования на информационные угрозы и их ослабления на основе научных подходов, таких как системы мониторинга, анализа и прогноза информационных угроз с целью предотвращения порождаемых ими негативных последствий. Необходимо, чтобы данные системы содержали подсистемы моделирования и прогнозирования этих процессов, включая иерархию соответствующих математических моделей, обеспеченных адекватным социологическим «оснащением».

В пособии рассматривается задача оптимального управления, моделирующая одновременное распространение нескольких видов информации, построенная на основе математической модели, предложенной в работе [12].

## 8.1. Построение модели

Будем предполагать, что в сообществе с численностью  $N_0$  человек распространяется информация из двух источников. Пусть в начальный момент времени ( $t_0 = 0$ ) оба источника начинают передавать информацию, в результате чего оба вида информации распространяются в сообществе. Людей, воспринявших информацию из 1-го источника будем относить к первой группе и условно называть «агентами информации 1-го источника», а людей, усваивающих информацию из 2-го источника отнесем ко второй группе и будем называть «агентами информации 2-го источника».

Так как информация первого и второго источников не совпадает между собой, то процесс распространения информации следует рассматривать как информационную конкуренцию. В случае диаметрально противоположной информации речь идет о противоборстве, а в случае частичного несоответствия информации источников можно говорить о соперничестве источников.

Конечным результатом конкуренции является определение «победителя» или «побеждённого». Под победителем понимают того, кто к конечному моменту времени смог распространить информацию среди наибольшего числа членов общества по сравнению с соперников, то есть величины большей, чем  $\frac{N_0}{2}$ . Для определенности будем считать информацию из первого источника благоприятной, а из второго – нежелательной для данного сообщества.

При построении модели учтем предположения, сформулированные ниже.

1. Каждый поток распространяется по внешнему и внутреннему каналам.

- а) Под внешним каналом понимается его отношение к общности, например, рекламная кампания. Сила распространения информации для



первого источника описывается параметром  $\alpha_1 > 0$ , а для второго – параметром  $\alpha_2 > 0$ . Считается, что  $\alpha_1$  и  $\alpha_2$  не зависят от времени.

б) Под внутренним каналом подразумевается общение внутри сообщества. Интенсивность межличностного общения для первого источника информации –  $\beta_1 > 0$ , а для второго источника –  $\beta_2 > 0$ . Считается, что  $\beta_1$  и  $\beta_2$  не зависят от времени. В результате общения внутри сообщества агенты первой информации, их численность определяется функцией  $N_1(t)$ , влияют на процесс вербовки людей, не вошедших ни в одну из групп, их численность вычисляется по формуле  $N_0 - N_1(t) - N_2(t)$ . Для второго вида информации ситуация аналогична.

2. Количество завербованных агентов в каждой группе в единицу времени складывается из следующих составляющих.

а) Скоростей внешней вербовки, они пропорциональны произведениям сил воздействия  $\alpha_1$  и  $\alpha_2$  на число незавербованных членов сообщества  $(N_0 - N_1(t) - N_2(t))$ , а значит определяются следующими формулами  $\alpha_1(N_0 - N_1(t) - N_2(t))$  для первой группы и  $\alpha_2(N_0 - N_1(t) - N_2(t))$  для второй.

б) Скоростей внутренней вербовки, которые пропорциональны произведениям интенсивностей  $\beta_1$  и  $\beta_2$  на число незавербованных членов сообщества  $(N_0 - N_1(t) - N_2(t))$  и число действующих адептов  $N_1(t)$  и  $N_2(t)$ , то есть для каждой группы скорость внутренней вербовки определяется формулой  $\beta_1 N_1(t)(N_0 - N_1(t) - N_2(t))$  или  $\beta_2 N_2(t)(N_0 - N_1(t) - N_2(t))$ .

Параметры  $\alpha_1, \alpha_2, \beta_1, \beta_2$  описывают склонность к восприятию и силу информационного воздействия. Исходя из этого, незавербованный пользователь в момент времени  $t$  поддается воздействию тем быстрее, чем больше числовых значения параметров  $\alpha_1, \alpha_2, \beta_1, \beta_2$ . Однако нет полной монополии какого-либо информационного потока (так при  $\alpha_1 > \alpha_2$ ,  $\beta_1 > \beta_2$  (воздействие первого источника информации сильнее) часть

членов примет сторону второго источника). Считается, что первоначально среднестатистический член сообщества имеет нейтральное отношение к обоим видам информации.

с) Скорость перевербовки агентов из противоположной группы пропорциональна произведению количества агентов каждой группы и зависит от разности коэффициентов перевербовки двух групп  $(\gamma_1 - \gamma_2)$ . В итоге скорости перевербовки в первой группы определяется формулой  $(\gamma_1 - \gamma_2)N_1(t)N_2(t)$ , для второй –  $(\gamma_2 - \gamma_1)N_1(t)N_2(t)$ .

Исходя из сделанных предположений, опишем динамику модели системой обыкновенных дифференциальных уравнений

$$\begin{aligned}\dot{N}_1(t) &= (\alpha_1 + \beta_1 N_1(t))(N_0 - N_1(t) - N_2(t)) + \\ &\quad + (\gamma_1 - \gamma_2)N_2(t)N_1(t), \\ \dot{N}_2(t) &= (\alpha_2 + \beta_2 N_2(t))(N_0 - N_1(t) - N_2(t)) + \\ &\quad + (\gamma_2 - \gamma_1)N_2(t)N_1(t), \\ t &\in [0, T]\end{aligned}\tag{8.1}$$

Так как сообщество в целом заинтересовано в распространении информации из первого источника будем считать параметры  $\alpha_1$  и  $\gamma_1$  изменяющимися, и выберем их в качестве управляющих функций. Для ясности изложения обозначим через  $u(t)$  силу распространения информации для первого источника, а через  $v(t)$  функцию, характеризующую скорость перевербовки агентов из второй группы в первую. В итоге получим уравнения:

$$\begin{aligned}\dot{N}_1(t) &= (u(t) + \beta_1 N_1(t))(N_0 - N_1(t) - N_2(t)) + \\ &\quad + (v(t) - \gamma)N_2(t)N_1(t), \\ \dot{N}_2(t) &= (\alpha_2 + \beta_2 N_2(t))(N_0 - N_1(t) - N_2(t)) + \\ &\quad + (\gamma - v(t))N_2(t)N_1(t), \\ t &\in [0, T].\end{aligned}\tag{8.2}$$

Число адептов в начальный момент времени будем считать известными:

$$N_1(0) = 0, N_2(0) = 0. \quad (8.3)$$

В задаче должны выполняться ограничения на управляющие функции и фазовые ограничения:

$$0 \leq u(t) \leq \alpha_2, 0 \leq v(t) \leq V, \quad (8.4)$$

$$N_1(t) \geq 0, N_2(t) \geq 0, t \in [0, T]. \quad (8.5)$$

Целью управления процессом, описываемый системой уравнений (8.2), (8.3) является максимально возможное распространение информации из первого источника в сообществе при минимальных затратах на рекламную кампанию и затратах на перевербовку адептов, при выполнении соотношений (8.4), (8.5).

$$J(u(\cdot)) = \int_0^T (M_1 C_1 u(t) + M_2 C_2 v(t)) dt - \int_0^T M_3 C_3 N_1(t) dt \rightarrow \min. \quad (8.6)$$

Задачу (8.2) – (8.6) можно классифицировать как задачу оптимального управления с фазовыми ограничениями. Для применения классического принципа максимума и численных методов поиска решения воспользуемся методом внешних штрафов и учтем фазовые ограничения (8.5) в минимизируемом функционале:

$$\begin{aligned} J(u(\cdot)) = & \int_0^T (M_1 C_1 u(t) + M_2 C_2 v(t) - M_3 C_3 N_1(t)) dt + \\ & + \int_0^T K_1 \max^2(0, -N_1(t)) dt + \int_0^T K_2 \max^2(0, -N_2(t)) dt - \\ & - M_3 C_3 N_1(T) + K_1 \max^2(0, -N_1(T)) + K_2 \max^2(0, -N_2(T)) \rightarrow \min. \end{aligned} \quad (8.7)$$

Для поиска оптимального решения воспользуемся теоремой о необходимых условиях оптимальности, которую принято называть принципом максимума Понтрягина, и сформулируем краевую задачу принципа максимума.

## 8.2. Необходимые условия оптимальности

Функция Понтрягина для сформулированной задачи (8.2) - (8.5), (8.7) имеет вид

$$H(t, N(t), u(t), v(t), p(t), \lambda_0) = -\lambda_0 M_1 C_1 u(t) - \lambda_0 M_2 C_2 v(t) + \quad (8.8)$$

$$\begin{aligned}
& +\lambda_0 M_3 C_3 N_1(t) - \lambda_0 K_1 \max^2(0, -N_1(t)) - \lambda_0 K_2 \max^2(0, -N_2(t)) \\
& + p_1(t)(u(t) + \beta_1 N_1(t))(N_0 - N_1(t) - N_2(t)) + \\
& + p_1(t)(v(t) - \gamma)N_2(t)N_1(t) + p_2(t)(\alpha_2 + \beta_2 N_2(t))(N_0 - N_1(t) - N_2(t)) \\
& + p_2(t)(\gamma - v(t))N_2(t)N_1(t).
\end{aligned}$$

Используя принцип максимума Понтрягина, выпишем необходимые условия оптимальности для задачи оптимального управления (8.2) – (8.4), (8.7).

Пусть процесс  $\bar{w} = (\bar{N}_1(t), \bar{N}_2(t), \bar{u}(t), \bar{v}(t))$  является оптимальным в поставленной задаче (8.2) – (8.5), (8.7). Тогда с необходимостью существует множитель  $\lambda_0 > 0$  и неравные одновременно нулю функции  $p_1(t), p_2(t)$  такие, что выполняются следующие условия:

1) оптимальное управление  $\bar{u}(t), t \in [0, T]$  во всех точках непрерывности доставляет максимум функции Понтрягина

$$H(t, \bar{N}(t), \bar{u}(t), \bar{v}(t), p(t), \lambda_0) = \max_{\substack{0 \leq u \leq \alpha_2 \\ 0 \leq v \leq V}} H(t, \bar{N}(t), u, v, p(t), \lambda_0), \quad (8.9)$$

то есть

$$\begin{aligned}
\bar{u}(t) &= \begin{cases} 0, & -\lambda_0 M_1 C_1 + p_1(t)(N_0 - N_1(t) - N_2(t)) < 0, \\ \alpha_2, & -\lambda_0 M_1 C_1 + p_1(t)(N_0 - N_1(t) - N_2(t)) \geq 0, \end{cases} \\
\bar{v}(t) &= \begin{cases} 0, & -\lambda_0 M_2 C_2 + (p_1(t) - p_2(t))N_2(t)N_1(t) < 0, \\ V, & -\lambda_0 M_2 C_2 + (p_1(t) - p_2(t))N_2(t)N_1(t) \geq 0. \end{cases}
\end{aligned} \quad (8.10)$$

2) сопряженные вектор-функции  $p_1(t), p_2(t)$  удовлетворяют системе дифференциальных уравнений

$$\begin{aligned}
\dot{p}_1(t) &= -\lambda_0 C_3 M_3 - 2\lambda_0 K_1 \max(0, -N_1(t)) - \\
& - p_1(t)\beta_1(N_0 - N_1(t) - N_2(t)) + p_1(t)(u(t) + \beta_1 N_1(t)) - \\
& - p_1(t)(v(t) - \gamma)N_2(t) + p_2(t)(\alpha_2 + \beta_2 N_2(t)) + p_2(t)(v(t) - \gamma)N_2(t), \\
\dot{p}_2(t) &= 2\lambda_0 K_2 \max(0, -N_2(t)) + p_1(t)(u(t) + \beta_1 N_1(t)) - \\
& - p_1(t)(v(t) - \gamma)N_1(t) - p_2(t)\beta_2(N_0 - N_1(t) - N_2(t)) + \\
& + p_2(t)(\alpha_2 + \beta_2 N_2(t)) + p_2(t)(v(t) - \gamma)N_1(t),
\end{aligned} \quad (8.11)$$

3) и условиям трансверсальности на свободном правом конце

$$\begin{aligned} p_1(T) &= \lambda_0 C_3 M_3 + 2\lambda_0 K_1 \max(0, -N_1(T)), \\ p_2(T) &= 2\lambda_0 \max(0, -N_2(t)). \end{aligned} \quad (8.12)$$

Принцип максимума Понтрягина позволяет свести решение задачи оптимального управления к решению краевой задачи, включающей в себя дифференциальные уравнения (8.2) с начальными условиями (8.3), дифференциальные уравнения (8.11) с граничными условиями (8.12) и оптимальное управление, определяемое условиями (8.10).

Рассмотрим нерегулярный случай. При  $\lambda_0 = 0$  сопряженная система дифференциальных уравнений принимает вид:

$$\begin{aligned} \dot{p}_1(t) &= -p_1(t)\beta_1(N_0 - N_1(t) - N_2(t)) + p_1(t)(u(t) + \beta_1 N_1(t)) - \\ &\quad - p_1(t)(v(t) - \gamma)N_2(t) + p_2(t)(\alpha_2 + \beta_2 N_2(t)) + p_2(t)(v(t) - \gamma)N_2(t), \\ \dot{p}_2(t) &= p_1(t)(u(t) + \beta_1 N_1(t)) - p_1(t)(v(t) - \gamma)N_1(t) - \\ &\quad - p_2(t)\beta_2(N_0 - N_1(t) - N_2(t)) \\ &\quad + p_2(t)(\alpha_2 + \beta_2 N_2(t)) + p_2(t)(v(t) - \gamma)N_1(t) \end{aligned}$$

и имеют место условия трансверсальности:  $p_1(T) = 0, p_2(T) = 0$ .

Очевидно, что функции  $p_1(t) = p_2(t) \equiv 0$  удовлетворяют последним четырем уравнениям. По теореме существования и единственности решения задачи Коши для систем дифференциальных уравнений имеем, что кроме полученных решений  $p_1(t) = p_2(t) \equiv 0$  в нерегулярном случае других решений нет. Следовательно, в этом случае все множители Лагранжа одновременно обращаются в ноль, что невозможно по условию теоремы, а значит, задача не имеет нерегулярного решения. Аналитическое решение краевой задачи принципа максимума невозможно, поэтому для поиска оптимального решения воспользуемся численными методами.

### **8.3. Поиск численного решения задачи оптимального управления**

Для построения численной схемы приближенного решения задачи оптимального управления динамикой информационного противоборства

проведем дискретную аппроксимацию непрерывной задачи (8.2) – (8.5), (8.7).

Разобьем отрезок  $[0, T]$  точками  $t_i = i \cdot \Delta t, i = \overline{0, q}$  на  $q$  частей  $(0 = t_0 < t_1 < \dots < t_q = T)$ . Проведем дискретную аппроксимацию с постоянным шагом интегрирования  $\Delta t = t_{i+1} - t_i, i = \overline{0, q-1}$ .

Запишем рекуррентные формулы для вычисления поведения траектории на всем временном промежутке

$$\begin{aligned} N_1^{k+1} &= N_1^k + \Delta t[(u^k + \beta_1 N_1^k)(N_0 - N_1^k - N_2^k) + (v^k - \gamma)N_2^k N_1^2], \\ k &= \overline{0, q-1}, \\ N_2^{k+1} &= N_2^k + \Delta t[(\alpha_2 + \beta_2 N_2^k)(N_0 - N_1^k - N_2^k) + (\gamma - v^k)N_2^k N_1^2], \\ k &= \overline{0, q-1}, \\ N_1^0 &= 0, N_2^0 = 0. \end{aligned} \quad (8.13)$$

В дискретной задаче оптимального управления требуется найти минимум функции

$$\begin{aligned} I &= \Delta t \sum_{k=0}^{q-1} (M_1 C_1 u^k + M_2 C_2 v^k - M_3 C_3 N_1^k) + \\ &+ \Delta t \sum_{k=0}^{q-1} K_1 \max^2(0, -N_1^k) + \Delta t \sum_{k=0}^{q-1} K_2 \max^2(0, -N_2^k) - \\ &- M_3 C_3 N_1^q + K_1 \max^2(0, -N_1^q) + K_2 \max^2(0, -N_2^q) \end{aligned} \quad (8.14)$$

при ограничениях на управление

$$0 \leq u^i \leq \alpha_2, 0 \leq v^i \leq V, i = \overline{0, q-1}. \quad (8.15)$$

Для решения дискретной задачи воспользуемся методом множителей Лагранжа. Составим функцию Лагранжа

$$\begin{aligned} L &= \Delta t \lambda_0 \sum_{k=0}^{q-1} (M_1 C_1 u^k + M_2 C_2 v^k - M_3 C_3 N_1^k) \\ &+ \Delta t \lambda_0 \sum_{k=0}^{q-1} K_1 \max^2(0, -N_1^k) + \Delta t \lambda_0 \sum_{k=0}^{q-1} K_2 \max^2(0, -N_2^k) - \\ &- M_3 C_3 N_1^q + \lambda_0 K_1 \max^2(0, -N_1^q) + \lambda_0 K_2 \max^2(0, -N_2^q) + \end{aligned}$$

$$\begin{aligned}
& + \sum_{k=0}^{q-1} p_1^{k+1} (N_1^{k+1} - N_1^k) \\
& \quad - \Delta t [(u^k + \beta_1 N_1^k)(N_0 - N_1^k - N_2^k) + (v^k - \gamma) N_2^k N_1^k] \\
& \quad + \sum_{k=0}^{q-1} p_2^{k+1} (N_2^{k+1} - N_1^k) \\
& \quad - \Delta t [(\alpha_2 + \beta_2 N_2^k)(N_0 - N_1^k - N_2^k) + (\gamma - v^k) N_2^k N_1^k].
\end{aligned}$$

С помощью теоремы о необходимых условиях трансверсальности конечномерных задач выпишем условия стационарности функции Лагранжа

$$\begin{aligned}
\frac{\partial L}{\partial N_1^i} &= \lambda_0 (-\Delta t C_3 M_3 - 2\Delta t K_1 \max(0, -N_1^i)) + p_1^i - p_1^{i+1} - \\
& - p_1^{i+1} \Delta t \beta_1 (N_0 - N_1^i - N_2^i) + p_1^{i+1} \Delta t (u^i + \beta_1 N_1^i) - \\
& - p_1^{i+1} \Delta t (v^i - \gamma) N_2^i - p_2^{i+1} \Delta t (\gamma - v^i) N_2^i = 0,
\end{aligned}$$

$$\begin{aligned}
\frac{\partial L}{\partial N_2^i} &= -2\lambda_0 \Delta t K_2 \max(0, -N_2^i) + p_1^{i+1} \Delta t (u^i + \beta_1 N_1^i) - \\
& - p_1^{i+1} \Delta t (v^i - \gamma) N_1^i + p_2^i - p_2^{i+1} - p_2^{i+1} \Delta t \beta_2 (N_0 - N_1^i - N_2^i) + \\
& + p_2^{i+1} \Delta t (\alpha_2 + \beta_2 N_2^i) - p_2^{i+1} \Delta t (\gamma - v^k) N_1^i = 0,
\end{aligned}$$

$$\frac{\partial L}{\partial N_1^q} = -\lambda_0 C_3 M_3 - 2\lambda_0 K_1 \max(0, -N_1^q) + p_1^q = 0,$$

$$\frac{\partial L}{\partial N_2^q} = -2\lambda_0 K_2 \max(0, -N_2^q) + p_2^q = 0,$$

$$\frac{\partial L}{\partial u^i} = \lambda_0 \Delta t M_1 C_1 - p_1^{i+1} \Delta t (N_0 - N_1^i - N_2^i),$$

$$\frac{\partial L}{\partial v^i} = \lambda_0 \Delta t M_2 C_2 - (p_1^{i+1} - p_2^{i+1}) \Delta t N_2^i N_1^i.$$

Получим рекуррентные формулы для вычисления импульсов

$$\begin{aligned}
p_1^i &= \lambda_0 (\Delta t C_3 M_3 + 2\Delta t K_1 \max(0, -N_1^i)) + p_1^{i+1} + \\
& + p_1^{i+1} \Delta t \beta_1 (N_0 - N_1^i - N_2^i) - p_1^{i+1} \Delta t (u^i + \beta_1 N_1^i) +
\end{aligned}$$

$$\begin{aligned}
& +p_1^{i+1}\Delta t(v^i - \gamma)N_2^i - p_2^{i+1}\Delta t(\alpha_2 + \beta_2 N_2^i) + p_2^{i+1}\Delta t(\gamma - v^i)N_2^i, \\
& i = \overline{0, q-1}, \\
& p_2^i = 2\lambda_0\Delta t K_2 \max(0, -N_2^i) - p_1^{i+1}\Delta t(u^i + \beta_1 N_1^i) + \\
& + p_1^{i+1}\Delta t(v^i - \gamma)N_1^i + p_2^{i+1} + p_2^{i+1}\Delta t\beta_2(N_0 - N_1^i - N_2^i) - \\
& - p_2^{i+1}\Delta t(\alpha_2 + \beta_2 N_2^i) + p_2^{i+1}\Delta t(\gamma - v^i)N_1^i, \\
& i = \overline{0, q-1}, \\
& p_1^q = \lambda_0(C_3 M_3 + 2K_1 \max(0, -N_1^q)), \\
& p_2^q = \lambda_0 K_2 \max(0, -N_2^q).
\end{aligned}$$

Выясним, существует ли нерегулярное решение. Пусть  $\lambda_0 = 0$ , тогда  $p_1^q = p_2^q \equiv 0$ , а поскольку

$$\begin{aligned}
p_1^i &= -p_1^{i+1}\Delta t(u^i + \beta_1 N_1^i) + p_1^{i+1}\Delta t(v^i - \gamma)N_2^i - p_2^{i+1}\Delta t(\alpha_2 + \beta_2 N_2^i) + \\
& + p_2^{i+1}\Delta t(\gamma - v^i)N_2^i,
\end{aligned}$$

$$\begin{aligned}
p_2^i &= -p_1^{i+1}\Delta t(u^i + \beta_1 N_1^i) + p_1^{i+1}\Delta t(v^i - \gamma)N_1^i + p_2^{i+1} + \\
& + p_2^{i+1}\Delta t\beta_2(N_0 - N_1^i - N_2^i) - p_2^{i+1}\Delta t(\alpha_2 + \beta_2 N_2^i) + p_2^{i+1}\Delta t(\gamma - v^i)N_1^i,
\end{aligned}$$

следовательно,  $p_1^i = p_2^i \equiv 0$  для  $i = \overline{1, q}$ . В итоге получаем, что все множители в функции Лагранжа равны нулю, следовательно, нерегулярных решений нет. Таким образом, решение этой задачи будем искать только в регулярном случае при  $\lambda_0 \neq 0$ .

Сформулируем алгоритм метода проекции градиента для дискретной задачи оптимального управления (8.13) – (8.15):

1. задать начальное приближение по управлению,  $[u]^{(0)} = [u^{0(0)}, \dots, u^{q-1(0)}]$ ,  $u^{i(0)} \in [0, \alpha_2], i = \overline{0, q-1}$ ;

$[v]^{(0)} = [v^{0(0)}, \dots, v^{q-1(0)}]$ ,  $v^{i(0)} \in [0, V], i = \overline{0, q-1}$ ;

который должен удовлетворять условиям допустимости;

2. построить начальную траекторию  $[N_i]^{(0)} = [N_i^{0(0)}, \dots, N_i^{q(0)}]$ ,

$i = 1, 2$  по следующим формулам:

$$N_1^{k+1(0)} = N_1^{k(0)} + \Delta t (u^{k(0)} + \beta_1 N_1^{k(0)}) (N_0 - N_1^{k(0)} - N_2^{k(0)}) +$$



$$\begin{aligned}
& +\Delta t(v^{k(0)} - \gamma)N_2^{k(0)}N_1^{k(0)}, \quad k = \overline{0, q-1} \\
& N_2^{k+1(0)} = N_2^{k(0)} + \Delta t(\alpha_2 + \beta_2 N_2^{k(0)})(N_0 - N_1^{k(0)} - N_2^{k(0)}) + \\
& +\Delta t(\gamma - v^{k(0)})N_2^{k(0)}N_1^{k(0)}, \quad k = \overline{0, q-1}, \\
& N_1^0 = 0, \quad N_2^0 = 0.
\end{aligned}$$

3. вычислить начальное приближение целевой функции, используя формулу:

$$\begin{aligned}
I^{(0)} &= I(N^{(0)}, u^{(0)}, v^{(0)}) \\
&= \Delta t \sum_{k=0}^{q-1} (M_1 C_1 u^{k(0)} + M_2 C_2 v^{k(0)} - M_3 C_3 N_1^{k(0)}) + \\
&+ \Delta t \sum_{k=0}^{q-1} K_1 \max^2(0, -N_1^{k(0)}) + \Delta t \sum_{k=0}^{q-1} K_2 \max^2(0, -N_2^{k(0)}) \\
&\quad - M_3 C_3 N_1^{q(0)} + \\
&+ K_1 \max^2(0, -N_1^{q(0)}) + K_2 \max^2(0, -N_2^{q(0)});
\end{aligned}$$

4. вычислить сопряженный вектор, компоненты которого определяются формулами:

$$\begin{aligned}
p_1^i &= \lambda_0 (\Delta t C_3 M_3 + 2\Delta t K_1 \max(0, -N_1^{i(0)})) + p_1^{i+1} + \\
&+ p_1^{i+1} \Delta t \beta_1 (N_0 - N_1^{i(0)} - N_2^{i(0)}) - p_1^{i+1} \Delta t (u^{i(0)} + \beta_1 N_1^{i(0)}) + \\
&+ p_1^{i+1} \Delta t (v^{i(0)} - \gamma) N_2^i - p_2^{i+1} \Delta t (\alpha_2 + \beta_2 N_2^{i(0)}) + p_2^{i+1} \Delta t (\gamma - v^{i(0)}) N_2^{i(0)}; \\
p_2^i &= 2\lambda_0 \Delta t K_2 \max(0, -N_2^{i(0)}) - p_1^{i+1} \Delta t (u^{i(0)} + \beta_1 N_1^{i(0)}) + \\
&+ p_1^{i+1} \Delta t (v^{i(0)} - \gamma) N_1^{i(0)} + p_2^{i+1} + p_2^{i+1} \Delta t \beta_2 (N_0 - N_1^{i(0)} - N_2^{i(0)}) - \\
&- p_2^{i+1} \Delta t (\alpha_2 + \beta_2 N_2^{i(0)}) + p_2^{i+1} \Delta t (\gamma - v^{i(0)}) N_1^{i(0)}; \quad i = \overline{q-1, 1}, \\
p_1^q &= \lambda_0 (C_3 M_3 + 2K_1 \max(0, -N_1^q)), \\
p_2^q &= \lambda_0 K_2 \max(0, -N_2^q).
\end{aligned}$$

5. вычислить градиент функции Лагранжа по управлению  $\frac{\partial L^{(0)}}{\partial u}, \frac{\partial L^{(0)}}{\partial v}$  используя формулы:

$$\frac{\partial L^{(0)}}{\partial u^i} = \lambda_0 \Delta t M_1 C_1 - p_1^{i+1} \Delta t (N_0 - N_1^{i(0)} - N_2^{i(0)}),$$

$$\frac{\partial L^{(0)}}{\partial v^i} = \lambda_0 \Delta t M_2 C_2 - (p_1^{i+1} - p_2^{i+1}) \Delta t N_2^{i(0)} N_1^{i(0)}, i = \overline{0, q-1}.$$

6. задать начальное значение шага градиентного спуска  $\alpha^0$  и организовать цикл по шагам градиентного спуска, реализующий метод автоматического выбора шага;

7. найти управляющие вектора  $[\tilde{u}]^{(1)}, [\tilde{v}]^{(1)}$  по формулам  $\tilde{u}^{(1)} = u^{i(0)} - \alpha^{(0)} \frac{\partial L(u^{i(0)})}{\partial u^i}, \tilde{v}^{(1)} = v^{i(0)} - \alpha^{(0)} \frac{\partial L(v^{i(0)})}{\partial v^i}, i = \overline{0, q-1}$  и построить их проекции на допустимое множество

$$u^{i(1)} = \begin{cases} 0, & \tilde{u}^{i(1)} < 0 \\ \tilde{u}^{i(1)}, & 0 \leq \tilde{u}^{i(1)} \leq \alpha_2, \\ \alpha_2, & \tilde{u}^{i(1)} > \alpha_2 \end{cases} \quad i = \overline{0, q-1};$$

$$v^{i(1)} = \begin{cases} 0, & \tilde{v}^{i(1)} < 0 \\ \tilde{v}^{i(1)}, & 0 \leq \tilde{v}^{i(1)} \leq V, \\ V, & \tilde{v}^{i(1)} > V \end{cases} \quad i = \overline{0, q-1};$$

8. вычислить траекторию, соответствующую данному управлению по следующим формулам  $N_1^0 = 0, N_2^0 = 0, N_1^{k+1(1)} = N_1^{k(1)} + \Delta t (u^{k(1)} + \beta_1 N_1^{k(1)}) (N_0 - N_1^{k(1)} - N_2^{k(1)}) + \Delta t (v^{k(1)} - \gamma) N_2^{k(1)} N_1^{k(1)},$   
 $N_2^{k+1(1)} = N_2^{k(1)} + \Delta t (\alpha_2 + \beta_2 N_2^{k(1)}) (N_0 - N_1^{k(1)} - N_2^{k(1)}) + \Delta t (\gamma - v^{k(1)}) N_2^{k(1)} N_1^{k(1)}, k = \overline{0, q-1};$

9. используя вектора, полученные на этапах 7) и 8), вычислить очередное приближение целевой функции по формуле:

$$I^{(1)} = I(N^{(1)}, u^{(1)}, v^{(1)}) = \Delta t \sum_{k=0}^{q-1} (M_1 C_1 u^{k(1)} + M_2 C_2 v^{k(1)} - M_3 C_3 N_1^{k(1)}) +$$

$$+ \Delta t \sum_{k=0}^{q-1} K_1 \max^2(0, -N_1^{k(1)}) + \Delta t \sum_{k=0}^{q-1} K_2 \max^2(0, -N_2^{k(1)}) - M_3 C_3 N_1^{q(1)} + \\ + K_1 \max^2(0, -N_1^{q(1)}) + K_2 \max^2(0, -N_2^{q(1)});$$

10. проверить выполнение условия: если  $I^{(1)} < I^{(0)}$ , то перейти к 12), иначе – перейти к 11);

11. уменьшить шаг градиентного спуска  $\alpha^{(0)} = \frac{\alpha^{(0)}}{2}$ , перейти к 7);

12. проверить, достигнута ли заданная точность вычислений. Если выполняются условия  $|I^{(1)} - I^{(0)}| < \varepsilon_y, \max_{i=0,q} |x^{i(0)} - x^{i(1)}| < \varepsilon_x$ , то перейти к 14), иначе — перейти к 13);

13. переобозначить  $I^{(0)} = I^{(1)}, [u]^{(0)} = [u]^{(1)}, [v]^{(0)} = [v]^{(1)}, [N_i]^{(0)} = [N_i]^{(1)}, i = 1, 2$ , идем к 4);

14. Решением задачи является набор управлений  $[u]^{(1)}, [v]^{(1)}$  траектория  $[N_i]^{(1)}, i = 1, 2$  и значение целевой функции  $I^{(1)}$ .

#### **8.4. Анализ зависимости численных решений от выбора параметров метода и модели**

Проанализируем зависимость численных решений от выбора параметров метода. Анализ будем проводить при следующих параметрах модели: время  $T = 40$ , численность сообщества  $N_0 = 500000$ , коэффициенты  $\alpha_1 = 0,0008, \alpha_2 = 0,0004, \beta_1 = 0,000002, \beta_2 = 0,000003, V = 0,0000007, \gamma = 0,0000004, C_1 = 1000000, C_2 = 500000000$ .

1) Исследуем зависимость решения от выбора начального приближения по управлению  $[u^{(0)}]$ . Будем считать, что на 0-ой итерации управление постоянно и принимает значения, представленные в таблице 8.1.

Численные эксперименты показали, что оптимальные управления имеют следующую структуру:

$$\bar{v}(t) = \begin{cases} V, & t \in [\tau_1, \tau_2], \\ 0, & t \in [0, \tau_1) \cup (\tau_2, T], \end{cases} \quad \bar{u}(t) = \begin{cases} \alpha_1, & t \in [0, \tau_3], \\ 0, & t \in (\tau_3, T], \end{cases}$$

где  $\tau_1, \tau_2, \tau_3$  – точки переключения управления.

Таблица 8.1. Зависимость решения от выбора  $[u^{(0)}]$

$[u^{(0)}]$	$I_{min}$	Количество итераций	Победитель
0,0004	-12679920,5565031	57007	1
0,00045	-12679920,5565031	57534	1
0,0005	-12679920,5565031	58099	1
0,00055	-12679920,5565031	58669	1
0,0006	-12679920,5565031	59240	1
0,00065	-12679920,5565031	59812	1
0,0007	-12679920,5565031	60385	1
0,00075	-12679920,5565031	60959	1
0,0008	-12679920,5565031	61536	1

Оптимальное решение устойчиво по выбору начального управления  $[u^{(0)}]$ . Изменяется только количество итераций, необходимых для нахождения оптимального решения. Можно предположить, что оптимальное управление  $[\bar{u}]$  является глобальным минимумом. Будем выбирать  $[u^{(0)}] = 0,0004$ , когда оптимальное решение получено за наименьшее количество итераций.

2) Исследуем зависимость решения от выбора начального приближения по управлению  $[v^{(0)}]$ . Будем считать, что на 0-ой итерации управление постоянно и принимает значения, представленные в таблице 8.2.

Таблица 8.2. Зависимость решения от выбора  $[v^{(0)}]$

$[v^{(0)}]$	$I_{min}$	Количество итераций	Победитель	$\tau_1$	$\tau_2$	$\tau_3$
0,0000001	-12697517,514594	15660	1	4,08	38,32	3,6
0,0000002	-12643226,641395	16624	1	4,08	36,08	3,6
0,0000003	-12653527,278758	23594	1	4,32	36,92	3,6
0,00000035	-12639745,150078	6710	1	4,32	36,44	3,6
0,0000004	-12694099,029498	7765	1	4,12	38,24	3,6
0,0000005	-12708031,312835	7579	1	3,96	38,68	3,6
0,0000006	-12610777,424233	52303	1	4,12	35,44	3,6

Оптимальное решение зависит от выбора начального управления  $[v^{(0)}]$ . Изменяется не только количество итераций, но и границы промежутка  $[\tau_1, \tau_2]$ . Можно предположить, что целевая функция имеет несколько локальных минимумов по управлению  $v(t)$ . Имеет смысл выбрать  $[v^{(0)}] = 0,0000035$ , исходя из соотношения точности численного решения и количество итераций для его поиска.

3) Исследуем зависимость решения от количества точек разбиения отрезка  $[0, T]$ . Результаты представлены в таблице 8.3.

Таблица 8.3. Зависимость решения от числа точек разбиения

$q$	$I_{min}$	Количество итераций	Победитель	$\tau_1$	$\tau_2$	$\tau_3$
200	-12745146,6941838	853	1	4,8	36,2	3,6
300	-12632663,8346031	1594	1	4,5	34,5	3,6
500	-12673263,9789820	6554	1	4,48	36,4	3,6
1000	-12679920,5565031	57007	1	4,28	38,04	3,6
2000	-12670203,4648984	68853	1	4,16	38,56	3,6
5000	-12662739,4343129	90178	1	4,06	38,83	3,58
10000	-12659890,5439845	156549	1	4	38,91	3,58

Уменьшение шага разбиение отрезка  $[0, T]$  приводит к более точным результатам оптимального решения. Увеличивается количество итераций, уточняются  $\tau_3$ ,  $\tau_1$ ,  $\tau_2$ . Целесообразно выбирать  $q = 1000$ , исходя из соотношения точности численного решения и количество итераций для его поиска.

4) Исследуем зависимость решения от шага градиентного спуска  $\alpha_u$ . Результаты представлены в таблице 8.4.

Таблица 8.4. Зависимость решения от  $\alpha_u$

$\alpha_u$	$I_{min}$	Количество итераций	Победитель	$\tau_3$	$\tau_1$	$\tau_2$
$1,0 \cdot e^{-2}$	-12639702,24893	9	1	3,6	4,32	36,44
$1,0 \cdot e^{-4}$	-12639702,24893	9	1	3,6	4,32	36,44
$1,0 \cdot e^{-6}$	-12639702,24893	9	1	3,6	4,32	36,44
$1,0 \cdot e^{-8}$	-12639702,24893	22	1	3,6	4,32	36,44
$1,0 \cdot e^{-10}$	-12639702,24893	843	1	3,6	4,32	36,44
$1,0 \cdot e^{-12}$	-12639745,15008	6710	1	3,6	4,32	36,44
$1,0 \cdot e^{-13}$	-12639745,12533	67004	1	3,6	4,32	36,44

Численный эксперимент показал, что выбор значения шага градиентного спуска для нахождения оптимального управления  $u(t)$  не влияет на вид оптимального решения. Как и следовало ожидать уменьшение шага градиентного спуска увеличивает количество итераций. Имеет смысл выбрать  $\alpha_u = 1,0 \cdot e^{-2}$ , исходя из наименьшего количества итераций для поиска численного решения.

5) Исследуем зависимость решения от шага градиентного спуска  $\alpha_v$ . Результаты представлены в таблице 5.

Таблица 8.5. Зависимость решения от  $\alpha_v$

$\alpha_v$	$I_{min}$	Количество итераций	Победитель	$\tau_1$	$\tau_2$	$\tau_3$
$1,0 \cdot e^{-4}$	-12639194,1185482	9	1	4,32	36,4	3,6
$1,0 \cdot e^{-5}$	-12639194,1185917	9	1	4,32	36,4	3,6
$1,0 \cdot e^{-6}$	-12639194,1186298	9	1	4,32	36,4	3,6
$1,0 \cdot e^{-8}$	-12639194,1186814	9	1	4,32	36,4	3,6
$1,0 \cdot e^{-10}$	-12639194,1186557	9	1	4,32	36,4	3,6
$1,0 \cdot e^{-12}$	-12639194,1186979	9	1	4,32	36,4	3,6
$1,0 \cdot e^{-14}$	-12639702,2489322	9	1	4,32	36,4	3,6
$1,0 \cdot e^{-16}$	-12630450,7289366	9	1	3,36	38,7	3,6

Численный эксперимент показал, что выбор значения шага градиентного спуска для нахождения оптимального управления  $v(t)$  незначительно влияет на вид оптимального решения. Количество итераций не изменилось. Целесообразно выбрать  $\alpha_v = 1,0 \cdot e^{-14}$ , так как при этом значении получен лучший результат численного решения.

6) Зависимость решения от выбора значения силы распространения  $\alpha_1$  первого источника. Результаты представлены в таблице 8.6. и в виде графиков на рисунках 8.1 и 8.2.

Таблица 8.6. Зависимость решения от выбора  $\alpha_1$

$\alpha_1$	$I_{min}$	Количество итераций	Победитель	$\tau_1$	$\tau_2$	$\tau_3$
0,0004	-10834745,3878	13	1	4,36	38,4	4,32
0,0005	-11397112,8303	13	1	4,36	36,7	4,12
0,0006	-11798263,1216	13	1	4,4	35,3	3,96
0,0007	-12264898,7713	13	1	4,4	35,96	3,76

0,00075	-12460986,8527	13	1	4,36	36,2	3,68
0,0008	-12639702,2489	9	1	4,32	36,4	3,6
0,00085	-12800956,1737	13	1	4,28	36,6	3,52
0,0009	-12950567,7251	13	1	4,2	36,84	3,44

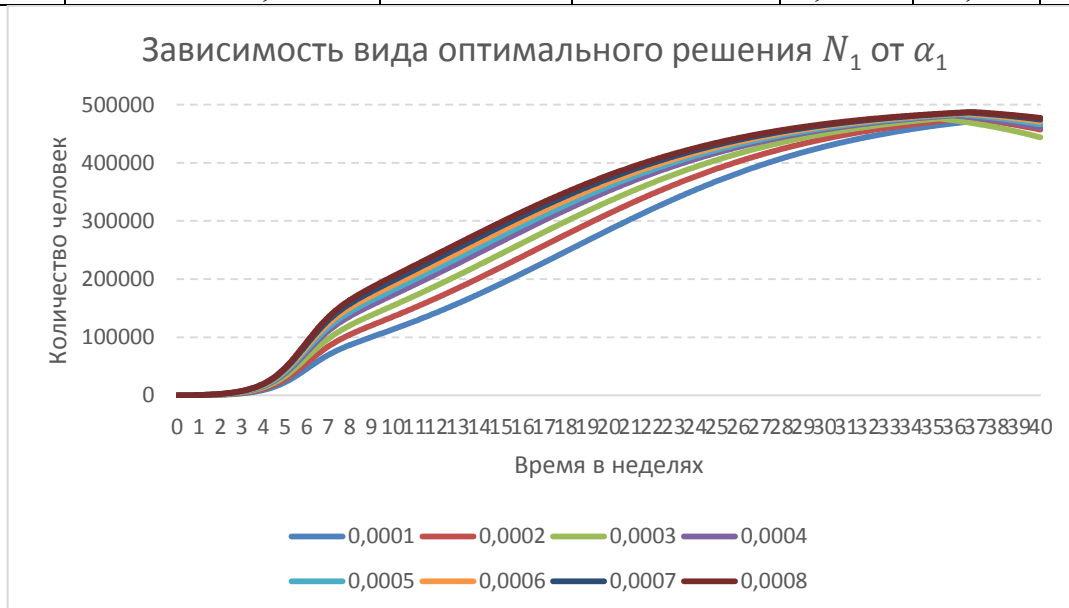


Рисунок 8.1. Зависимость вида оптимального решения  $N_1$  от  $\alpha_1$

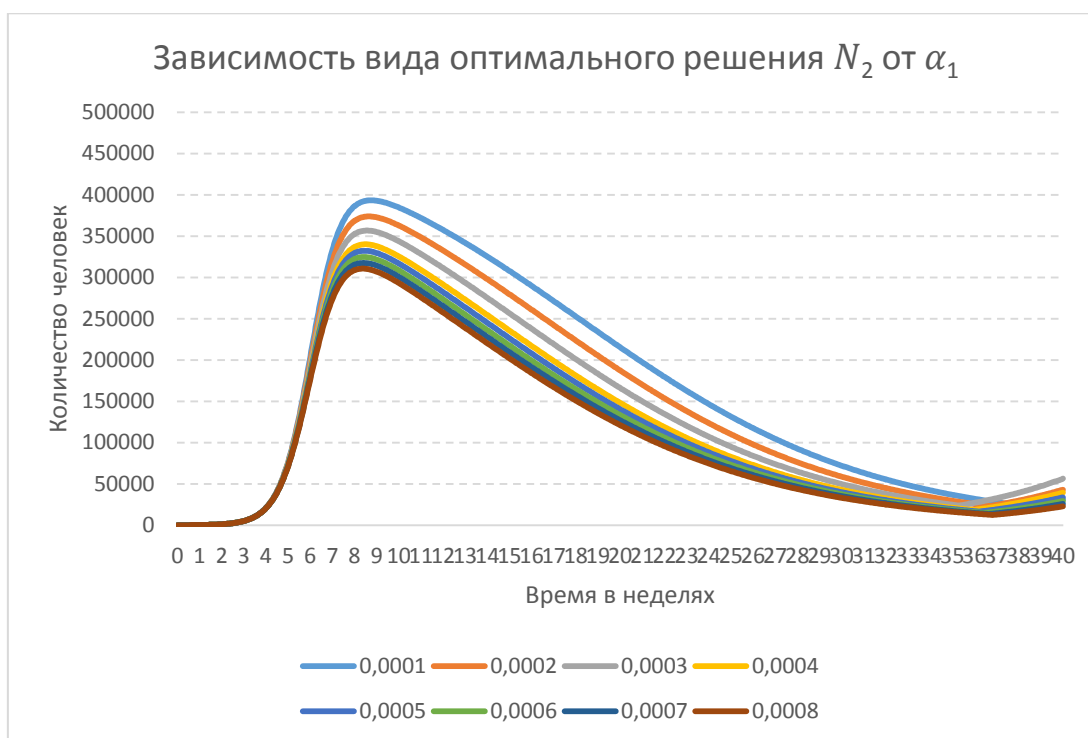


Рисунок 8.2. Зависимость вида оптимального решения  $N_2$  от  $\alpha_1$

Коэффициент  $\alpha_1$  отвечает за силу распространения информации из первого источника. При его увеличении количество агентов первой информации растет на протяжении всего процесса распространения

информации. Время необходимое для распространения информации по внешнему каналу уменьшается.

7) Зависимость решения от выбора значения силы распространения  $\alpha_2$  второго источника. Результаты в виде графиков функций представлены на рисунках 8.3 и 8.4. Численные значения результатов отражены в таблице 8.7.

Таблица 8.7. Зависимость решения от выбора  $\alpha_2$

$\alpha_2$	$I_{min}$	Количество итераций	Победитель	$\tau_1$	$\tau_2$	$\tau_3$
0,0001	-13707501,5052744	13	1	4,36	37,76	3,48
0,0002	-12639702,2489322	9	1	4,32	36,4	3,6
0,0003	-11906962,7971175	13	1	4,12	35,32	3,64
0,0004	-11522868,7066052	14	1	3,88	36,64	3,64
0,0005	-11200428,6240205	14	1	3,72	38	3,64
0,0006	-10909590,8963482	14	1	3,56	38,56	3,64
0,0007	-10656355,7724134	14	1	3,44	38,8	3,64
0,0008	-10430061,1148202	14	1	3,36	38,84	3,64

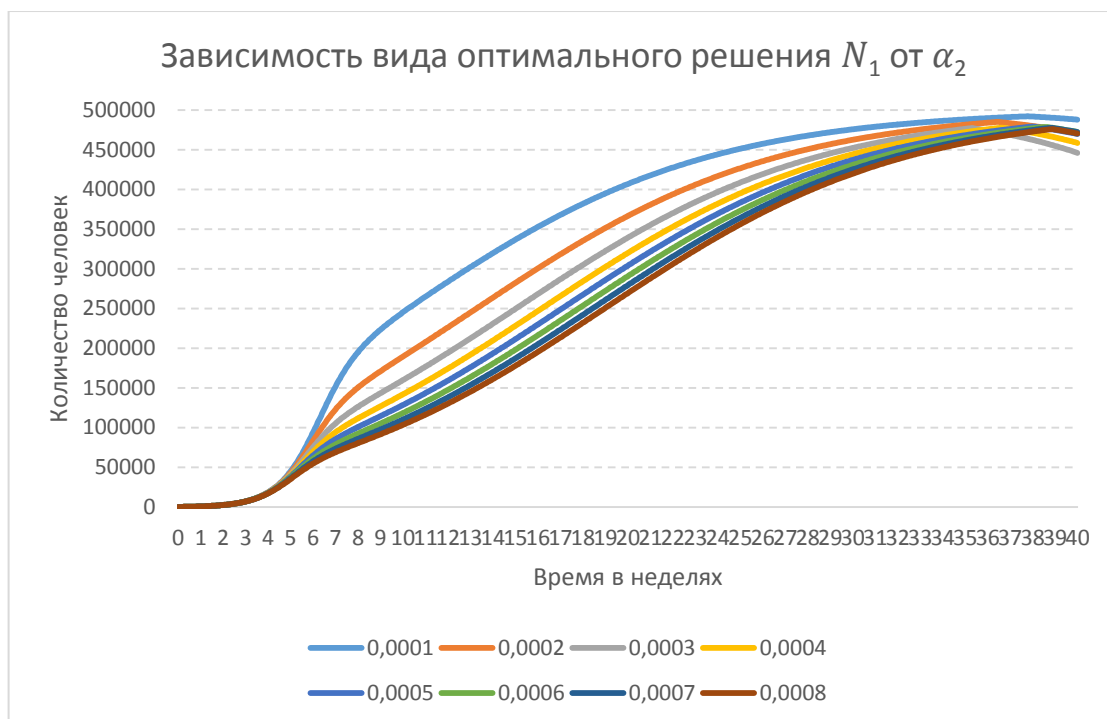


Рисунок 8.3. Зависимость вида оптимального решения  $N_1$  от  $\alpha_2$



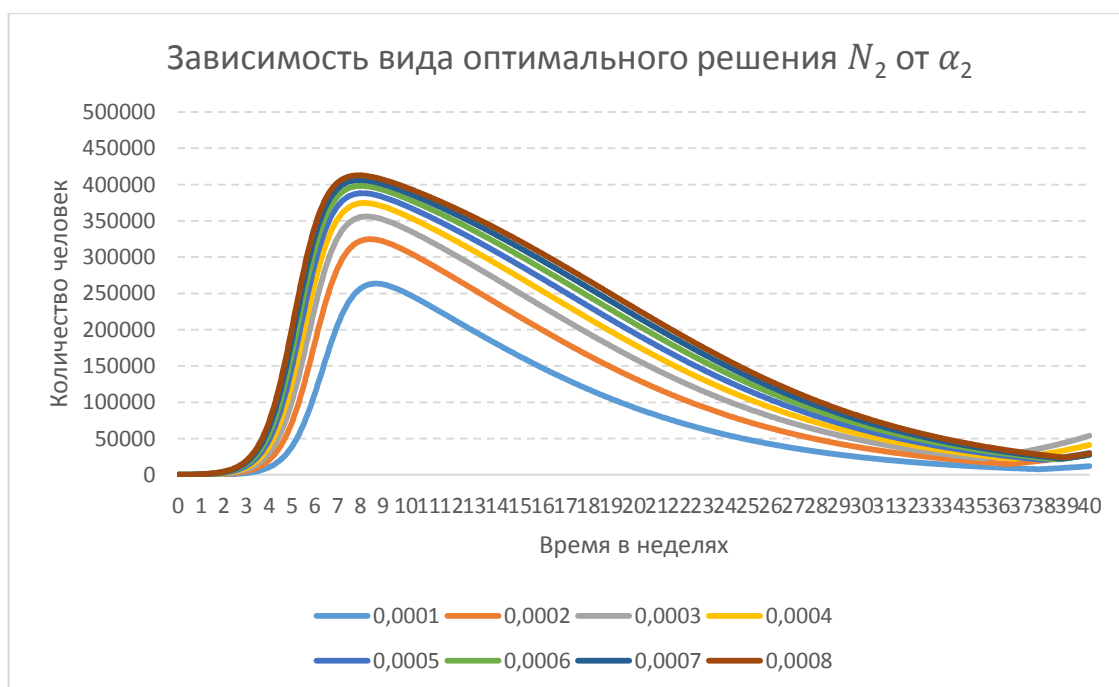


Рисунок 8.4. Зависимость вида оптимального решения  $N_2$  от  $\alpha_2$

Коэффициент  $\alpha_2$  отвечает за силу распространения информации из второго источника. При его увеличении количество агентов первой информации растет на протяжении всего процесса распространения информации. Время необходимое для распространения информации по внешнему каналу уменьшается.

8) Зависимость решения от выбора значения силы распространения  $\beta_1$  второго источника. Числовые характеристики исследуемой модели при различных значениях коэффициента  $\beta_1$  представлены в таблице 8.8.

Таблица 8.8. Зависимость решения от выбора  $\beta_1$

$\beta_1$	$I_{min}$	Количество итераций	Победитель	$\tau_1$	$\tau_2$	$\tau_3$
0,0000010	-34590,2648611637	7	2	0	39,96	1,36
0,0000014	-7634461,13261718	16	1	3,96	38,8	4,6
0,0000018	-10276331,4006851	14	1	3,8	38,84	3,92
0,0000022	-12785716,1481393	9	1	3,88	36,28	3,36
0,0000026	-14991213,5837791	14	1	3,32	38,28	2,76
0,0000030	-16433638,0632689	13	1	3,08	38,84	2,2
0,0000035	-17441200,7657017	13	1	3	38,64	1,64
0,0000040	-17988915,7088773	13	1	3	37,68	1,28

При увеличении значения параметра межличностного общения для первого источника информации, увеличивается скорость распространения информации из первого источника. Период активности рекламной кампании уменьшается, а время перевербовки изменяется незначительно.

Ниже представлены графики (рисунки 8.5 – 8.6.), демонстрирующие зависимость числа агентов первой и второй группы на протяжении всего процесса от выбора параметра  $\beta_1$ .

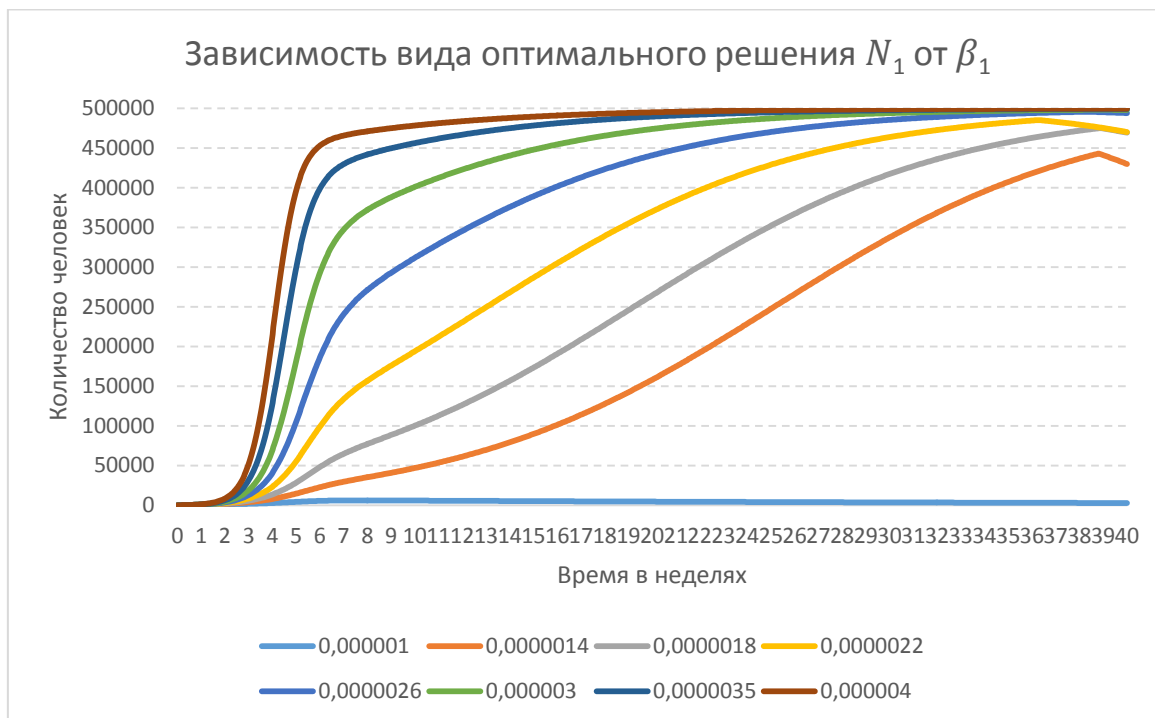


Рисунок 8.5. Зависимость оптимального решения  $N_1$  от  $\beta_1$

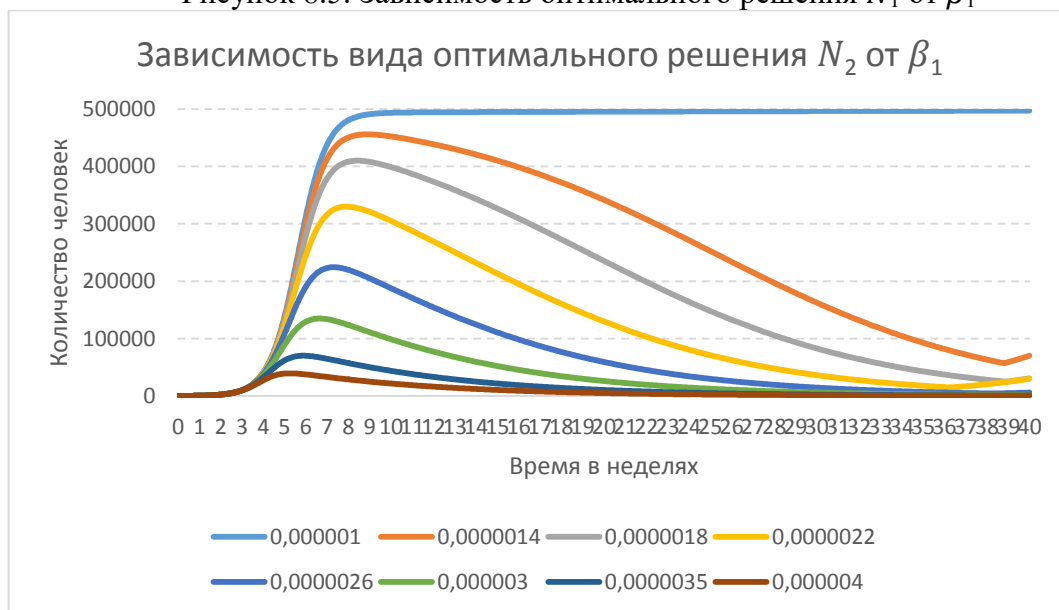


Рисунок 8.6. Зависимость оптимального решения  $N_2$  от  $\beta_1$

9) Исследуем зависимость решения от выбора скорости перевербовки. Результаты представлены в таблице 8.9.

Таблица 8.9. Зависимость решения от выбора скорости перевербовки

№	$v(t)$	$\gamma$	$I_{min}$	Количество итераций	Победитель	$\tau_1$	$\tau_2$	$\tau_3$
1	$9 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	-15226533,49	14	1	3,84	34,12	2,76
2	$8 \cdot 10^{-7}$	$2 \cdot 10^{-7}$	-14485772,94	13	1	3,68	38,36	3
3	$7 \cdot 10^{-7}$	$3 \cdot 10^{-7}$	-13009296,83	12	1	3,8	38,6	3,36
4	$6 \cdot 10^{-7}$	$4 \cdot 10^{-7}$	-9218712,13	14	1	3,68	38,84	3,88
5	$5 \cdot 10^{-7}$	$5 \cdot 10^{-7}$	-2495298,65	27	2	4,08	34,64	3,48
6	$4 \cdot 10^{-7}$	$6 \cdot 10^{-7}$	-547371,78	12	2	0	39,96	2,28
7	$3 \cdot 10^{-7}$	$7 \cdot 10^{-7}$	-282142,57	9	2	0	39,96	1,84
8	$2 \cdot 10^{-7}$	$8 \cdot 10^{-7}$	-153867,77	8	2	0	39,96	1,44
9	$1 \cdot 10^{-7}$	$9 \cdot 10^{-7}$	-97097,05	7	2	0	39,96	1,2

При уменьшении величины  $v(t) - \gamma$  уменьшается скорость перевербовки агентов из второй группы в первую. При уменьшении положительных величин время проведения рекламной кампании и время перевербовки увеличиваются. Когда скорость перевербовки становится неположительной, победителем становится информация из второго источника. Время рекламной кампании уменьшается, а перевербовка при отрицательных значениях величины  $v(t) - \gamma$  осуществляется на протяжении всего процесса. Ниже представлены графики, демонстрирующие зависимость числа агентов первой и второй группы на протяжении всего процесса от величины  $v(t) - \gamma$ .

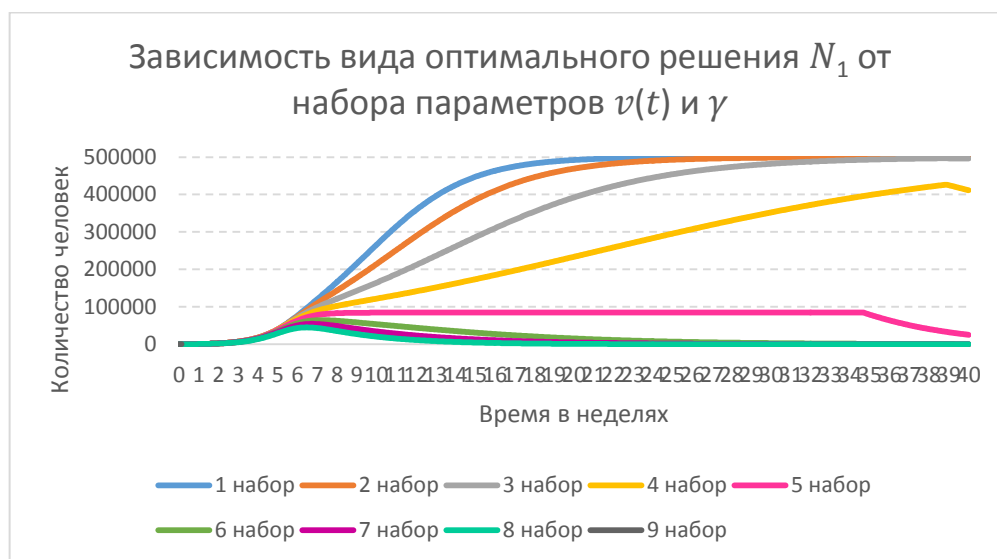


Рисунок 8.7. Зависимость  $N_1$  от выбора скорости перевербовки

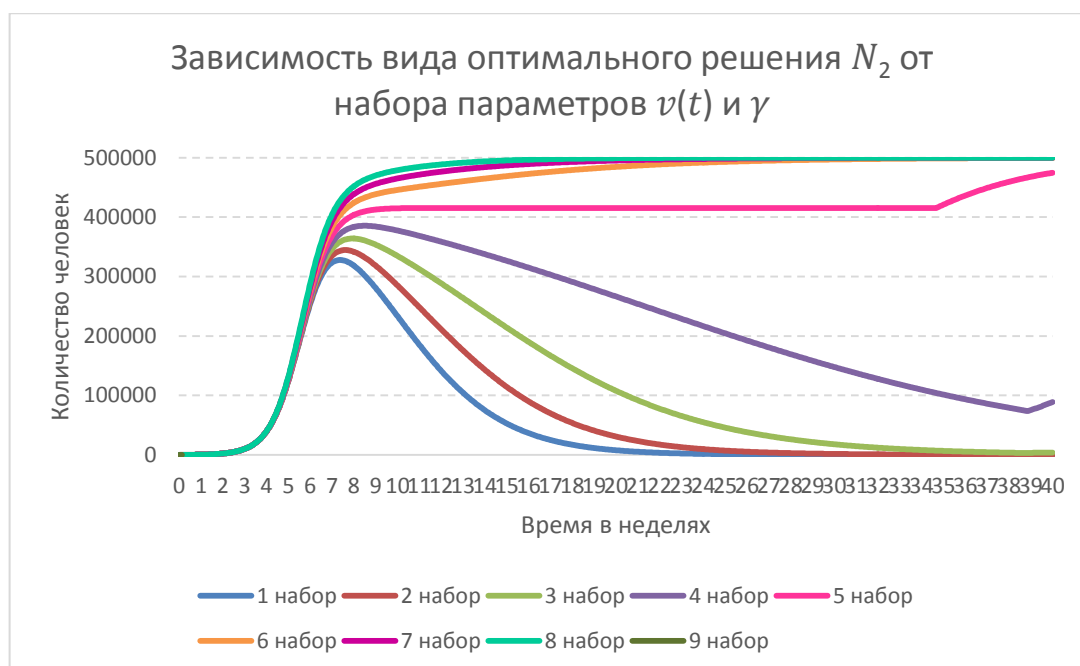


Рис. 8.8. Зависимость  $N_2$  от выбора скорости перевербовки

Анализ зависимости оптимального решения от выбора параметров метода и модели показывает, что изучаемый процесс в силу нелинейности допускает не всегда очевидные режимы развития ситуации. Тем самым, даже в простейших случаях, из анализа информационного противоборства определяются содержательные характеристики, управление которыми может стимулировать протекание этого процесса в нужном направлении.

## **9. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОБНАРУЖЕНИЕ DDOS АТАК С ПОМОЩЬЮ НЕЧЕТКОЙ НЕЙРОННОЙ СЕТИ**

DDoS – это сокращение английского выражения Distributed Denial of Service, что переводится на русский язык как «распределённый отказ от обслуживания». Это означает отказ от обслуживания сетевого ресурса в результате многочисленных распределённых, то есть происходящих с разных точек интернет-доступа, запросов.

Все DDoS атаки можно разделить на три обширные группы:

- первая группа атак направлена на переполнение канала связи;
- вторая группа атак направлена на уязвимости стека сетевых протоколов;
- третья группа атак направлена на уязвимости на уровне приложений.

Атаки, направленные на переполнение канала связи, приводят к насыщению полосы пропускания сетевого ресурса, путем отправки большого количества запросов. Мощность данных атак измеряется в битах в секунду.

Единственным способом борьбы с такими атаками является фильтрация пакетов на уровне промежуточных, специализированных центров обработки данных, с большими канальными мощностями и вычислительными ресурсами. Они способны справиться с большим потоком данных, отфильтровать пакеты злоумышленников и передать на сервер запросы пользователей.

Атаки на уровне протоколов используют ограничения оборудования или уязвимости сетевых протоколов. Они переполняют паразитными пакетами уже не канал связи, а стек с запросами ресурса сервера либо промежуточного оборудования. Результатом таких атак является

неспособность системы обрабатывать полезные запросы. Мощность атак данной группы измеряется в пакетах в секунду.

Одним из способов защиты от подобных атак, является, специально разработанные производителями аппаратных устройств, алгоритмы, которые помогают отсортировать и отфильтровать поток сетевых пакетов. Но, даже эти алгоритмы несовершенны.

Атаки на уровне приложений направлены на уязвимости в приложениях и операционных системах. Они вызывают сбой в работе программного обеспечения сервера или операционной системы в целом.

Подобные атаки весьма узко направлены, из-за чего приводят к серьезному ущербу владельцев сервера при относительно не больших затратах злоумышленников.

Для DDoS-атаки второй группы типа SYN FLOOD имеет смысл построить нечеткий классификатор, позволяющий распознать начало DDoS-атаки. Данный тип атак является одним из самых распространённых. Как и все атаки второй группы, тип атак SYN FLOOD направлен на уязвимость протоколов.

Атаки рассматриваемого типа используют уязвимость в одном из базовых принципов, заложенных в протокол TCP – принципе «тройного рукопожатия». Сетевой узел, инициирующий соединение, отправляет другому сетевому узлу SYN-пакет. После чего он отвечает пакетом SYN-ACK, на что первый узел должна ответить ACK-пакетом. При совершении атаки ACK-пакет не отправляется, в результате чего соединение закрывается только через определенное количество времени. Количество подключений, которые сервер способен одновременно держать открытыми, ограничено, следовательно, при превышении данного лимита подключений, происходит отказ в обслуживании.

Не так давно, в декабре 2016 года, компанией «Ростелеком» были зафиксированы SYN FLOOD атаки на 5 крупнейших банков и финансовых организаций России. Несмотря на то, что атаки были отражены, они

обладали мощностью в 3.2 миллиона пакетов в секунду, при этом самая продолжительная атака длилась более 2 часов.

### 9.1. Постановка задачи

В качестве основы математической модели была взята модель классификатора, предложенная И.И. Слеповичевым, П.В. Ирматовым, М.С. Комаровой и А.А. Бежиным в статье «Обнаружение DDoS атак нечеткой нейронной сетью» [13], затем она была модифицирована.

Классификатор оценивает последовательность пакетов, поступивших серверу на обработку. Существенными являются пакеты с флагом SYN, а также следующие параметры:

- IP адреса отправителя и получателя;
- направление пакета (входящее или исходящее);
- время поступления пакета;
- порт получателя;
- корректность заголовков.

Данные параметры позволяют получить следующую статистику на поступившую последовательность пакетов:

- процент пакетов с различными внешними IP адресами;
- процент пакетов с различными внешними портами;
- среднее время поступления одного пакета;
- процент пакетов с некорректными заголовками.

Для решения задачи анализа воспользуемся аппаратом нечеткой логики. Для формализации знаний экспертов о DDoS атаке создадим пять лингвистических переменных, каждая из которых характеризует одну из компонент вектора параметров.

Построим лингвистические переменные на основе собранной статистики из поступивших серверу пакетов:

1.  $(X_1, \{ \text{«мало»}, \text{«средне»}, \text{«велико»} \}, [0,100], \{ f_{11}(x) = \frac{1}{1+e^{a_{11}(x-b_{11})}}, f_{12}(x) = e^{a_{12}(x-b_{12})^2}, f_{13}(x) = 1 - \frac{1}{1+e^{a_{13}(x-b_{13})}} \} );$  где

$X_1$  – название лингвистической переменной «Время поступления пакетов»;  $x$  – это среднее время поступления одного пакета.

2.  $(X_2, \{ \text{«мал»}, \text{«велик»} \}, [0,100], \{ f_{14}(x) = \frac{1}{1+e^{a_{14}(x-b_{14})}}, f_{15}(x) = 1 - \frac{1}{1+e^{a_{15}(x-b_{15})}} \}$ ; где  $X_2$  – название лингвистической переменной «Процент различных внешних IP адресов»;  $x$  – это процент пакетов с различными внешними IP адресами.

3.  $(X_3, \{ \text{«мал»}, \text{«велик»} \}, [0,100], \{ f_{16}(x) = \frac{1}{1+e^{a_{16}(x-b_{16})}}, f_{17}(x) = 1 - \frac{1}{1+e^{a_{17}(x-b_{17})}} \})$ ; где  $X_3$  – название лингвистической переменной «Процент различных портов»;  $x$  – это процент пакетов с различными внешними портами.

4.  $(X_4, \{ \text{«велик»} \}, [0,100], \{ f_{18}(x) = \frac{1}{1+e^{a_{18}(x-b_{18})}} \})$ ; где  $X_4$  – название лингвистической переменной «Процент пакетов с поврежденными заголовками»;  $x$  – это процент пакетов с некорректными заголовками.

5.  $(S, \{ \text{«низкая»}, \text{«средняя»}, \text{«высокая»} \}, [0,100], \{ f_{41}(x) = \frac{1}{1+e^{a_{41}(x-b_{41})}}, f_{42}(x) = e^{a_{42}(x-b_{42})^2}, f_{43}(x) = 1 - \frac{1}{1+e^{a_{43}(x-b_{43})}} \})$ ; где  $S$  – название лингвистической переменной «Степень уверенности»;  $x$  – это выходной сигнал нейронной сети.

Для определения степени уверенности в угрозе, введем следующие правила:

1. если  $X_1$  есть «мало» И ( $X_2$  есть «мал» ИЛИ  $X_3$  есть «мал» ИЛИ  $X_4$  есть «велик»), тогда  $S$  есть «высокая»;
2. если ( $X_1$  есть «мало» ИЛИ  $X_1$  есть «средне») И ( $X_2$  есть «велик» ИЛИ  $X_3$  есть «велик»), тогда  $S$  есть «средняя»;
3. если  $X_1$  есть «велико», тогда  $S$  есть «низкая».

Для реализации нечеткой системы классификатора может быть использована многослойная нейронная сеть с прямым распространением сигнала.



Указанное представление нечеткого классификатора дает возможность использовать такие достоинства нейронных сетей, как обучение и адаптация под конкретную ситуацию. Это может быть полезным в том случае, когда конкретные параметры лингвистических переменных неизвестны и подбирать их приходится в процессе эксплуатации системы обнаружения атак.

На основе приведенных лингвистических переменных и правил определения уверенности в угрозе построена нейронная сеть со структурой, приведенной на рисунке 9.1.

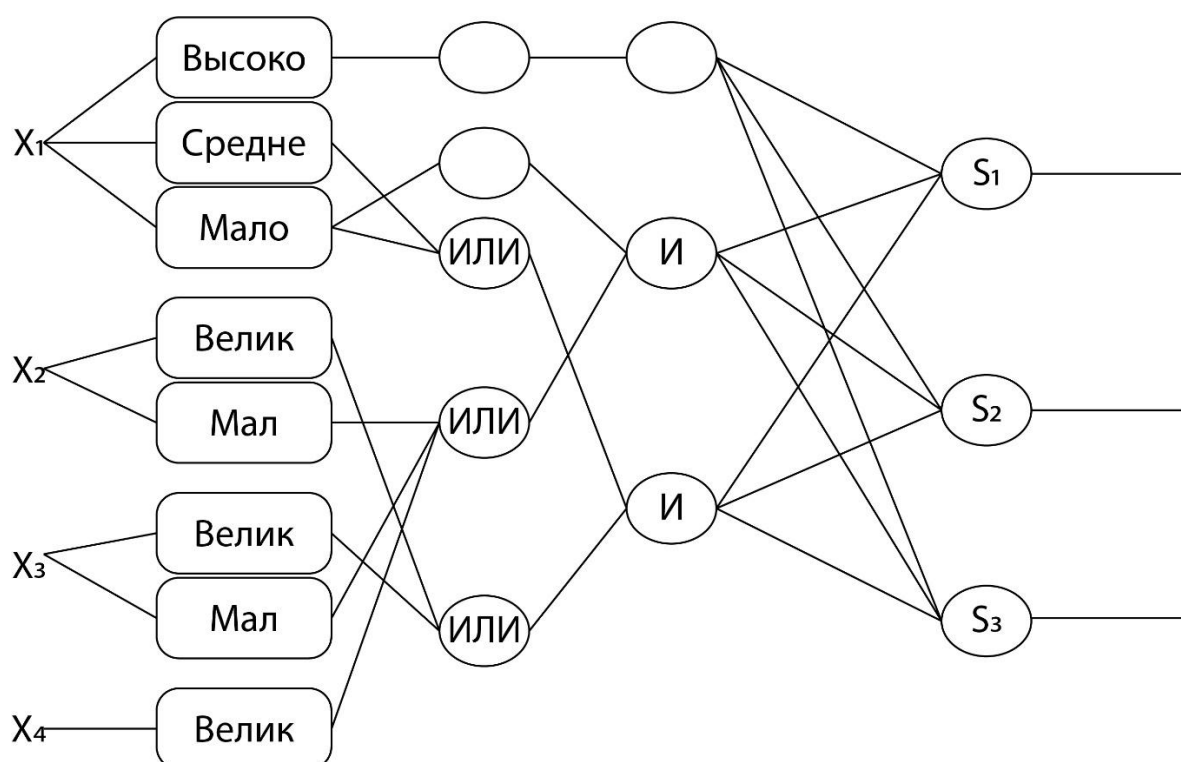


Рисунок 9.1. Структура нечеткого классификатора

Эта сеть имеет 4 входа ( $X_1 - X_4$ ) и 4 слоя с нейронами.

**1 слой.** Нейроны этого слоя предназначены для расчета степени принадлежности входных сигналов нечетким множествам. Он не имеет весовых коэффициентов, а функциями активации являются функции принадлежности из лингвистических переменных, приведенных выше.

**2 и 3 слои.** Нейроны данных слоев вычисляют степень истинности предпосылок каждого правила. Для расчёта истинности предпосылок

правил используются нейроны трех видов: «И»-нейрон, «ИЛИ»-нейрон и нейрон «смещения».

**Нечеткий нейрон «И».** Сигналы  $x_i$  и веса  $w_i$  в данном случае объединяются с помощью треугольной конормы:

$$p_i = K(w_i, x_i), i = 1, 2, \dots, n,$$

а выход образуется с применением треугольной нормы:

$$y = T(p_1, p_2, \dots, p_n) = T(K(w_1, x_1), K(w_2, x_2), \dots, K(w_n, x_n)).$$

**Нечеткий нейрон «ИЛИ».** Сигналы  $x_i$  и веса  $w_i$  здесь объединяются с помощью треугольной нормы:

$$p_i = T(w_i, x_i), i = 1, 2, \dots, n,$$

а выход образуется с применением треугольной конормы:

$$y = K(p_1, p_2, \dots, p_n) = K(T(w_1, x_1), T(w_2, x_2), \dots, T(w_n, x_n)).$$

**Нейрон «смещения».** Данный нейрон предназначен для передачи сигнала на следующий слой. Поэтому он имеет только один вход и не имеет весовых коэффициентов, а его выходом является его входной сигнал

$$y = x.$$

**4 слой.** Нейроны этого слоя являются обычными нейронами с функцией активации следующего вида:

$$f_i = f_{5i} \left( \sum_{j=1}^n x_j w_j \right),$$

где  $n$  – число нейронов с предыдущего слоя (в модели представленной выше  $n = 3$ ),  $f_{5i}, i = 1, 2, 3$  – функции принадлежности для лингвистической переменной  $S$  («Степень уверенности») к нечетким множествам «низкая», «средняя» и «высокая» соответственно.

Треугольная норма  $T$  будет иметь следующий вид:

$$T(a, b) = a \cdot b.$$

Треугольная норма  $K$  будет иметь следующий вид:

$$K(a, b) = a + b - a \cdot b.$$

Для описания математической модели введем обозначения:

- $y_i^k$  – функция рассчитывающая выходное значение  $i$ -го нейрона с  $k$ -го слоя;
- $a_{ki}$  – параметр функции активации сигмоидного вида  $i$ -го нейрона с  $k$ -го слоя;
- $b_{ki}$  – параметр функции активации сигмоидного вида  $i$ -го нейрона с  $k$ -го слоя;
- $X_i$  –  $i$ -й элемент входного вектора;
- $w_{ij}^k$  – весовой коэффициент связи между  $i$ -м нейроном  $k$ -го слоя и  $j$ -м нейроном с  $(k + 1)$ -го слоя.

Входные сигналы преобразуются в значения нейронов 1-го слоя по формулам:

$$\begin{aligned} y_1^1 &= \frac{1}{1+e^{a_{11}(X_1-b_{11})}}; y_2^1 = e^{a_{12}(X_1-b_{12})^2}; y_3^1 = 1 - \frac{1}{1+e^{a_{13}(X_1-b_{13})}}; \\ y_4^1 &= \frac{1}{1+e^{a_{14}(X_2-b_{14})}}; y_5^1 = 1 - \frac{1}{1+e^{a_{15}(X_2-b_{15})}}; y_6^1 = \frac{1}{1+e^{a_{16}(X_3-b_{16})}}; \\ y_7^1 &= 1 - \frac{1}{1+e^{a_{17}(X_3-b_{17})}}; y_8^1 = \frac{1}{1+e^{a_{18}(X_4-b_{18})}}; \end{aligned}$$

На втором слое значения нейронов вычисляются по формулам:

$$\begin{aligned} y_1^2 &= y_1^1; y_2^2 = y_3^1; \\ y_3^2 &= \text{ИЛИ}_1 = K(T(w_{23}^1; y_2^1); T(w_{33}^1; y_3^1)) = \\ &= w_{23}^1 \cdot y_2^1 + w_{33}^1 \cdot y_3^1 - w_{23}^1 \cdot w_{33}^1 \cdot y_2^1 \cdot y_3^1; \\ y_4^2 &= \text{ИЛИ}_2 = K(T(w_{54}^1; y_5^1); K(T(w_{74}^1; y_7^1); T(w_{84}^1; y_8^1))) = \\ &= w_{54}^1 \cdot y_5^1 + w_{74}^1 \cdot y_7^1 + w_{84}^1 \cdot y_8^1 - w_{74}^1 \cdot w_{84}^1 \cdot y_7^1 \cdot y_8^1 - \\ &- w_{54}^1 \cdot y_5^1 (w_{74}^1 \cdot y_7^1 + w_{84}^1 \cdot y_8^1 - w_{74}^1 \cdot w_{84}^1 \cdot y_7^1 \cdot y_8^1); \\ y_5^2 &= \text{ИЛИ}_3 = K(T(w_{45}^1; y_4^1); T(w_{65}^1; y_6^1)) = \\ &= w_{45}^1 \cdot y_4^1 + w_{65}^1 \cdot y_6^1 - w_{45}^1 \cdot w_{65}^1 \cdot y_4^1 \cdot y_6^1. \end{aligned}$$

На третьем слое значения нейронов вычисляются по формулам:

$$\begin{aligned} y_1^3 &= y_1^1; \\ y_2^3 &= \text{И}_1 = T(K(w_{22}^2; y_3^1); K(w_{42}^2; y_4^2)) = \\ &= (w_{22}^2 + y_3^1 - w_{22}^2 \cdot y_3^1)(w_{42}^2 + y_4^2 - w_{42}^2 \cdot y_4^2); \end{aligned}$$

$$y_3^3 = H_2 = T\left(K(w_{33}^2; y_3^2); K(w_{43}^2; y_5^2)\right) = \\ = (w_{33}^2 + y_3^2 - w_{33}^2 \cdot y_3^2)(w_{43}^2 + y_5^2 - w_{43}^2 \cdot y_5^2).$$

Выходные значения на последнем слое нейронной сети вычисляются по формулам:

$$y_1 = \frac{1}{1 + e^{a_{41}(s_1 - b_{41})}};$$

$$y_2 = e^{a_{42}(s_2 - b_{42})^2};$$

$$y_3 = 1 - \frac{1}{1 + e^{a_{43}(s_3 - b_{43})}};$$

$$s_1 = \sum_{i=1}^3 w_{i1}^3 y_i^3,$$

$$s_2 = \sum_{i=1}^3 w_{i2}^3 y_i^3,$$

$$s_3 = \sum_{i=1}^3 w_{i3}^3 y_i^3.$$

## 9.2. Обучение нейронной сети

Перед использованием нейронная сеть должна быть обучена. В данном случае целесообразно использовать обучение с учителем.

Решение задачи анализа заключается в обучение нейронной сети посредством минимизации функции ошибки:

$$\varepsilon = \frac{1}{2} \sum_{i=1}^3 (d_i - y_i)^2,$$

здесь  $i$  – номер выходного нейрона сети,  $d_i$  – ожидаемый выход,  $y_i$  –  $i$ -й выход нейронной сети.

Обучение нейронной сети будет производиться методом обратного распространения ошибки, который состоит в следующем: на каждой итерации алгоритма обратного распространения ошибки весовые коэффициенты нейронной сети модифицируются так, чтобы минимизировать значение функции ошибки  $\varepsilon$ . Таким образом, в процессе обучения циклически решаются однокритериальные задачи оптимизации методом градиентного спуска.

Формулы классического алгоритма градиентного спуска применить в общем виде невозможно, так как в представленной модели нейронной сети присутствуют нейроны различного типа, с различными функциями активации.

Можно описать модифицированный алгоритм следующим образом:

1. Инициализируется сеть. Весовым коэффициентам и параметрам функций активации сигмоидного вида ставятся в соответствие случайные небольшие начальные значения.

2. На вход сети подается очередная обучающая пара: входной вектор и вектор ожидаемого выхода.

3. Рассчитывается выход сети:

$$y_1 = \frac{1}{1 + e^{a_{41}(\sum_{i=1}^3 w_{i1}^3 y_i^3 - b_{41})}},$$

$$y_2 = e^{a_{42}(\sum_{i=1}^3 w_{i2}^3 y_i^3 - b_{42})},$$

$$y_3 = 1 - \frac{1}{1 + e^{a_{43}(\sum_{i=1}^3 w_{i3}^3 y_i^3 - b_{43})}}.$$

4. Рассчитывается значение функции ошибки:

$$\varepsilon = \frac{1}{2} \sum_{i=1}^3 (d_i - y_i)^2.$$

5. Если значение ошибки  $\varepsilon$  меньше заданного значения, то переход к шагу 8, иначе переход к шагу 6.

6. Корректируются весовые коэффициенты сети и параметры функций активации сигмоидального вида:

$$(w_{ij}^k)^{l+1} = \left( w_{ij}^k - \eta_1 \frac{\partial \varepsilon}{\partial w_{ij}^k} \right)^l;$$

$$(a_{ij})^{l+1} = \left( a_{ij} - \eta_2 \frac{\partial \varepsilon}{\partial a_{ij}} \right)^l;$$

$$(b_{ij})^{l+1} = \left( b_{ij} - \eta_3 \frac{\partial \varepsilon}{\partial b_{ij}} \right)^l,$$

здесь  $l$  - номер обучающей итерации.

7. Переход к шагу 3.

8. Если остались обучающие образы, то переход к шагу 2, иначе окончание обучения.

Частные производные, используемые в шаге 6 алгоритма, вычисляются по формулам, приведенным ниже.

Частные производные параметров функция активации сигмоидного вида нейронов выходного слоя определяются следующим образом:

$$\begin{aligned}
 \frac{\partial \varepsilon}{\partial a_{41}} &= \frac{1}{2} \cdot \frac{\partial (d_1 - y_1)^2}{\partial y_1} \cdot \frac{\partial y_1}{\partial a_{41}} = \frac{1}{2} \cdot 2 \cdot (d_1 - y_1) \cdot (-1) \cdot \frac{\partial \left( \frac{1}{1 + e^{a_{41}(s_1 - b_{41})}} \right)}{\partial a_{41}} \\
 &= \\
 &= (d_1 - y_1) \cdot \frac{1}{1 + e^{a_{41}(s_1 - b_{41})}} \cdot \frac{e^{a_{41}(s_1 - b_{41})}}{1 + e^{a_{41}(s_1 - b_{41})}} \cdot (s_1 - b_{41}) = \\
 &= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot (s_1 - b_{41}); \\
 \frac{\delta \varepsilon}{\partial b_{41}} &= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot (-a_{41}); \\
 \frac{\delta \varepsilon}{\partial a_{42}} &= -(d_2 - y_2) \cdot y_2 \cdot (s_2 - b_{42})^2; \\
 \frac{\delta \varepsilon}{\partial b_{42}} &= (d_2 - y_2) \cdot y_2 \cdot a_{42} \cdot 2 \cdot (s_2 - b_{42}); \\
 \frac{\delta \varepsilon}{\partial a_{43}} &= -(d_3 - y_3) \cdot y_3 \cdot (1 - y_3) \cdot (s_3 - b_{43}); \\
 \frac{\delta \varepsilon}{\partial b_{43}} &= -(d_3 - y_3) \cdot y_3 \cdot (1 - y_3) \cdot (-a_{43}); \\
 \frac{\partial \varepsilon}{\partial w_{11}^3} &= \frac{1}{2} \cdot \frac{\partial (d_1 - y_1)^2}{\partial y_1} \cdot \frac{\partial y_1}{\partial w_{11}^3} = -(d_1 - y_1) \cdot \frac{\partial \left( \frac{1}{1 + e^{a_{41}(s_1 - b_{41})}} \right)}{\partial s_1} \cdot \frac{\partial s_1}{\partial w_{11}^3} = \\
 &= (d_1 - y_1) \cdot \frac{e^{a_{41}(s_1 - b_{41})}}{(1 + e^{a_{41}(s_1 - b_{41})})^2} \cdot \frac{\partial (a_{41}(s_1 - b_{41}))}{\partial s_1} \cdot \frac{\partial s_1}{\partial w_{11}^3} = \\
 &= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot a_{41} \cdot \frac{\partial (w_{11}^3 \cdot y_1^1 + w_{21}^3 \cdot y_2^3 + w_{31}^3 \cdot y_3^3)}{\partial w_{11}^3} =
 \end{aligned}$$

$$= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot a_{41} \cdot y_1^1.$$

Частные производные весовых коэффициентов связей нейронов с третьего и четвертого слоев определяются следующим образом:

$$\begin{aligned} \frac{\partial \varepsilon}{\partial w_{21}^3} &= \frac{1}{2} \cdot \frac{\partial (d_1 - y_1)^2}{\partial y_1} \cdot \frac{\partial y_1}{\partial w_{21}^3} = -(d_1 - y_1) \cdot \frac{\partial \left( \frac{1}{1 + e^{a_{41}(s_1 - b_{41})}} \right)}{\partial s_1} \cdot \frac{\partial s_1}{\partial w_{21}^3} = \\ &= (d_1 - y_1) \cdot \frac{e^{a_{41}(s_1 - b_{41})}}{(1 + e^{a_{41}(s_1 - b_{41})})^2} \cdot \frac{\partial (a_{41}(s_1 - b_{41}))}{\partial s_1} \cdot \frac{\partial s_1}{\partial w_{21}^3} = \\ &= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot a_{41} \cdot \frac{\partial s_1}{\partial w_{21}^3} = \\ &= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot a_{41} \cdot \frac{\partial (w_{11}^3 \cdot y_1^1 + w_{21}^3 \cdot y_2^3 + w_{31}^3 \cdot y_3^3)}{\partial w_{21}^3} = \\ &= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot a_{41} \cdot y_2^3; \\ \frac{\partial \varepsilon}{\partial w_{31}^3} &= (d_1 - y_1) \cdot y_1 \cdot (1 - y_1) \cdot a_{41} \cdot y_3^3; \\ \frac{\partial \varepsilon}{\partial w_{12}^3} &= -2 \cdot a_{42} \cdot (d_2 - y_2) \cdot y_2 \cdot (s_2 - b_{42}) \cdot y_1^1; \\ \frac{\partial \varepsilon}{\partial w_{22}^3} &= -2 \cdot a_{42} \cdot (d_2 - y_2) \cdot y_2 \cdot (s_2 - b_{42}) \cdot y_2^3; \\ \frac{\partial \varepsilon}{\partial w_{32}^3} &= -2 \cdot a_{42} \cdot (d_2 - y_2) \cdot y_2 \cdot (s_2 - b_{42}) \cdot y_3^3; \\ \frac{\partial \varepsilon}{\partial w_{13}^3} &= -(d_3 - y_3) \cdot y_3 \cdot (1 - y_3) \cdot a_{43} \cdot y_1^1; \\ \frac{\partial \varepsilon}{\partial w_{23}^3} &= -(d_3 - y_3) \cdot y_3 \cdot (1 - y_3) \cdot a_{43} \cdot y_2^3; \\ \frac{\partial \varepsilon}{\partial w_{33}^3} &= -(d_3 - y_3) \cdot y_3 \cdot (1 - y_3) \cdot a_{43} \cdot y_3^3. \end{aligned}$$

Частные производные весовых коэффициентов связей нейронов со второго и третьего слоев определяются следующим образом:

$$\begin{aligned} \frac{\partial \varepsilon}{\partial w_{22}^2} &= (\delta_{w_{21}^3} \cdot w_{21}^3 + \delta_{w_{22}^3} \cdot w_{22}^3 + \delta_{w_{23}^3} \cdot w_{23}^3) \cdot \frac{\partial y_2^3}{\partial w_{22}^2} = \\ &= (\delta_{w_{21}^3} \cdot w_{21}^3 + \delta_{w_{22}^3} \cdot w_{22}^3 + \delta_{w_{23}^3} \cdot w_{23}^3) \cdot \end{aligned}$$

$$\begin{aligned}
& \cdot \frac{\partial(w_{22}^2 + y_3^1 - w_{22}^2 \cdot y_3^1)(w_{42}^2 + y_4^2 - w_{42}^2 \cdot y_4^2)}{\partial w_{22}^2} = \\
& = (\delta_{w_{21}^3} \cdot w_{21}^3 + \delta_{w_{22}^3} \cdot w_{22}^3 + \delta_{w_{23}^3} \cdot w_{23}^3) \cdot (w_{42}^2 + y_4^2 - w_{42}^2 \cdot y_4^2) \cdot (1 - y_3^1); \\
& \frac{\partial \varepsilon}{\partial w_{42}^2} = (\delta_{w_{21}^3} \cdot w_{21}^3 + \delta_{w_{22}^3} \cdot w_{22}^3 + \delta_{w_{23}^3} \cdot w_{23}^3) \cdot (w_{22}^2 + y_3^1 - w_{22}^2 \cdot y_3^1) \cdot \\
& \quad \cdot (1 - y_4^2); \\
& \frac{\partial \varepsilon}{\partial w_{33}^2} = (\delta_{w_{31}^3} \cdot w_{31}^3 + \delta_{w_{32}^3} \cdot w_{32}^3 + \delta_{w_{33}^3} \cdot w_{33}^3) \cdot (w_{43}^2 + y_5^2 - w_{43}^2 \cdot y_5^2) \cdot \\
& \quad \cdot (1 - y_3^2); \\
& \frac{\partial \varepsilon}{\partial w_{43}^2} = (\delta_{w_{31}^3} \cdot w_{31}^3 + \delta_{w_{32}^3} \cdot w_{32}^3 + \delta_{w_{33}^3} \cdot w_{33}^3) \cdot (w_{33}^2 + y_3^2 - w_{33}^2 \cdot y_3^2) \cdot \\
& \quad \cdot (1 - y_5^2).
\end{aligned}$$

Частные производные весовых коэффициентов связей нейронов с первого и второго слоев определяются следующим образом:

$$\begin{aligned}
& \frac{\partial \varepsilon}{\partial w_{23}^1} = \delta_{w_{33}^2} \cdot (1 - w_{33}^2) \cdot \frac{\partial y_3^2}{\partial w_{23}^1} = \\
& = \delta_{w_{33}^2} \cdot (1 - w_{33}^2) \cdot \frac{\partial(w_{23}^1 \cdot y_2^1 + w_{33}^1 \cdot y_3^1 - w_{23}^1 \cdot w_{33}^1 \cdot y_2^1 \cdot y_3^1)}{\partial w_{23}^1} = \\
& = \delta_{w_{33}^2} \cdot (1 - w_{33}^2) \cdot (y_2^1 - w_{33}^1 \cdot y_2^1 \cdot y_3^1) = \\
& = \delta_{w_{33}^2} \cdot (1 - w_{33}^2) \cdot (1 - w_{33}^1 \cdot y_3^1) \cdot y_2^1; \\
& \frac{\partial \varepsilon}{\partial w_{33}^1} = \delta_{w_{33}^2} \cdot (1 - w_{33}^2) \cdot (1 - w_{23}^1 \cdot y_2^1) \cdot y_3^1; \\
& \frac{\partial \varepsilon}{\partial w_{54}^1} = \delta_{w_{42}^2} \cdot (1 - w_{42}^2) \cdot (1 - w_{74}^1 \cdot y_7^1 + w_{84}^1 \cdot y_8^1 - w_{74}^1 \cdot w_{84}^1 \cdot y_7^1 \cdot y_8^1) \cdot y_5^1; \\
& \frac{\partial \varepsilon}{\partial w_{74}^1} = \delta_{w_{42}^2} \cdot (1 - w_{42}^2) \cdot (1 - w_{84}^1 \cdot y_8^1 - w_{54}^1 \cdot y_5^1 \cdot (1 - w_{84}^1 \cdot y_8^1)) \cdot y_7^1; \\
& \frac{\partial \varepsilon}{\partial w_{84}^1} = \delta_{w_{42}^2} \cdot (1 - w_{42}^2) \cdot (1 - w_{74}^1 \cdot y_7^1 - w_{54}^1 \cdot y_5^1 \cdot (1 - w_{74}^1 \cdot y_7^1)) \cdot y_8^1; \\
& \frac{\partial \varepsilon}{\partial w_{45}^1} = \delta_{w_{43}^2} \cdot (1 - w_{43}^2) \cdot (1 - w_{65}^1 \cdot y_6^1) \cdot y_4^1;
\end{aligned}$$



$$\frac{\partial \varepsilon}{\partial w_{65}^1} = \delta_{w_{43}^2} \cdot (1 - w_{43}^2) \cdot (1 - w_{45}^1 \cdot y_4^1) \cdot y_6^1.$$

Частные производные параметров функция активации сигмоидного вида нейронов входного слоя определяются следующим образом:

$$\begin{aligned} \frac{\partial \varepsilon}{\partial a_{11}} &= (\delta_{w_{11}^3} \cdot w_{11}^3 + \delta_{w_{12}^3} \cdot w_{12}^3 + \delta_{w_{13}^3} \cdot w_{13}^3) \cdot \frac{\partial y_1^1}{\partial a_{11}} = \\ &= (\delta_{w_{11}^3} \cdot w_{11}^3 + \delta_{w_{12}^3} \cdot w_{12}^3 + \delta_{w_{13}^3} \cdot w_{13}^3) \frac{\partial \left( \frac{1}{1 + e^{a_{11}(X_1 - b_{11})}} \right)}{\partial a_{11}} = \\ &= -(\delta_{w_{11}^3} \cdot w_{11}^3 + \delta_{w_{12}^3} \cdot w_{12}^3 + \delta_{w_{13}^3} \cdot w_{13}^3) \cdot \frac{e^{a_{11}(X_1 - b_{11})}}{(1 + e^{a_{11}(X_1 - b_{11})})^2} \cdot \\ &\quad \cdot \frac{\partial (a_{11}(X_1 - b_{11}))}{\partial a_{11}} \\ &= -(\delta_{w_{11}^3} \cdot w_{11}^3 + \delta_{w_{12}^3} \cdot w_{12}^3 + \delta_{w_{13}^3} \cdot w_{13}^3) \cdot y_1^1 \cdot (1 - y_1^1) \cdot (X_1 - b_{11}); \\ \frac{\partial \varepsilon}{\partial b_{11}} &= (\delta_{w_{11}^3} \cdot w_{11}^3 + \delta_{w_{12}^3} \cdot w_{12}^3 + \delta_{w_{13}^3} \cdot w_{13}^3) \cdot y_1^1 \cdot (1 - y_1^1) \cdot a_{11}; \\ \frac{\partial \varepsilon}{\partial a_{12}} &= \delta_{w_{23}^1} \cdot w_{23}^1 \cdot y_2^1 \cdot (X_1 - b_{12})^2; \\ \frac{\partial \varepsilon}{\partial b_{12}} &= -\delta_{w_{23}^1} \cdot w_{23}^1 \cdot y_2^1 \cdot a_{12} \cdot 2 \cdot (X_1 - b_{12}); \\ \frac{\partial \varepsilon}{\partial a_{13}} &= (\delta_{w_{22}^2} \cdot (1 - w_{22}^2) + \delta_{w_{33}^1} \cdot w_{33}^1) \cdot y_3^1 \cdot (1 - y_3^1) \cdot (X_1 - b_{13}); \\ \frac{\partial \varepsilon}{\partial b_{13}} &= -(\delta_{w_{22}^2} \cdot (1 - w_{22}^2) + \delta_{w_{33}^1} \cdot w_{33}^1) \cdot y_3^1 \cdot (1 - y_3^1) \cdot a_{13}; \\ \frac{\partial \varepsilon}{\partial a_{14}} &= -\delta_{w_{45}^1} \cdot w_{45}^1 \cdot y_4^1 \cdot (1 - y_4^1) \cdot (X_2 - b_{14}); \\ \frac{\partial \varepsilon}{\partial b_{14}} &= \delta_{w_{45}^1} \cdot w_{45}^1 \cdot y_4^1 \cdot (1 - y_4^1) \cdot a_{14}; \\ \frac{\partial \varepsilon}{\partial a_{15}} &= \delta_{w_{54}^1} \cdot w_{54}^1 \cdot y_5^1 \cdot (1 - y_5^1) \cdot (X_2 - b_{15}); \\ \frac{\partial \varepsilon}{\partial b_{15}} &= -\delta_{w_{54}^1} \cdot w_{54}^1 \cdot y_5^1 \cdot (1 - y_5^1) \cdot a_{15}; \end{aligned}$$

$$\frac{\partial \varepsilon}{\partial a_{16}} = -\delta_{w_{65}^1} \cdot w_{65}^1 \cdot y_6^1 \cdot (1 - y_6^1) \cdot (X_3 - b_{16});$$

$$\frac{\partial \varepsilon}{\partial b_{16}} = \delta_{w_{65}^1} \cdot w_{65}^1 \cdot y_6^1 \cdot (1 - y_6^1) \cdot a_{16};$$

$$\frac{\partial \varepsilon}{\partial a_{17}} = \delta_{w_{74}^1} \cdot w_{74}^1 \cdot y_7^1 \cdot (1 - y_7^1) \cdot (X_3 - b_{17});$$

$$\frac{\partial \varepsilon}{\partial b_{17}} = -\delta_{w_{74}^1} \cdot w_{74}^1 \cdot y_7^1 \cdot (1 - y_7^1) \cdot a_{17};$$

$$\frac{\partial \varepsilon}{\partial a_{18}} = -\delta_{w_{84}^1} \cdot w_{84}^1 \cdot y_8^1 \cdot (1 - y_8^1) \cdot (X_4 - b_{18});$$

$$\frac{\partial \varepsilon}{\partial b_{18}} = \delta_{w_{84}^1} \cdot w_{84}^1 \cdot y_8^1 \cdot (1 - y_8^1) \cdot a_{18}.$$

### 9.3. Программная реализация

Используя расчеты, представленные выше, была написана программная реализация модели нечеткого классификатора. Реализованная программа представляет собой библиотеку, написанную на языке Java 8. Данную библиотеку можно подключить к веб-серверу и осуществлять анализ трафика, проходящего к веб-серверу. Для обучения нейронной сети, был смоделирован набор обучающих векторов.

Для демонстрации работы программы был добавлен класс, реализующий REST API и веб-страницы для ввода данных и вывода результатов. Веб интерфейс для проверки работы программы имеет вид, представленный на рисунке 9.2.

При ответе сервера, отображается только один блок результата: зеленый (низкая уверенность в атаке), желтый (средняя уверенность в атаке), красный (высокая уверенность в атаке).

## Анализ степени уверенности в атаке

Время поступления пакетов

Введите показатель среднего времени поступления одного пакета среди отобранных для анализа пакетов.

Процент различных внешних IP адресов

Введите значение, отображающее процент различных внешних IP адресов среди отобранных для анализа пакетов.

Процент различных портов

Введите значение, отображающее процент различных портов среди отобранных для анализа пакетов.

Процент пакетов с поврежденными заголовками

Введите значение, отображающее процент пакетов с поврежденными заголовками среди отобранных для анализа пакетов.

Проверить

## Результат анализа

N - Время поступления пакетов

N - Процент различных внешних IP адресов

N - Процент различных портов

N - Процент пакетов с поврежденными заголовками

Низкий уровень уверенности в атаке.

Средний уровень уверенности в атаке.

Высокий уровень уверенности в атаке.

Ввести другие значения

Рисунок 9.2. Веб-интерфейс ввода входного вектора и ответа классификатора

Обучение нейронной сети производилось на наборе обучающих примеров следующего вида:

- Входной вектор = (X1: 54.0; X2: 80.0; X3: 32.0; X4: 25.0)
  - Выход сети = (y1: 0.0; y2: 0.9; y3: 0.0)
- Входной вектор = (X1: 20.0; X2: 26.0; X3: 90.0; X4: 46.0)
  - Выход сети = (y1: 0.0; y2: 0.9; y3: 0.0)
- Входной вектор = (X1: 40.0; X2: 90.0; X3: 91.0; X4: 51.0)
  - Выход сети = (y1: 0.0; y2: 0.9; y3: 0.0)
- Входной вектор = (X1: 6.0; X2: 59.0; X3: 89.0; X4: 82.0)
  - Выход сети = (y1: 0.0; y2: 0.9; y3: 0.0)
- Входной вектор = (X1: 36.0; X2: 85.0; X3: 26.0; X4: 18.0)
  - Выход сети = (y1: 0.0; y2: 0.9; y3: 0.0)
- Входной вектор = (X1: 84.0; X2: 70.0; X3: 74.0; X4: 38.0)
  - Выход сети = (y1: 0.0; y2: 0.0; y3: 0.9)

- Входной вектор = (X1: 82.0; X2: 0.0; X3: 70.0; X4: 85.0)
  - Выход сети = (y1: 0.0; y2: 0.0; y3: 0.9)
- Входной вектор = (X1: 96.0; X2: 34.0; X3: 94.0; X4: 81.0)
  - Выход сети = (y1: 0.0; y2: 0.0; y3: 0.9)
- Входной вектор = (X1: 53.0; X2: 32.0; X3: 98.0; X4: 3.0)
  - Выход сети = (y1: 0.0; y2: 0.9; y3: 0.0)
- Входной вектор = (X1: 80.0; X2: 54.0; X3: 22.0; X4: 28.0)
  - Выход сети = (y1: 0.0; y2: 0.0; y3: 0.9)

На рисунках 9.3 и 9.4 приведен пример применения программы.

## Анализ степени уверенности в атаке

### Время поступления пакетов

Введите показатель среднего времени поступления одного пакета среди отобранных для анализа пакетов.

### Процент различных внешних IP адресов

Введите значение, отображающее процент различных внешних IP адресов среди отобранных для анализа пакетов.

### Процент различных портов

Введите значение, отображающее процент различных портов среди отобранных для анализа пакетов.

### Процент пакетов с поврежденными заголовками

Введите значение, отображающее процент пакетов с поврежденными заголовками среди отобранных для анализа пакетов.

Рисунок 9.3. Пример ввод данных в программу

## Результат анализа

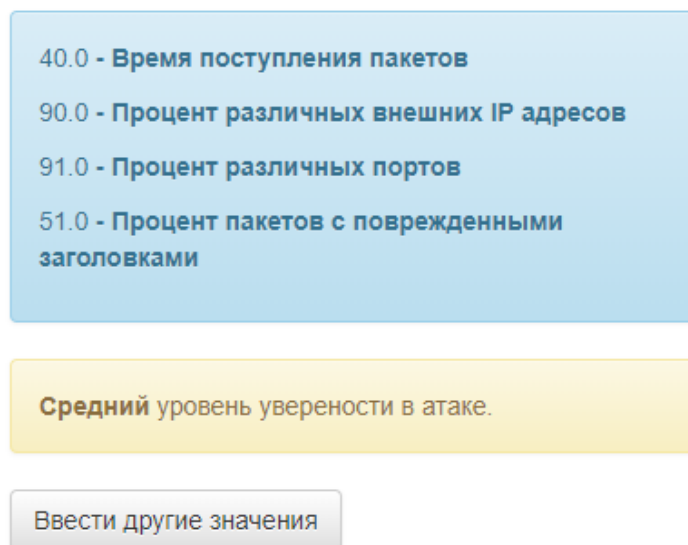


Рисунок 9.4. Пример ответа классификатора

Программная реализация представлена как библиотека на языке Java для подключения к веб-серверу и определения степени угрозы на основе подаваемых статистических данных трафика.

Улучшением данной реализации является разработка программного модуля, который будет перехватывать пакеты, поступающие на сервер, анализировать каждые  $n$  пакетов, составлять статистический вектор, и подавать его на вход уже обученной нейронной сети.

## 10. ЗАДАЧИ ДЛЯ САМОСТОЯТЕЛЬНОГО ИССЛЕДОВАНИЯ

### 1) *Модель распространения информационной угрозы* [14]

Обозначим через  $X_0$ , число людей, которое подвержено воздействию информационной угрозы,  $X(t)$  - количество приверженцев (адептов) в момент времени  $t$ .

Будем считать, что движение информационной угрозы происходит по двум каналам: внешнему и внутреннему. Заметим информацию можно получить как по внешнему, так и по внутреннему каналу. Исходя из этого, можно говорить о том, что скорость внешней вербовки определяется значениями:  $X_0 - X(t)$ , а скорость внутренней вербовки:  $X(t)$ .

$$\frac{dX(t)}{dt} = (a + bX(t))(X_0 - X(t)), \quad X(0) = 0, t > 0.$$

Далее будем рассматривать величины  $a = u_1(t), b = u_2(t)$  – как функции управления, меняющиеся в заданном диапазоне  $|u_i| \leq A_i$ .

Управляемый процесс описывается дифференциальным уравнением

$$\frac{dX(t)}{dt} = (u_1(t) + u_2(t)X(t))(X_0 - X(t)), \quad t \in [0, T].$$

Целью управления является минимизации затрат и привлечения максимального числа адептов. Данная цель формализуется в виде функционала, состоящего из интегрального и терминального слагаемых.

$$J(u) = \int_0^T (M_1 u_1^2 + M_2 u_2^2) dt + M_3 (X_0 - X(T))^2 \rightarrow \min.$$

$M_1, M_2, M_3$  – положительные масштабирующие множители.

### 2) *Математическая модель информационной безопасности на предприятиях малого бизнеса* [15]

Пусть в технической или социально-экономической системе заданы зависимости рисков  $r_i$  отказа работоспособности системы от затрат  $x_i$  на их избежание (исключение, уменьшение) в  $i$ -м направлении обеспечения информационной безопасности (отказ аппаратного, программного

обеспечения, отказ работоспособности системы из-за недостаточной квалификации сотрудников, управленцев и т.п.).

$$r_i = f(x_i), \quad i = 1, \dots, n,$$

где  $n$  – количество указанных направлений.

При минимизации рисков информационной безопасности будем использовать такой показатель, как уровень затрат (в материальном или стоимостном выражении) на восстановление работоспособности системы в случае ее отказа по одному или нескольким направлениям. Определим следующие величины:

$R$  – суммарный риск отказа системы, который определяется по формуле

$$R = \sum_{i=1}^n r_i;$$

$Z$  – максимальная сумма затрат на уменьшение (устранение) выделенных рисков;

$ZMAX_i$  – максимальная сумма затрат на реализацию  $i$ -го направления;

$ZMIN_i$  – минимальная сумма затрат на реализацию  $i$ -го направления, то можно сформулировать следующую задачу математического программирования:

$$R_i \rightarrow \min, \tag{10.1}$$

$$\sum_{i=1}^n x_i \leq Z,$$

$$ZMIN_i \leq x_i \leq ZMAX_i, \quad x_i \geq 0.$$

Пусть  $f(x_i) = a_i - b_i x_i$ , то есть являются линейными функциями от  $x_i$  с отрицательными угловыми коэффициентами. Тогда (10.1) можно записать в виде следующей задачи линейного программирования:

$$\sum_{i=1}^n (b_i x_i - a_i) \rightarrow \max,$$

$$\sum_{i=1}^n x_i \leq Z,$$

$$ZMIN_i \leq x_i \leq ZMAX_i, \quad x_i \geq 0.$$

Коэффициенты  $a_i$  можно трактовать как издержки, которые может понести система в случае отсутствия затрат или, иначе, как максимальные затраты на организацию бескризисной работы системы на  $i$ -м направлении обеспечения безопасности, а коэффициенты  $b_i$  – как весовые коэффициенты, отражающие относительную значимость  $i$ -го направления обеспечения безопасности.

### 3) *Модель атаки и противодействия в распределенной телекоммуникационной системе (РТКС) [16]*

РТКС состоит из нескольких автономных подсетей. Каждый компьютер РИВС может взаимодействовать в любой момент времени с любым другим (и произвольным количеством компьютеров вне РТКС, например в Интернете).

Пусть жертвы – уязвимые компьютеры – узлы РТКС, их количество  $y_1(t)$ , хищники – пораженные компьютеры (узлы), они осуществляют информационные преднамеренные воздействия – атаки, количество таких компьютеров  $y_2(t)$ . С течением времени в отсутствии атак поврежденная система восстанавливается, коэффициент  $a$  будет выражать скорость прироста уязвимых компьютеров. В случае отсутствия уязвимых компьютеров (т.е. РТКС неуязвима для атаки) число атакующих компьютеров уменьшается, параметр  $c$  выражает скорость такого уменьшения. Параметр  $d$  будет отражать влияние на скорость прироста атакующих компьютеров числа уязвимых компьютеров (назовем данный параметр «коэффициентом уязвимости»).  $\mu$  – доля уязвимых компьютеров, которые были успешно атакованы за время  $t$ , тогда  $(N \mu)$  представляет собой общее количество успешно атакованных компьютеров, каждый из которых будет использован для проведения последующих атак.



Введем параметр  $p_j$  – вероятность того, что захваченный компьютер в подсети, состоящей из  $N_j$  компьютеров, будет атаковать компьютеры в этой же подсети, тогда  $(1 - p_j)$  – вероятность того, что атакуемый компьютер будет находиться вне этой подсети.

Пусть РТКС содержит  $N$  (потенциально уязвимых к атакам) компьютеров (узлов). Поскольку система информационной защиты «срабатывает» не сразу, т.е. с момента начала атаки проходит некоторое время, введем дополнительный параметр  $\lambda$ , который будет выражать задержку в срабатывании системы безопасности. Тогда конечная система уравнений будет иметь вид

$$\begin{aligned}\frac{dy_1(t)}{dt} &= (a - (s_j \mu p_j + (1 - p_j)(1 - s_j) \mu (1 - \mu) y_2(t))) y_1(t) - \lambda y_1^2(t), \\ \frac{dy_2(t)}{dt} &= (d y_1(t) - c) y_2(t) - \lambda y_2^2(t).\end{aligned}$$

Здесь  $s_j = N_j / N$ .

#### 4) *SAIR-модель («Susceptible–Antidotal–Infected–Removed model»)* [4]

Эта модель предусматривает случай развития эпидемии в сети с установленным антивирусом. Все моделируемые хосты в сети делятся на 4 группы: неинфицированные хосты, восприимчивые к заражению (S); неинфицированные хосты с установленным антивирусом (A); инфицированные хосты (I); вылеченные и восстановленные узлы (R).

Динамика модели описывается следующими дифференциальными уравнениями

$$\begin{aligned}\frac{dS}{dt} &= N - \alpha \cdot S \cdot A - \beta_{SI} S \cdot I - \mu \cdot S + \sigma_{IS} \cdot I + \sigma_{RS} \cdot R, \\ \frac{dI}{dt} &= \beta_{SI} \cdot S \cdot I + \beta_{AI} \cdot A \cdot I - \sigma_{IS} \cdot I - \delta \cdot I - \mu \cdot I, \\ \frac{dR}{dt} &= \delta I - \sigma_{RS} R - \mu R, \\ \frac{dA}{dt} &= \alpha SA - \mu A - \beta_{AI} AI.\end{aligned}$$

В формализации модели используются обозначения:  $N$  – частота добавления новых хостов в сети;  $\mu$  – частота «смерти» хостов не из-за вируса;  $\beta_{SI}$  – частота заражения уязвимых хостов;  $\beta_{AI}$  – частота заражения новым червем хостов с установленным антивирусом;  $\delta$  – частота удаления зараженных хостов;  $\sigma_{IS}$  – частота восстановления зараженных хостов;  $\alpha$  – преобразование уязвимого хоста в неуязвимый путем установки на нем антивирусного программного обеспечения.

Целью является минимизация нанесенного ущерба компьютерной эпидемией. Потери учитываются с помощью функционала, который характеризуется количеством инфицированных узлов в течение всего рассматриваемого промежутка времени  $[0, T]$

$$J(t) = \int_0^T I(t) dt.$$

#### **5) Модель влияния кибератак на функционирование конкурирующих фирм [17]**

На некотором рынке товаров и услуг функционируют две конкурирующие фирмы, каждая из которых с помощью специальных программно-технических средств атакует компьютерные сети конкурента, и одновременно проводит мероприятия по обеспечению собственной информационной безопасности. Эффект от проведения кибератак проявляется в снижении экономического потенциала конкурента и в сужении емкости рынка, где он может реализовывать товары или оказывать услуги. При этом эффективность или действенность самих кибератак будем характеризовать двумя величинами:  $q_i$  ( $i=1,2$ ) – вероятностью того, что кибератаки сторон, направленные на снижение экономического потенциала конкурента, достигнут целей;  $p_i$  ( $i=1,2$ ) – вероятностью того, что кибератаки сторон, направленные на сужение емкости рынка конкурента, достигнут целей. В качестве интегрального показателя, характеризующего экономическую эффективность

конкурирующих фирм, будем использовать объемы реализованных ими товаров или оказанных услуг  $E_i$  ( $i=1,2$ ) за определенный период времени (сутки, неделя, месяц и др.) с размерностью шт./ед. времени или руб./ед. времени.

Введем следующие обозначения:  $r_i$  – экономический потенциал  $i$ -й фирмы, характеризующий удельную скорость роста объема реализуемых товаров и оказываемых услуг при отсутствии конкурента, с размерностью 1/ед. времени;  $K_i$  – емкость рынка для  $i$ -й фирмы, характеризующая наибольший объем потребляемых рынком товаров и услуг данной фирмы за период времени  $\Delta T$ , с размерностью шт./ед. времени или руб./ед. времени;  $t$  – текущее время;  $t_0$  – начальный момент времени;  $E_i^0$  – начальная экономическая эффективность  $i$ -й фирмы в момент времени  $t = t_0$ .

Будем предполагать, что взаимное влияние конкурентов на эффективность функционирования друг друга характеризуется линейной функцией, то есть с ростом экономической эффективности одного конкурента происходит пропорциональное снижение экономической эффективности другого конкурента. При этом пропорциональность задается безразмерными коэффициентами  $0 < \alpha_{12} \leq 1$  и  $0 < \alpha_{21} \leq 1$ , выражающие меру относительного влияния конкурирующих субъектов друг на друга. С учетом сделанных допущений математическая модель функционирования конкурирующих фирм в условиях взаимных кибератак может быть записана в виде системы дифференциальных уравнений следующего вида:

$$\begin{aligned}\frac{dE_1(t)}{dt} &= E_1(t) \left( \left( r_1 - \frac{r_1 E_1(t)}{K_1 - p_2 E_2(t)} \right) (1 - q_2) - \alpha_{12} q_2 \frac{r_1 E_2(t)}{K_2 - (1 - p_2) E_2(t)} \right), \\ \frac{dE_2(t)}{dt} &= E_2(t) \left( \left( r_2 - \frac{r_2 E_2(t)}{K_2 - p_1 E_1(t)} \right) (1 - q_1) - \alpha_{21} q_1 \frac{r_2 E_1(t)}{K_1 - (1 - p_1) E_1(t)} \right), \\ E_i(t_0) &= E_i^0, i=1,2.\end{aligned}$$

Задача будет состоять в том, чтобы установить и выразить в количественной форме зависимость динамики изменения экономической эффективности конкурирующих фирм в условиях ведения ими взаимных кибератак и определить условия устойчивости такой конкуренции, когда, несмотря на взаимные кибератаки, конкуренты, хотя и теряют в эффективности, но не претерпевают банкротства  $E_i > 0$  ( $i=1,2$ ).

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Поповский В.В., Лемешко А.В., Евсеева О.Ю. Динамическое управление ресурсами ТКС: математические модели в пространстве состояний // Наукові записки УНДІЗ. – 2009. – №1(9). – С. 3–26.
2. Лемешко, А. В. Динамическое представление тензорной модели многопутевой QoS-маршрутизации в нестационарном режиме работы сетевых интерфейсов / А. В. Лемешко, А. С. Еременко // Проблеми телекомунікацій. – 2016. – № 1 (18). – С. 3–21. – Режим доступа: [http://pt.journal.kh.ua/2016/1/1/161\\_lemeshko\\_dynamic.pdf](http://pt.journal.kh.ua/2016/1/1/161_lemeshko_dynamic.pdf)
3. Бабанин Д. В. Модели оценки структурных решений по защите компьютерных сетей от вирусных атак. Москва – 2012. – Режим доступа: <http://miem.edu.ru/uploads/dissertation/referat/93cec9da4a4eb6bd8f9faf5917245131251b06c5.pdf>
4. Котенко И. В., Воронцов В. В. Аналитические модели распространения сетевых червей /И. В. Котенко, В. В. Воронцов// Труды СПИИРАН. Вып. 4. — СПб.: Наука, 2007. С. 208 – 224.
5. Шушков Г. М. Концептуальные основы информационной безопасности Российской Федерации /Г. М. Шушков, И. В. Сергеев// Актуальные вопросы научной и научно-педагогической деятельности молодых учёных: сб. науч. трудов III всеросс. заочн. науч.-практ. конф. М.: ИИУ МГОУ, 2016. С. 69-76.
6. Форрестер Д. Основы кибернетики предприятия (индустриальная динамика). М.: Прогресс, 1971. 340 с.
7. Модель информационного противоборства в социуме при периодическом дестабилизирующем воздействии / Михайлов А. П., Петров А. П., Прончева О. Г., Маревцева Н. А. // Математическое моделирование, 2017. Т. 29. № 2. С. 23-32.

8. Львович Я.Е., Чернышева Г.Д., Каширина И.Л. Оптимизация проектных решений в САПР на основе эквивалентных преобразований задачи о минимальном покрытии. Электронное научно-техническое издание № ФС 77-30569. Государственная регистрация № 0421100025 . – Режим доступа: <http://technomag.edu.ru/index.html>.

9. Кацупеев, А.А. Постановка и формализация задачи формирования информационной защиты распределённых систем/ А.А. Кацупеев, Е.А. Щербакова, С.П. Воробьёв //Инженерный вестник Дона, №1, ч.2 (2015) – Режим доступа: <http://technomag.edu.ru/index.html>. [ivdon.ru/ru/magazine/archive/n1y2015/2868](http://ivdon.ru/ru/magazine/archive/n1y2015/2868).

10. Государственный реестр сертифицированных средств защиты информации. – Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>

11. Михайлов А. П. , Петров А. П. , Калиниченко М. И. , Поляков С. В., Моделирование одновременного распространения легальных и контрафактных копий инновационных продуктов, Математическое моделирование, 2013, том 25, номер 6, с. 54– 63

12. А. П. Михайлов, Н. А. Маревцева, Модели информационной борьбы/ А. П. Михайлов, Н. А. Маревцева // Математическое моделирование. – 2011. – том 23. –№10. – с19–32.

13. Слеповичев И. И., Ирматов П. В., Комарова М. С., Бежин А. А., Обнаружение DDoS атак нечеткой нейронной сетью, Изв. Саратов. ун-та. Нов. сер. Сер. Математика. Механика. Информатика, 2009, том 9, выпуск 3, 84 – 89.

14. Н. А. Маревцева. Простейшие математические модели информационного противоборства. Математическое моделирование социальных процессов, вып.11. – М.: МАКС Пресс, 2010, с.59-72.

15. Иванченко П.Ю., Кацура Д.А., Медведев А.В., Трусов А.Н. Математическое моделирование информационной и экономической безопасности на предприятиях малого и среднего бизнеса // Фундаментальные исследования. – 2013. – № 10-13. – С. 2860-2863. – Режим доступа: <http://fundamental-research.ru/ru/article/view?id=32923> .

16. Теоретическое и экспериментальное исследование распределенных телекоммуникационных систем в условиях воздействия вредоносных программ: монография / Ю. М. Монахов, Л. М. Груздева; ФГБОУ ВПО "Владимирский гос. ун-т им. Александра Григорьевича и Николая Григорьевича Столетовых". - Владимир : ВлГУ, 2013. - 131 с.

17. Новосельцев, В.И. Модель влияния кибератак на функционирование конкурирующих фирм /В.И. Новосельцев, А.Н. Ноев, Д.Е. Орлова// Моделирование, оптимизация и информационные технологии. 2017, №4(19). – Режим доступа: <http://moit.vivt.ru/>

Отпечатано с авторских оригиналов.

Подписано в печать 5.10.2020. Формат 60х84 1/16.

Усл. печ. л. 7,4. Тираж 300 экз. Заказ № 193.

Редакционно-издательское управление

Тверского государственного университета

Адрес: Россия, 170100, г. Тверь, Студенческий пер., д. 12, кор. Б.

Тел. РИУ: (4822) 35-60-63.