

# Тема дипломной работы:

## Разработка датчика оценки деструктивных воздействий оператора в РВС по видеoinформации

Дипломник: студент гр. ИУ10-121 Князев Б.А.

Научный руководитель: д.т.н. Климов С.М.

**Цель исследования:** Повышение устойчивости функционирования КВИС в условиях деструктивных воздействий оператора.

**Задача исследования:** Разработка методики и алгоритмов оценки функционального состояния оператора КВИС на основе оперативного выявления признаков деструктивных воздействий оператора.

Достижение максимума обобщенного показателя эффективности противодействия ДВО, обеспечивающего устойчивость функционирования КВИС:

$$P_{\text{ОБН ДВО}} = \underset{M_{\text{ДВО}}^{\text{ДОП}} \in M_{\text{ДВО}}, Z_{\text{ДВО}}^{\text{ДОП}} \in Z_{\text{ДВО}}}{\text{arg max}} P_{\text{ОБН}}[(M_{\text{ДВО}}^{\text{ДОП}}, Z_{\text{ДВО}}^{\text{ДОП}})] | \varphi \quad (1.1)$$

Ограничения на параметры, от которых зависит критерий эффективности обнаружения ДВО:

$$\varphi = \begin{cases} T_{\text{Н}} \leq T_{\text{ОБН}} \leq T_{\text{К}}, \\ \forall S_i \in S (\exists Q_j \in Q, Y_k \in Y : \{S_i, Q_j, Y_k\} \in S_p), \\ C_{\text{ДВО}} \leq C_{\text{ЗД}}, \\ 0.1 \leq \varepsilon_{\text{ОШ}} \leq 0.2 \end{cases} \quad (1.2)$$

**Деструктивное воздействие оператора (ДВО)** – действие или бездействие оператора АРМ, приводящее к нарушению или снижению эффективности выполнения технологических циклов управления (ТЦУ) КВИС и нанесению ему ущерба.

**Таблица 1.1 – Источники атак**

Источник атак (название)	Источник атак, %
<b>Недобросовестные сотрудники</b>	<b>81</b>
<b>Хакеры</b>	<b>77</b>
Конкуренты	44
Зарубежные компании	26
Зарубежные правительства	21

**Таблица 1.2 – Частота обнаружения атак**

Тип атаки	Частота обнаружения, %
<b>Вирусы</b>	<b>85</b>
<b>Злоупотребления в Internet со стороны сотрудников</b>	<b>79</b>
<b>Несанкционированный доступ со стороны сотрудников</b>	<b>71</b>
Отказ в обслуживании	27
Атаки внешних злоумышленников	25
Кража конфиденциальной информации	20

Источник: CSI/FBI Computer Crime and Security Survey, 2000

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеoinформации				
Изм.	Лист	Документ №	Подпись	Дата	Цель и задачи дипломной работы	Литер.	Масса	Масшт.
Разраб.		Князев Б.А.				Лист 1	Листов 11	
Провер.		Климов С.М.						
Т.контр.								
Принят.								
Н.Конт.								
Утв.		Климов С.М.						
						МГТУ им. Н.Э. Баумана Группа ИУ10-121		



# Методическая схема исследования методов и моделей противодействия деструктивным воздействиям оператора

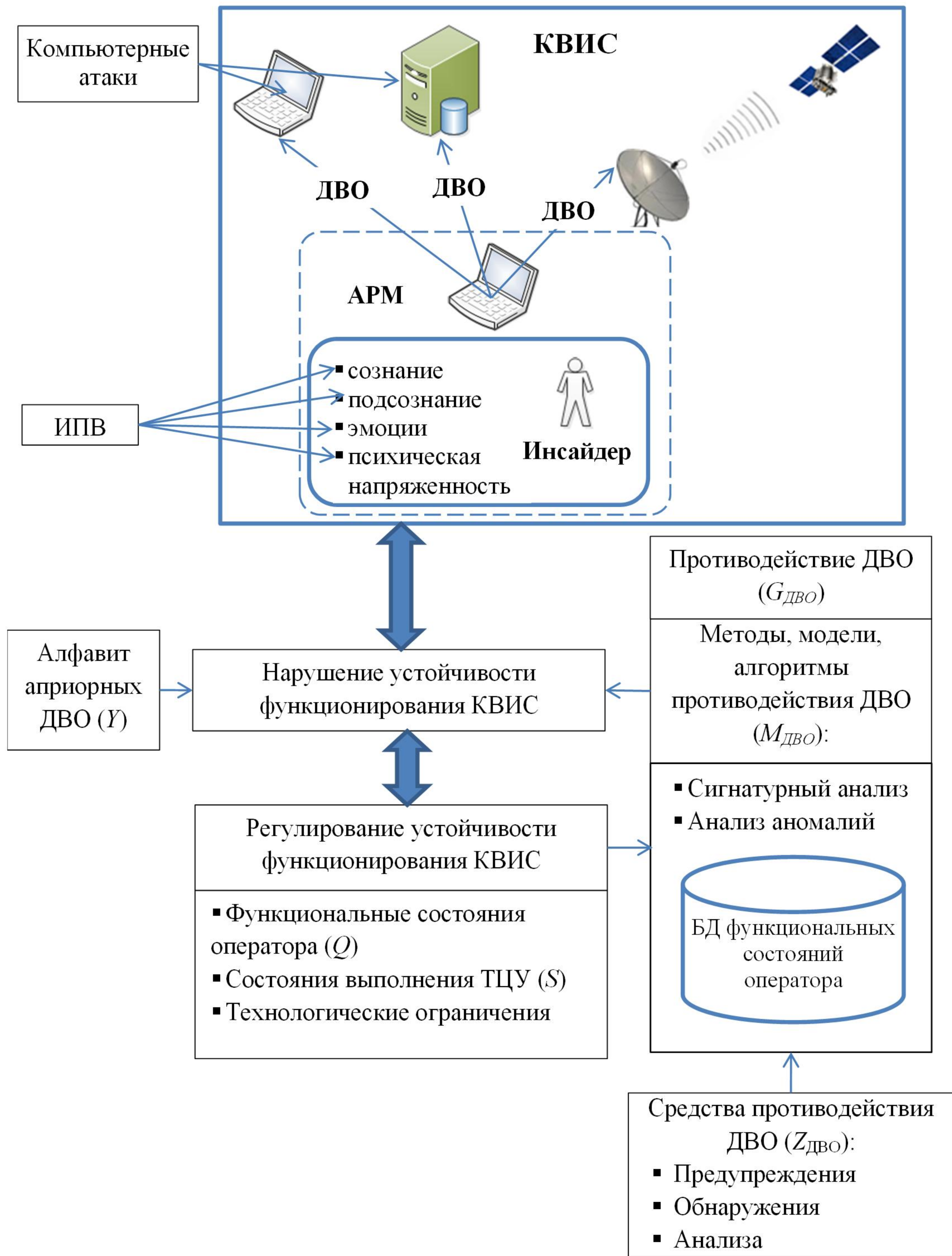


Рисунок 2.1 – Обобщенная схема подхода к разработке методов и моделей противодействия ДВО

Дипломная работа					Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации		
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
Разраб.		Князев Б.А.					
Провер.		Климов С.М.					
Т.эксперт.							
Принят.							
Н.Конт.							
Утв.		Климов С.М.					

Методическая схема исследования методов и моделей противодействия ДВО		Лист 2	Листов 11
МГТУ им. Н.Э. Баумана Группа ИУ10-121			



# Модель внутренних угроз



Таблица 3.1 – Полномочия операторов и минимально необходимые для реализации ДВО средства

Полномочия	Классы ДВО			
	Y <sub>1</sub>	Y <sub>2</sub>	Y <sub>3</sub>	Y <sub>4</sub>
Оператор (R <sub>1</sub> )	штатные (W <sub>1</sub> )	средства из Интернет, специальные средства (W <sub>2</sub> )	криминалистические (W <sub>3</sub> )	террористические (W <sub>4</sub> )
привилегированный оператор (R <sub>2</sub> )	штатные (W <sub>1</sub> )	штатные (W <sub>1</sub> )	средства из Интернет, специальные средства (W <sub>2</sub> )	криминалистические (W <sub>3</sub> )
оператор-администратор (R <sub>3</sub> )	штатные (W <sub>1</sub> )	штатные (W <sub>1</sub> )	штатные (W <sub>1</sub> )	средства из Интернет, специальные средства (W <sub>2</sub> )

Таблица 3.2 – Классификация ДВО по признакам

Признаки		Классы ДВО											
Элементы алфавита y	Название	1			2			3			4		
		Полномочия			Полномочия			Полномочия			Полномочия		
		R <sub>1</sub>	R <sub>2</sub>	R <sub>3</sub>	R <sub>1</sub>	R <sub>2</sub>	R <sub>3</sub>	R <sub>1</sub>	R <sub>2</sub>	R <sub>3</sub>	R <sub>1</sub>	R <sub>2</sub>	R <sub>3</sub>
y <sub>1</sub>	гнев	0.3	0.3	0.3	0.5	0.3	0.3	0.8	0.5	0.3	0.95	0.8	0.5
y <sub>2</sub>	отвращение	0.4	0.4	0.4	0.6	0.4	0.4	0.9	0.6	0.4	0.99	0.9	0.6
y <sub>3</sub>	страх	0.3	0.3	0.3	0.8	0.3	0.3	0.7	0.8	0.3	0.5	0.7	0.8
y <sub>4</sub>	счастье	0.8	0.8	0.8	0.5	0.8	0.8	1	0.5	0.8	1	1	0.5
y <sub>5</sub>	печаль	0.8	0.8	0.8	0.9	0.8	0.8	0.95	0.9	0.8	0.99	0.95	0.9
y <sub>6</sub>	удивление	0.5	0.5	0.5	0.5	0.5	0.5	1	0.5	0.5	1	1	0.5
y <sub>7</sub>	уровень напряженности	0.5	0.5	0.5	0.7	0.5	0.5	0.8	0.7	0.5	0.95	0.8	0.7

y – множество признаков деструктивных воздействий оператора

Множество разрешенных состояний КВИС:  $Q \times S \times Y \mapsto S_p$  (3.1)

Множество деструктивных воздействий оператора:  $D \subset Q \times S \times Y: \forall (d_i \in D, Q_m \in Q, S_n \in S, Y_k \in Y) \exists y_j \in y:$  (3.2)

$$(f(y_j) > y_{\text{пор } j}) \wedge (S_p^{(i)} = \{Q_m, S_n, Y_k\} \notin S_p)$$

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации			
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
Разраб.		Князов Б.А.			3		
Провер.		Климов С.М.					
Т.контр.							
Принят.							
Н.Контр.							
Утв.		Климов С.М.					

Модель внутренних угроз

Лист 3 Листов 11

МГТУ им. Н.Э. Баумана  
Группа ИУ10-121



# Алгоритм распознавания биометрических признаков ДВО

## Характеристики нейросетей

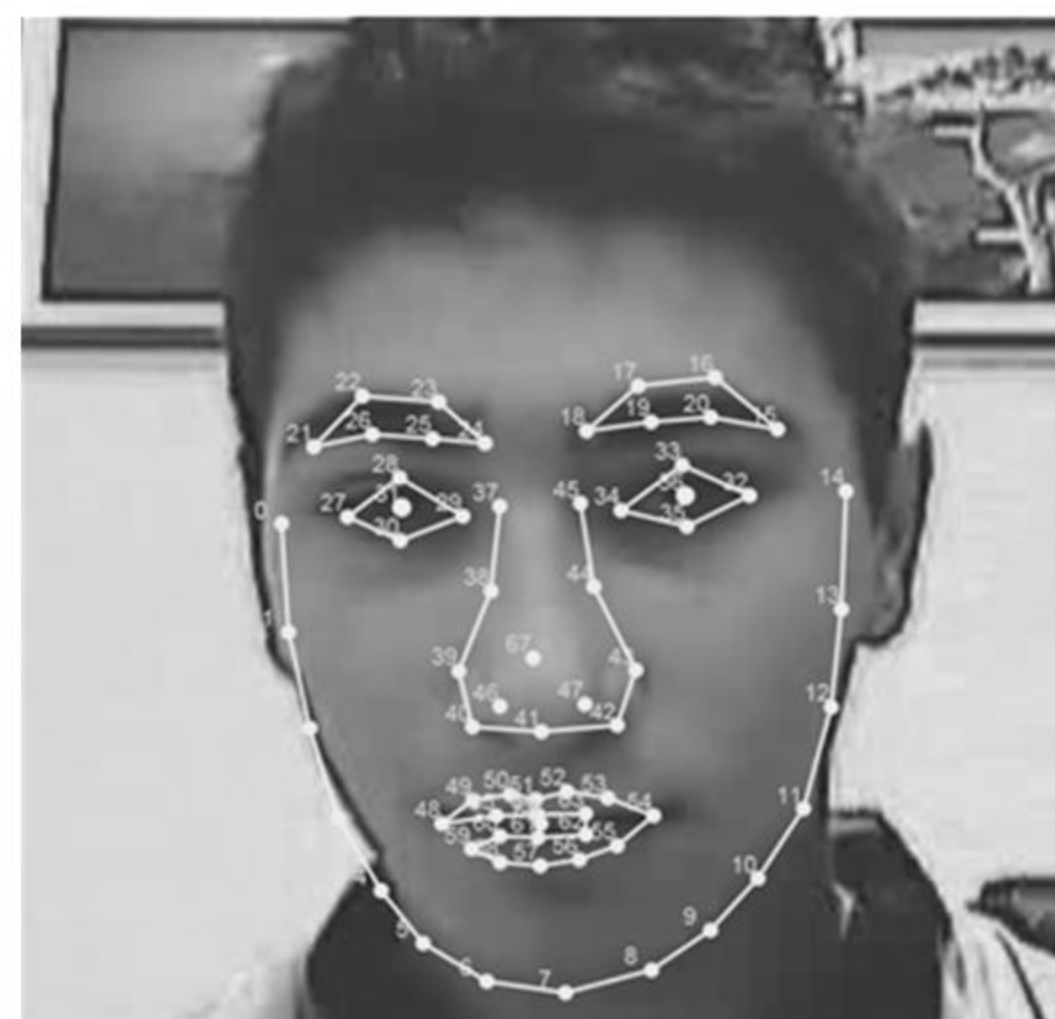
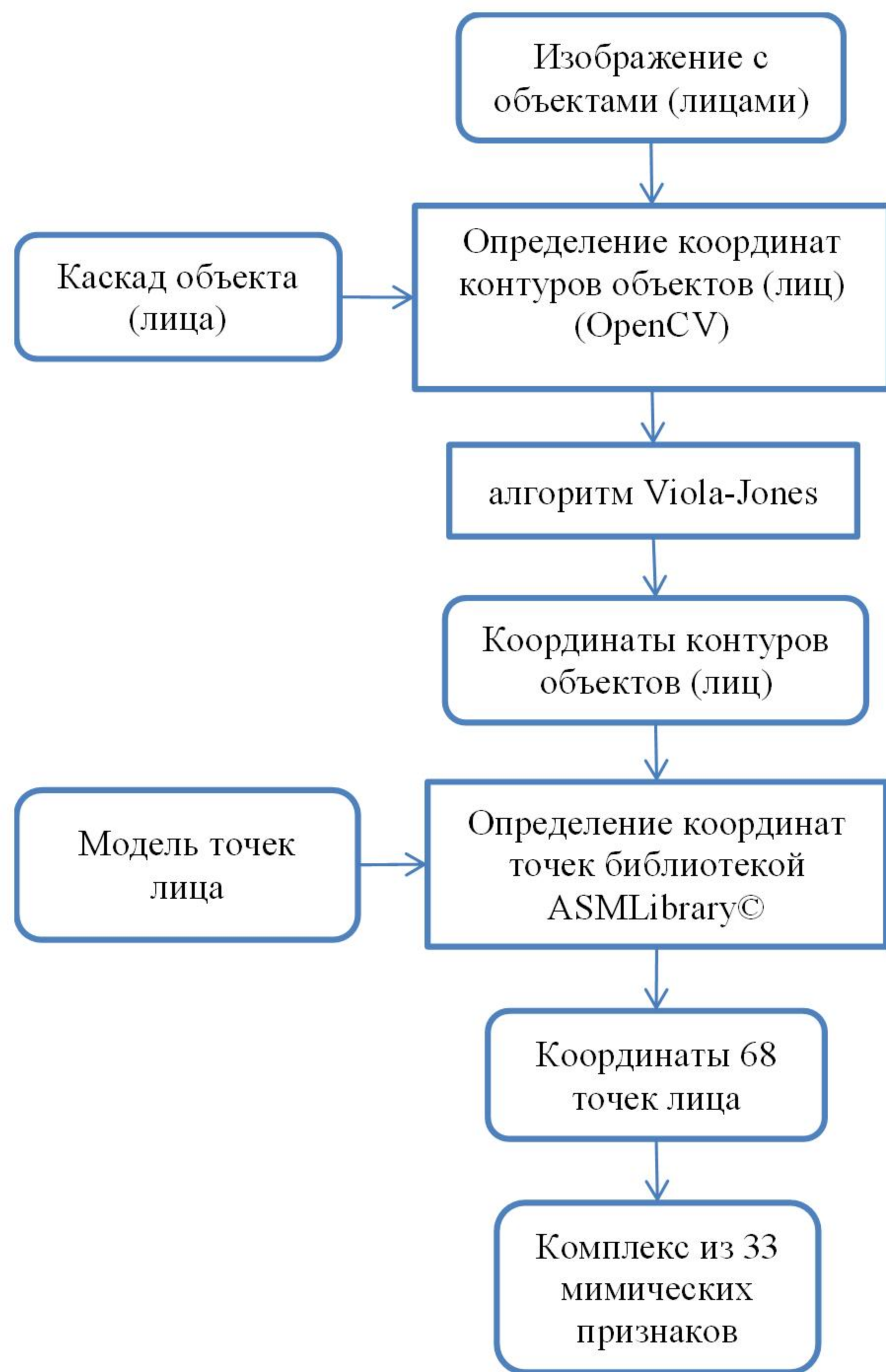


Рисунок 4.2 – Пример автоматически расставленных антропометрических точек лица с помощью библиотеки ASMLibrary©

Таблица 4.1 – Характеристики ANN, классифицирующей эмоциональные признаки ДВО

Признак-эмоция (y <sub>i</sub> )	P <sub>y<sub>i</sub></sub>	P* <sub>y<sub>i</sub></sub>
y <sub>1</sub> Гнев	0.20	0.45
y <sub>2</sub> Отвращение	0.52	0.56
y <sub>3</sub> Страх	0.17	0.31
y <sub>4</sub> Счастье	0.70	0.67
y <sub>5</sub> Печаль	0.35	0.49
y <sub>6</sub> Удивление	0.76	0.82
<b>Среднее значение</b>	<b>0.51</b>	<b>0.60</b>

Таблица 4.2 – Характеристики ANN, классифицирующей признаки-напряженности ДВО

Признак-напряженность (y <sub>напр i</sub> )	P <sub>y<sub>i</sub></sub>	P* <sub>y<sub>i</sub></sub>	
y <sub>7</sub>	У <sub>напр1</sub> Слабая	0.79	0.87
	У <sub>напр2</sub> Умеренная	0.83	0.91
	У <sub>напр3</sub> Чрезмерная	0.85	0.92
<b>Среднее значение</b>	<b>0.83</b>	<b>0.90</b>	

Рисунок 4.1 – Алгоритм вычисления комплекса мимических признаков с помощью библиотеки ASMLibrary©

Обобщенный показатель уровня напряженности (7ой признак ДВО):

$$y_7 = \frac{y_{напр 2}}{2} + y_{напр 3} \tag{4.1}$$

Соотношение для нейронов выходного слоя:

$$y_k = f_{act out} \left( \sum_{i=1}^N w_{out ki} \cdot f_{act} \left( \sum_{j=1}^M w_{ij} \cdot x_j + b_i \right) + b_k \right), k \in \overline{1, K} \tag{4.2}$$

Таблица 4.3 – Характеристики ANN

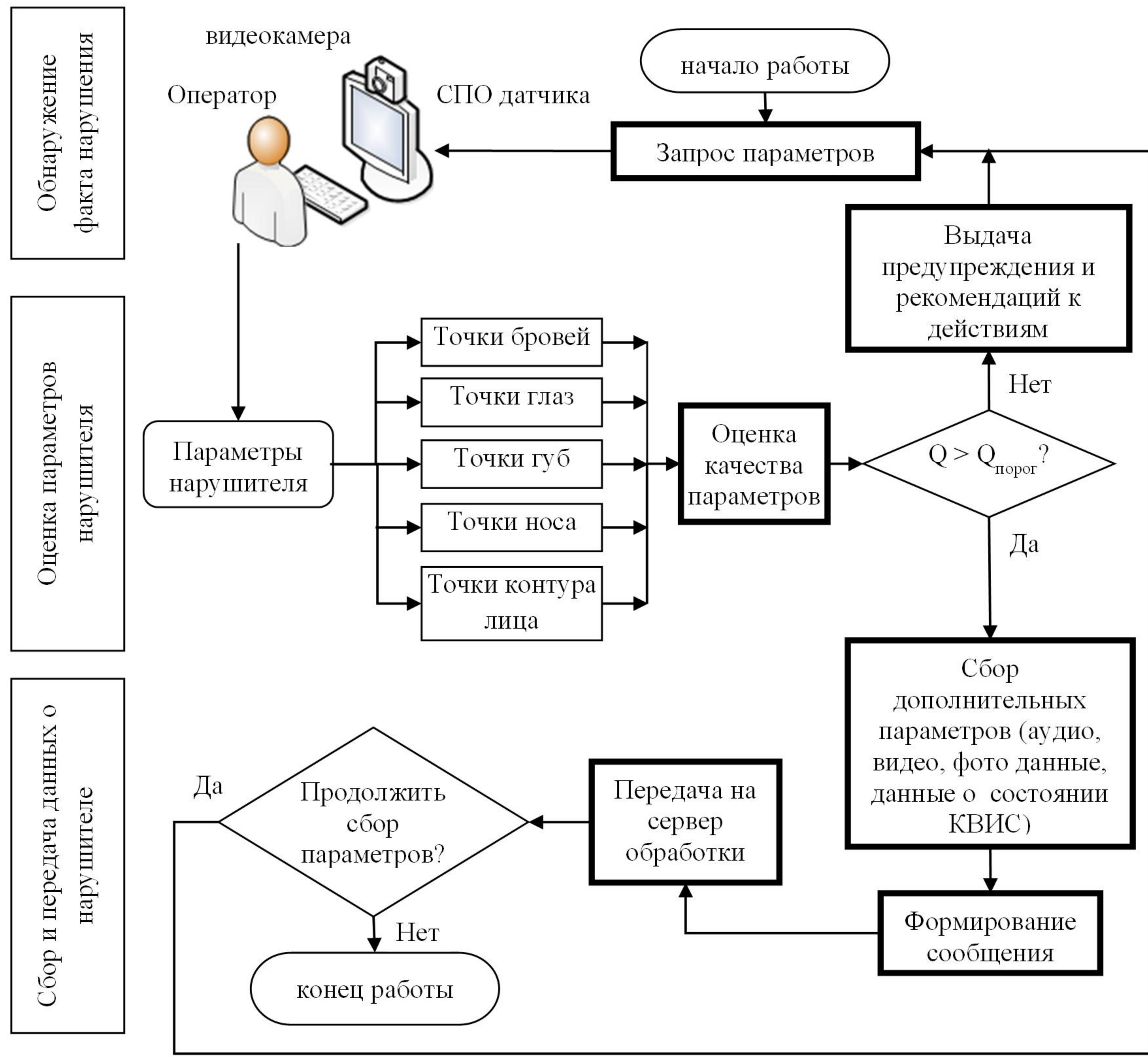
ANN	M	N	K	f <sub>act</sub>	f <sub>act out</sub>
эмоции	33	99	7	tanh	softmax
напряженность	33	58	3	logistic	softmax



Дипломная работа					Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации		
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
					Модель распознавания биометрических признаков ДВО Лист 4 Листов 11 МГТУ им. Н.Э. Баумана Группа ИУ10-121		
Разраб.		Князева Е.А.					
Провер.		Климов С.М.					
Т.эксперт.							
Принят.							
Н.Конт.							
Утв.		Климов С.М.					



# Схема методики организации процесса обнаружения ДВО с помощью биометрического датчика



Обнаружение факта нарушения

Оценка параметров нарушителя

Сбор и передача данных о нарушителе

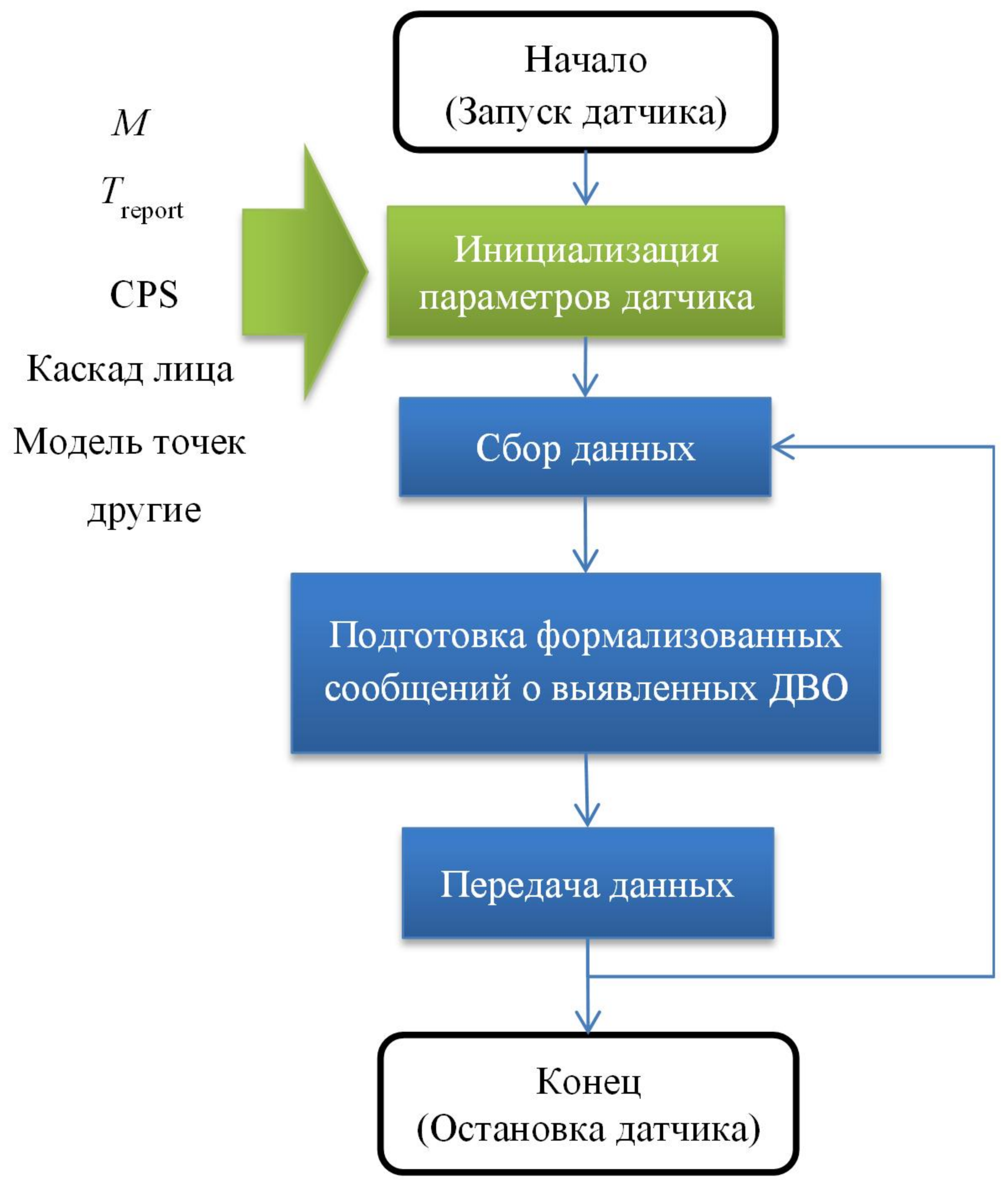
Рисунок 5.1 – Методическая схема организации процесса обнаружения ДВО с помощью биометрического датчика

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации			
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
		Разраб.	Князов Б.А.				
		Провер.	Климов С.М.				
		Т.контр.					
		Принят.					
		Н.Конт.					
		Утв.	Климов С.М.				

Лист 5 Листов 11  
МГТУ им. Н.Э. Баумана  
Группа ИУ10-121



# Обобщенный алгоритм работы биометрического датчика ДВО



### Параметры запуска датчика :

- $M$  – режим работы (анализ видео файла, анализ видео с камеры в реальном масштабе времени),
- CPS (Calculations per second) – максимальная частота вычисления биометрических параметров в секунду.
- $T_{report}$  – период (частота) отправления отчета, эквивалентен периоду вычисления усредненных биометрических параметров.
- Каскад лица
- Модель точек лица

Рисунок 6.1 – Обобщенный алгоритм работы биометрического датчика ДВО

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации				
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.	
Разраб.		Князев Б.А.						
Провер.		Климов С.М.						
Т.контр.								
Принят.								
Н.Контр.								
Утв.		Климов С.М.						
Обобщенный алгоритм работы биометрического датчика ДВО					Лист	6	Листов	11
					МИГУ им. Н.Э. Баумана			Группа ИУ10-121



# Алгоритмы сбора данных и подготовки формализованных сообщений о выявленных ДВО по видеоинформации

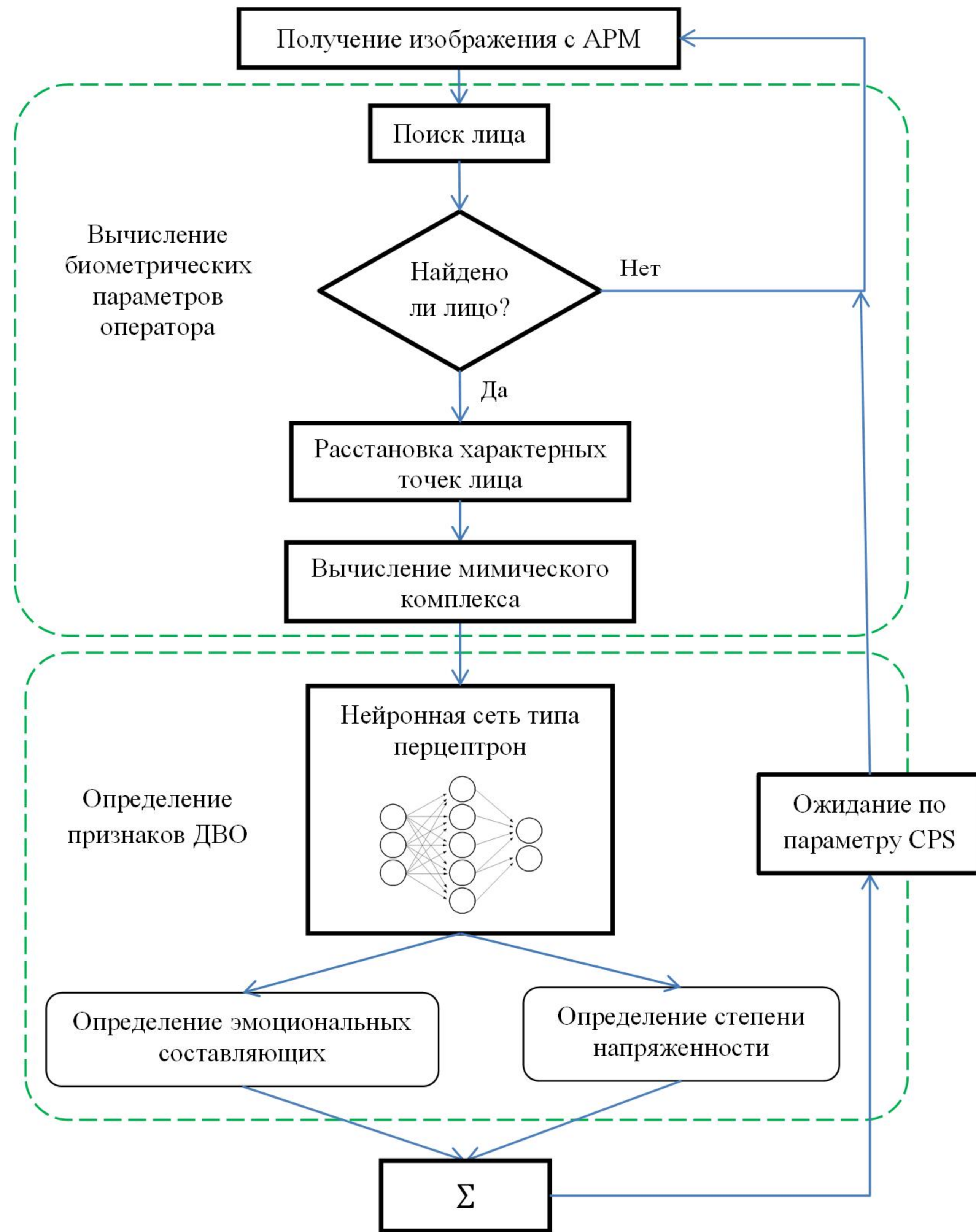


Рисунок 7.1 – Алгоритм сбора данных



Рисунок 7.2 – Алгоритм подготовки формализованных сообщений о выявленных ДВО

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации			
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
		Разраб.	Князев Б.А.				
		Провер.	Климов С.М.				
		Т.контр.					
		Принят.					
		Н.Контр.					
		Утв.	Климов С.М.				

Алгоритмы сбора данных и подготовки формализованных сообщений о выявленных ДВО по видеоинформации

Лист 7 Листов 11

МГТУ им. Н.Э. Баумана  
Группа ИУ10-121



# Результаты оценки эффективности применения разработанного датчика

Практическое представление по решению системы обнаружения вторжений с биометрическим датчиком

НИР «Представление»

Нормативная база «Кальций»

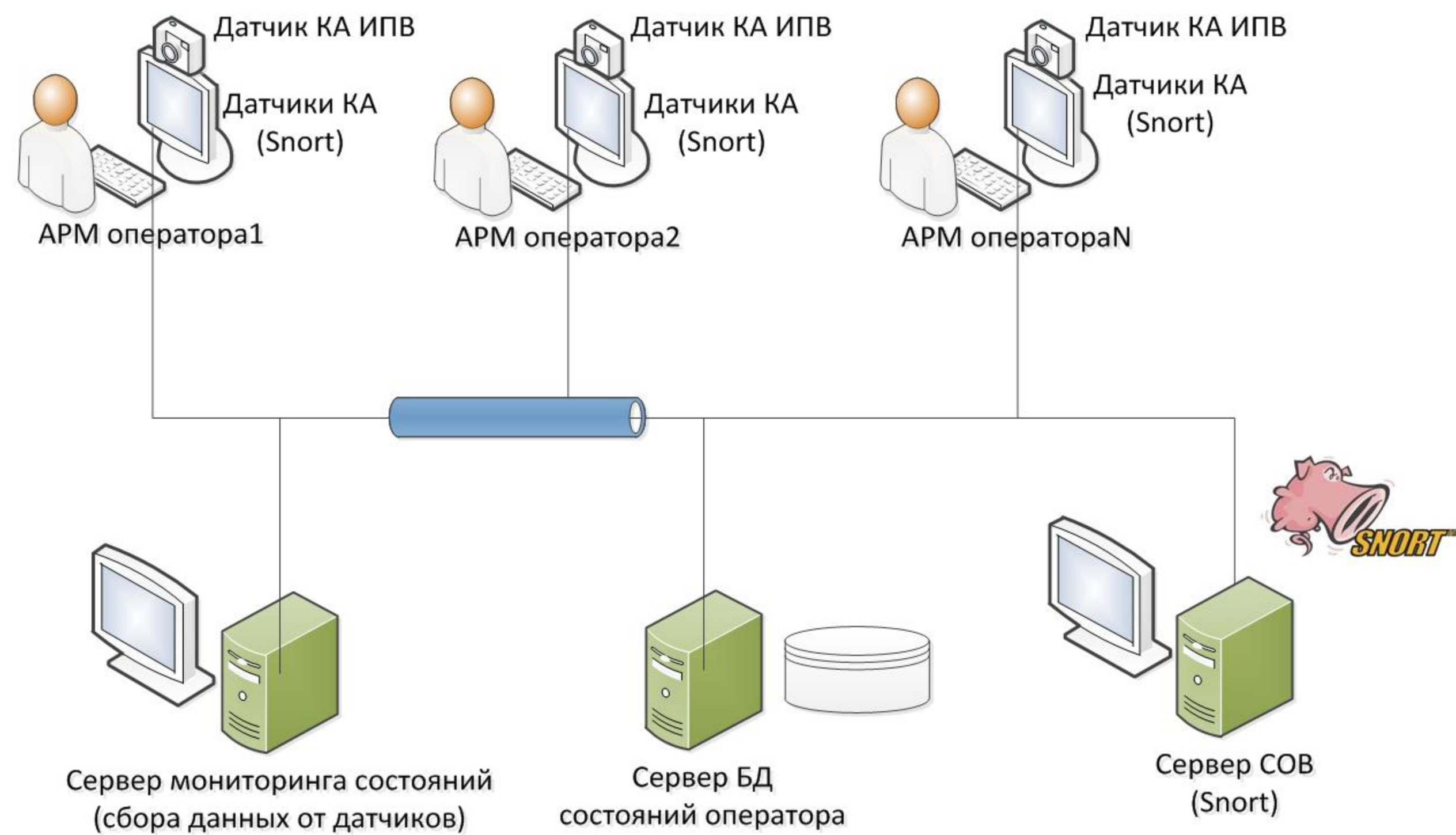


Рисунок 8.1 – Типовой стенд исследования вопроса противодействия ДВО

Оценка возможностей распознавания деструктивных воздействий оператора в РВС

Вероятность успешного противодействия ДВО

$$P_{\text{ПД ДВО}} = \max_{y_i \in Y} P_{y_i} = P_{y_7} = 0.83 \quad (8.1)$$

Вероятность верного обнаружения класса ДВО

$$P_{\text{ОБН}} = P_{\text{ОБН } Y_1} = P_{\text{ОБН } Y_2} = P_{\text{ОБН } Y_3} = P_{\text{ОБН } Y_4} = \begin{cases} 0.83, & y_7 \geq 0.7 \\ 0.42, & y_7 < 0.7 \end{cases} \quad (8.2)$$

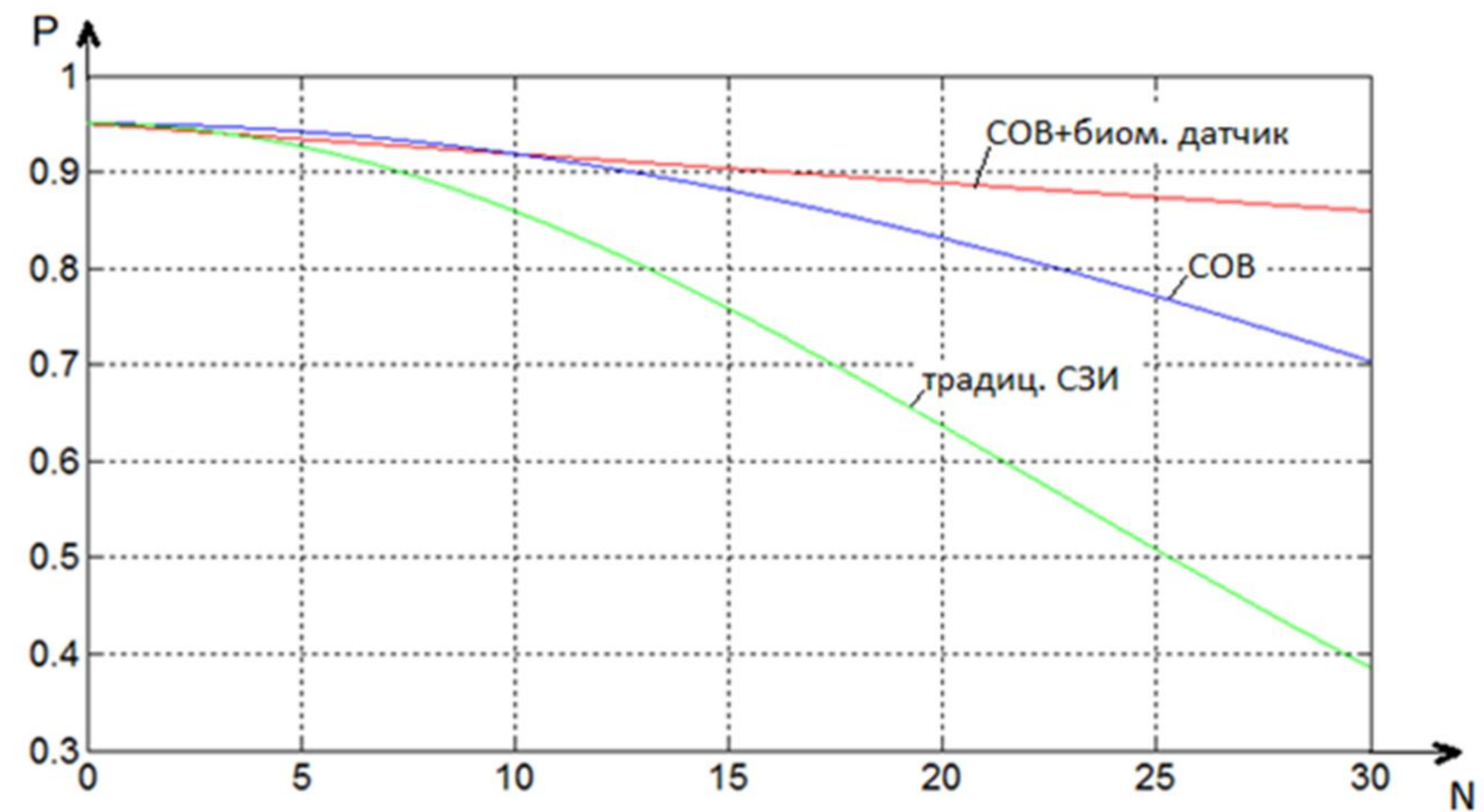


Рисунок 8.3 – Зависимость вероятности предупреждения ДВО от количества атак

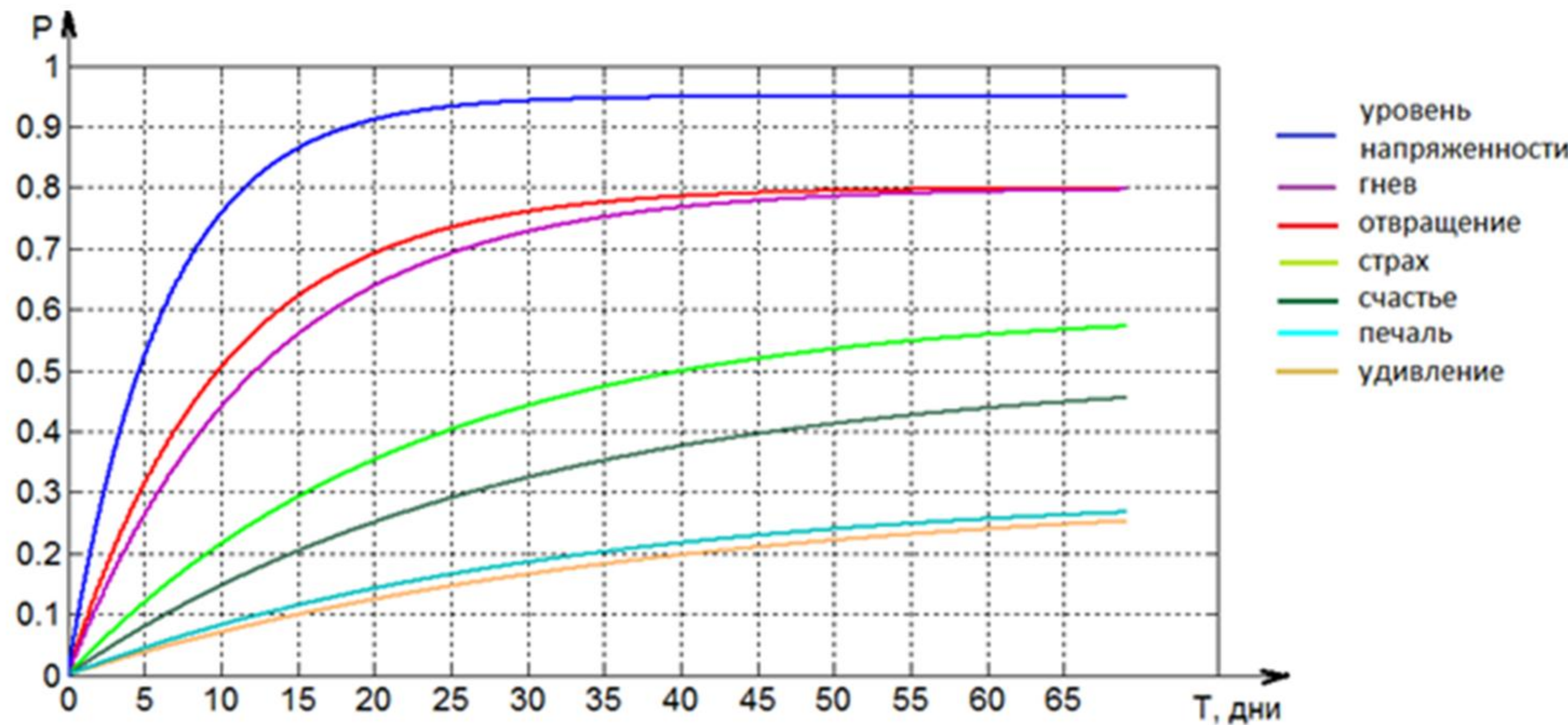


Рисунок 8.2 – Зависимость вероятности предупреждения ДВО по признакам от времени выполнения ТЦУ

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации			
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
		Разраб.	Князов Б.А.				
		Провер.	Климов С.М.				
		Т.контр.					
		Принят.					
		Н.Контр.					
		Утв.	Климов С.М.				

Результаты оценки эффективности применения разработанного датчика

Лист 8 Листов 11

МГТУ им. Н.Э. Баумана  
Группа ИУ10-121



# Экологическая часть

## 1. Анализ потенциальных опасностей, вредностей при разработке ПО и мероприятия по их устранению

Требования к микроклимату

Требования к уровням шума и вибрации

Требования к освещению

Требования к уровням ЭМ полей

Требования к визуальным параметрам ВДТ

Электробезопасность

Пожаропасность

Требования к организации и оборудованию рабочих мест

Отходы и утилизация

## 2. Расчет освещенности рабочего места

До проведения мероприятий

После проведения мероприятий

Диаграмма пространственного распределения силы света в помещении

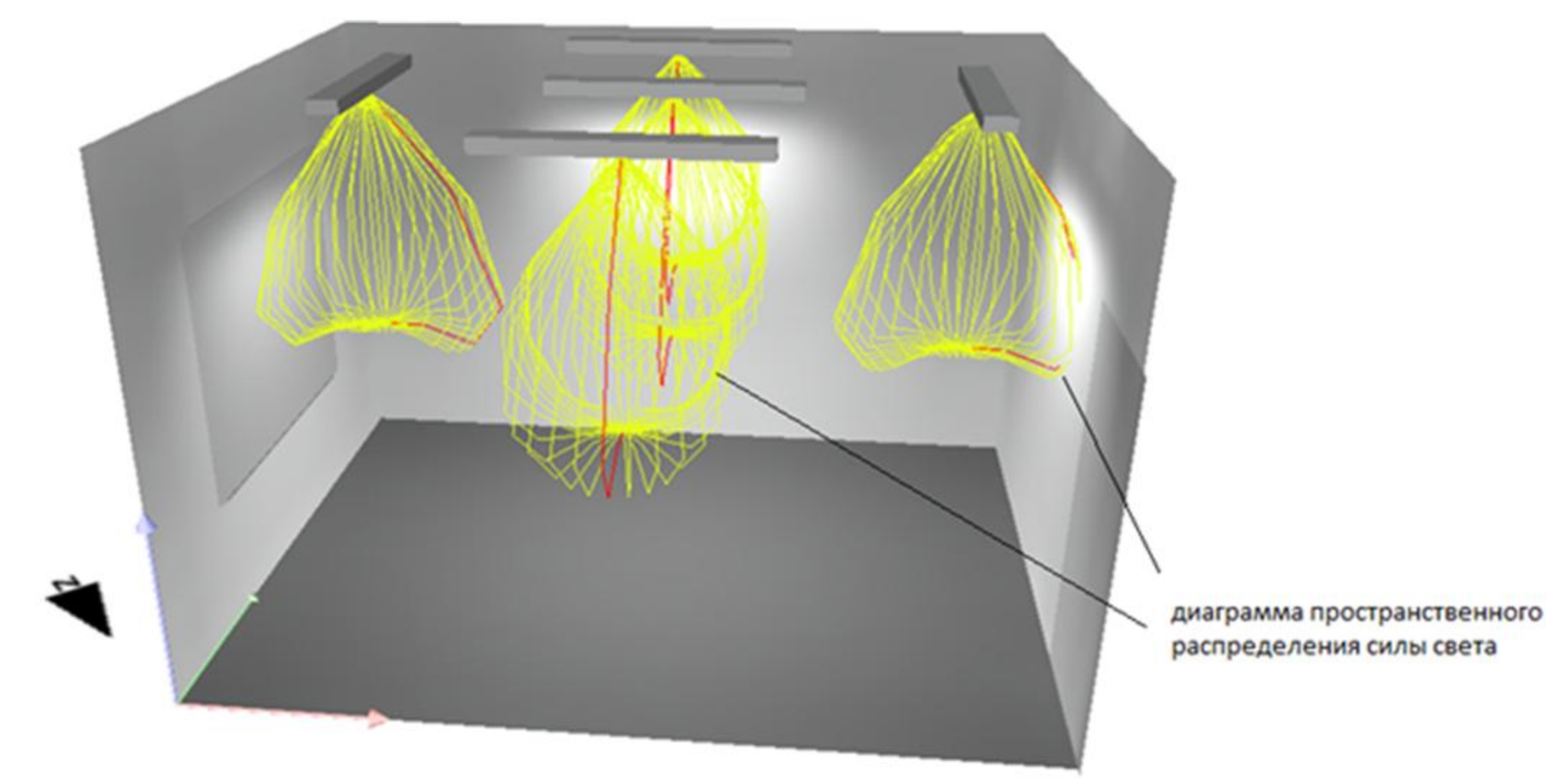
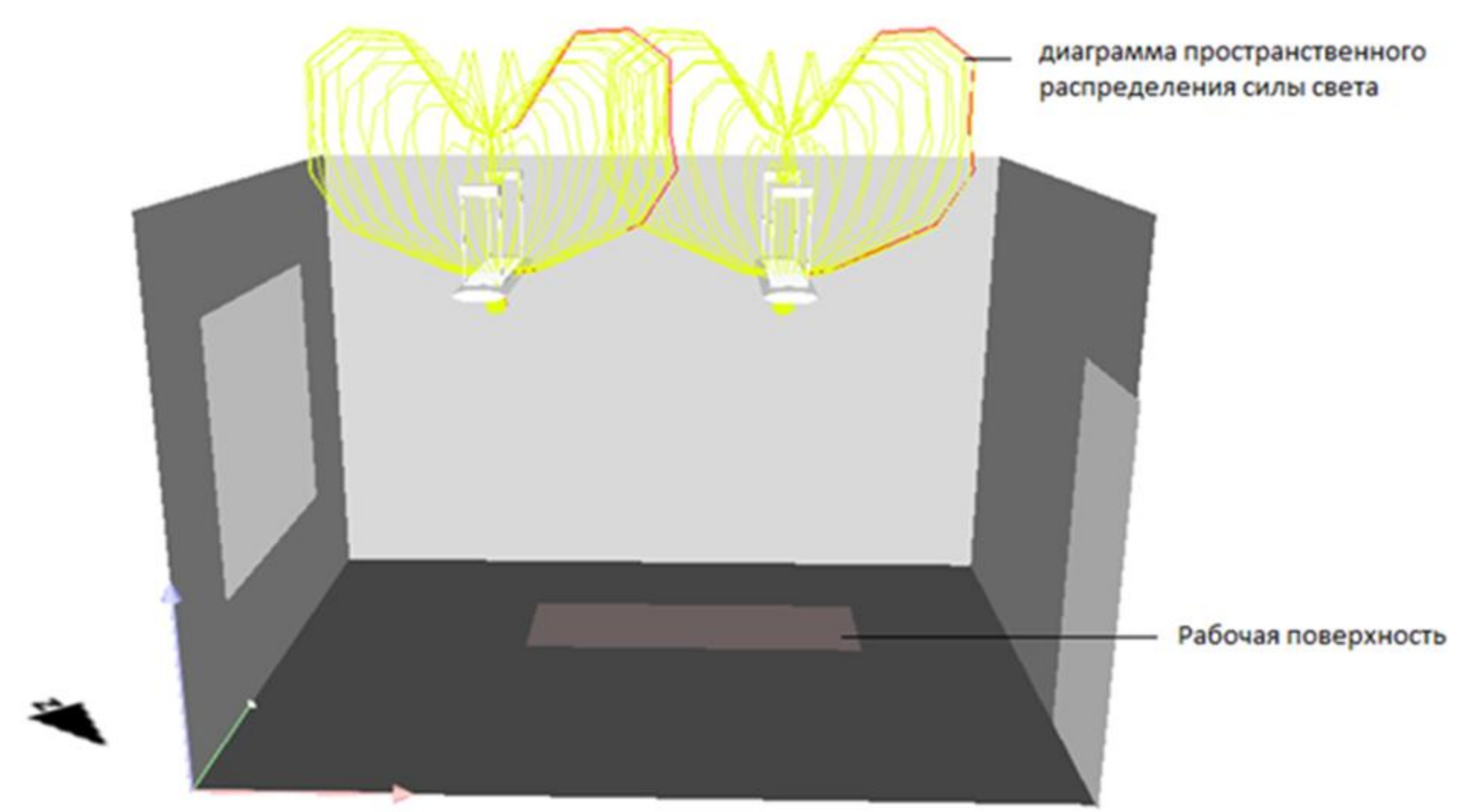


Рисунок 9.1 – Диаграмма пространственного распределения силы света в помещении

Рисунок 9.3 – Диаграмма пространственного распределения силы света в помещении

Распределение освещенности на высоте рабочей поверхности

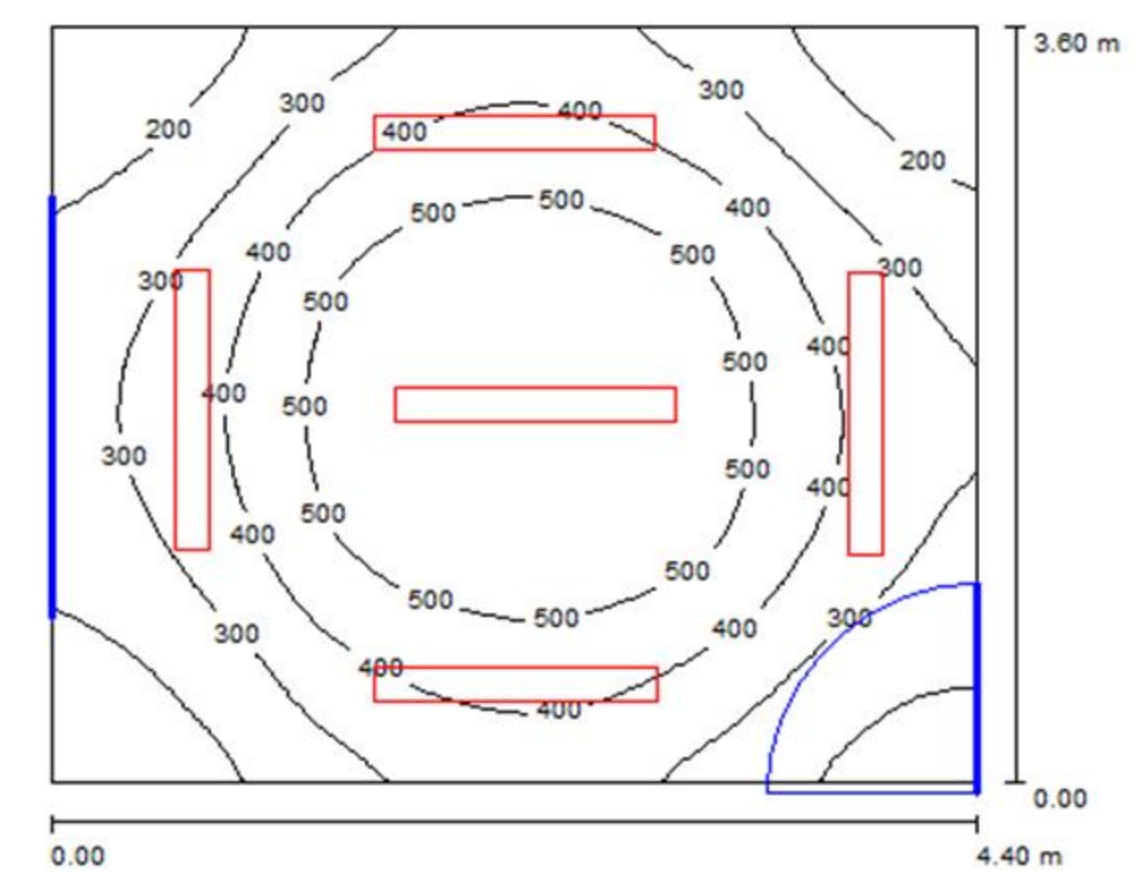
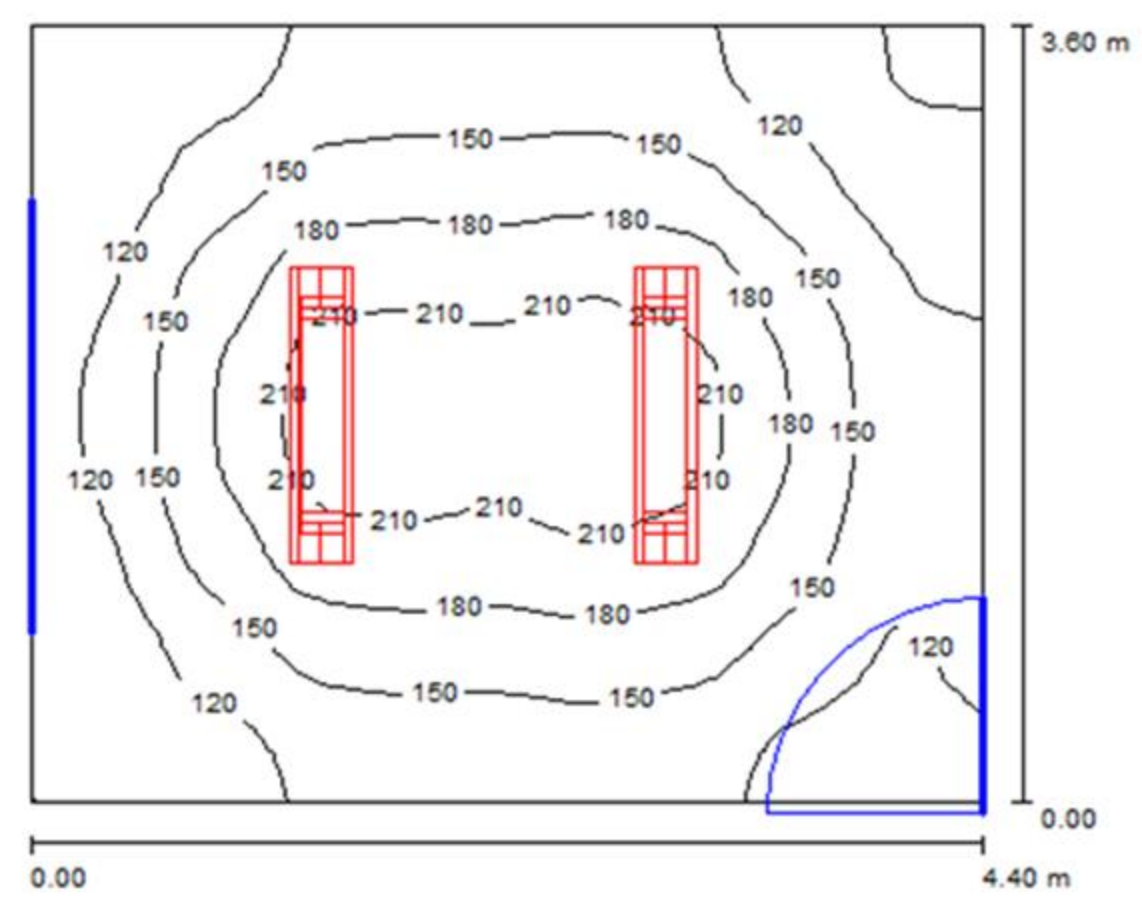


Рисунок 9.2 – Распределение освещенности на высоте рабочей поверхности

Рисунок 9.4 – Распределение освещенности на высоте рабочей поверхности

### Выводы

Расчеты показали, что в производственном помещении средняя освещенность рабочей плоскости составляла 152 лк, что меньше требуемых СанПиН значений (300 - 500 лк) . Были разработаны мероприятия по устранению несоответствий освещения нормам, в результате которых по расчетам программы DIALux освещение в помещение должно стать более равномерным, средняя освещенность рабочей плоскости будет составлять 372 лк, что удовлетворяет требованиям СанПиН

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации			
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
		Разраб.	Князев Б.А.				
		Провер.	Климов С.М.				
		Принят.					
		Н.Конт.					
		Утв.	Климов С.М.				
Экологическая часть					Лист 9	Листов 11	
					МГТУ им. Н.Э. Баумана		



# Организационно-экономическая часть

Таблица 10.1 – Планирование работ по разработке системы

№ этапа	Содержание работ	Продолжительность, раб. дней	Исполнители		Календарные дни																			
			Категория	Число	Количество рабочих дней																			
					01.02-10.02	11.02-20.02	21.02-02.03	03.03-12.03	13.03-22.03	23.03-01.04	02.04-11.04	12.04-21.04	22.04-01.05	02.05-11.05	12.05-21.05	22.05-31.05								
8	6	7	6	7	8	6	8	6	6	8	6	6	7	7										
1	Техническое задание	8	Инженер по защите информации – I категории	1	3	5																		
		8	Инженер – Программист – I категории	1	3	5																		
2	Эскизный проект	8	Инженер по защите информации – I категории	1		1	7																	
		8	Инженер – Программист – I категории	1		1	7																	
3	Технический проект	15	Инженер по защите информации – I категории	1				6	7	2														
		15	Инженер – Программист – I категории	1				6	7	2														
4	Рабочий проект	23	Инженер по защите информации – I категории	1						6	6	8	3											
		23	Инженер – Программист – I категории	1						6	6	8	3											
5	Внедрение	23	Специалист по защите информации - I категории	1										3	6	7	7							
		23	Инженер – Программист – I категории	1											3	6	7	7						

77 рабочих дней

### Оценка эффективности инвестиций

Для оценки инвестиций необходимо рассчитать чистый дисконтированный доход в течение, как минимум 10 лет, по формуле

$$NPV = -IC + \sum_{t=1}^N \frac{CF_t}{(1+i)^t} \quad (1)$$

и определить, в какой момент суммарный дисконтированный доход от реализации проекта будет равен размеру инвестиций

$$i = Rf + R1 + \dots + Rn, \quad (2)$$

где *i* – ставка дисконтирования;  
*Rf* – безрисковая ставка дохода (8,5% – ставка по российским европейским облигациям);  
*R1 + ... + Rn* – рискованные премии по различным факторам риска.

Таблица 10.2 – Сравнительный анализ рынка предложений на выполнение данного проекта

Наименование организации	Стоимость выполнения работ, рублей	Срок выполнения работ, рабочих дней
МГТУ им. Н.Э. Баумана	657 928	77
ЗАО "Современные Телекоммуникации"	823 537	52
Г'son & Partners	689 174	59
МГУ им. М.В. Ломоносова	671 258	75
ЗАО "Синтерра"	605 251	92

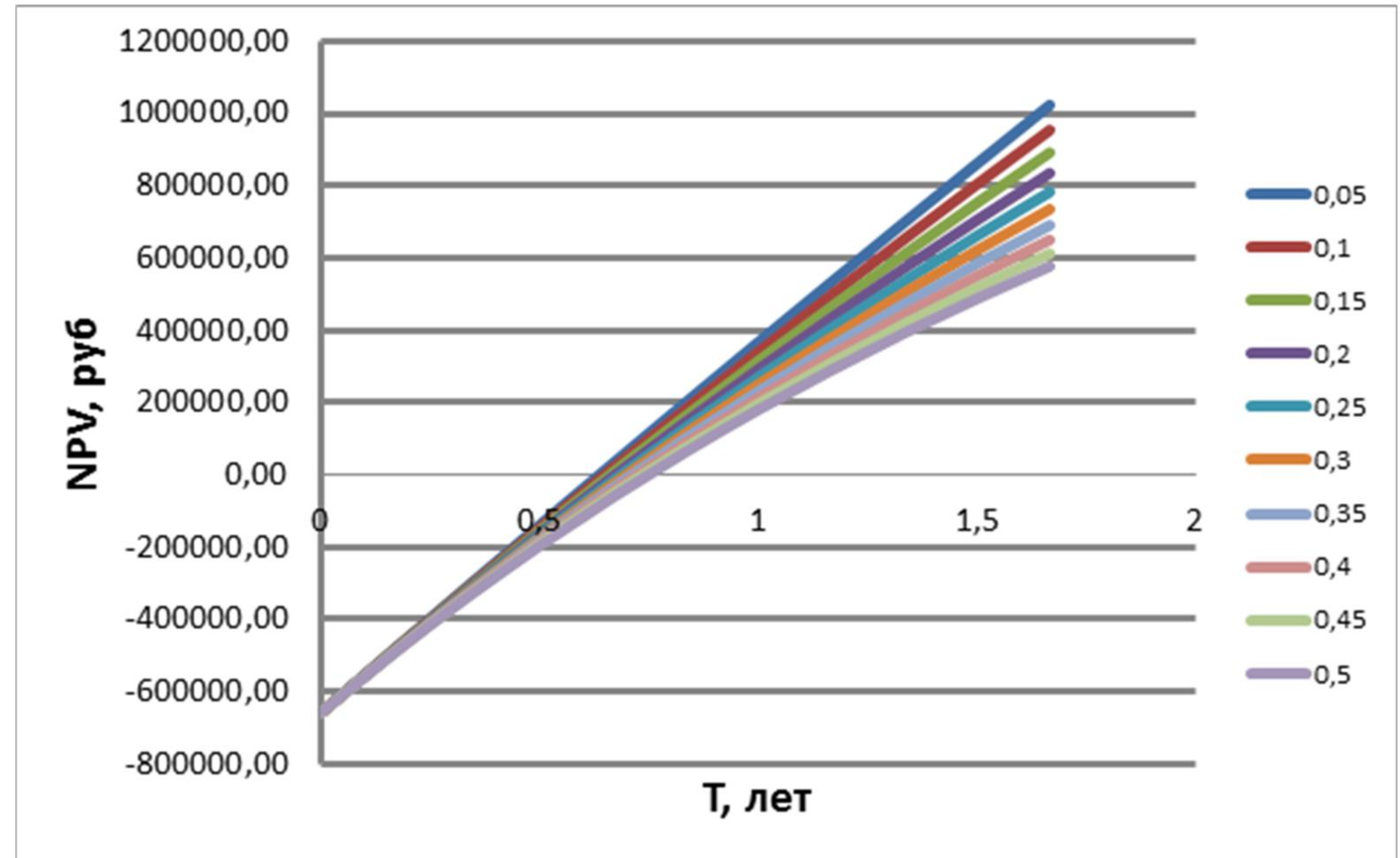


Рисунок 10.1 – Графики зависимостей чистого дисконтированного дохода от периода времени для различных значений ставок дисконтирования

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеoinформации			
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
Разраб.		Князов Б.А.					
Провер.		Климов С.М.					
Т.контр.							
Принят.							
Н.Контр.							
Утв.		Климов С.М.					

Лист 10 из 11  
МГТУ им. Н.Э. Баумана  
Группа ИУ10-121



## Выводы:

1. Проанализированы существующие системы и средства обнаружения атак, в результате чего доказана актуальность задачи разработки методики, модели и алгоритмов противодействия деструктивным воздействиям оператора в РВС.
2. Разработана модель внутренних угроз нарушителя, включающая в себя классификацию внутренних нарушителей по полномочиям доступа и по психологическим признакам, классификацию деструктивных воздействий по биометрическим признакам оператора.
3. Разработана модель автоматического детектирования биометрических признаков нарушителя.
4. Разработана обобщенная методика выявления деструктивных воздействий оператора в РВС по видеоинформации.
5. Разработаны алгоритмы функционирования датчика предупреждения потенциального ДВО в составе СОВ.
6. Разработан макет датчика предупреждения ДВО, вероятность распознавания потенциального ДВО которого составляет 83%.
7. Приведены результаты оценки эффективности применения разработанного макета биометрического датчика в составе СОВ, по которым можно наблюдать преимущество использования СОВ с биометрическим датчиком по сравнению с имеющимися СОВ и традиционными средствами противодействия.
8. Для успешности применения разработанной методики противодействия ДВО на КВИС необходимо увеличивать вероятность распознавания признаков ДВО путем модификации алгоритмов автоматической расстановки антропометрических точек (с целью увеличения точности расстановки точек) и алгоритмов вычисления функционального состояния оператора.

Дипломная работа				Разработка датчика оценки деструктивных воздействий оператора в РВС по видеоинформации			
Изм.	Лист	Документ №	Подпись	Дата	Литер.	Масса	Масшт.
Разраб.		Князов Б.А.			Заключение		
Провер.		Климов С.М.					
Т.контр.							
Принят.							
Н.Контр.							
Утв.		Климов С.М.					
					Лист 11	Листов 11	
					МГТУ им. Н.Э. Баумана Группа ИУ10-121		