Российские сети
вещания и оповещения

ПРЕДИКТИВНАЯ АНАЛИТИКА УГРОЗ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ДИНАМИЧЕСКОГО АНАЛИЗА

Докладчик: кандидат технических наук, профессор Тамп В.Л.
Управление разработок ФГУП РСВО

Онлайн-конференция Groteck
«Комплексная безопасность и защищенность объектов промышленности,
нефтегазового сектора и электроэнергетики». – 2021»

Одним из приоритетов национальных интересов Российской Федерации определенных Указом Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» является создание единой комплексной системы обеспечения безопасности жизнедеятельности населения (КСОБЖ) в границах субъектов Российской Федерации.

В рамках реализации данной концепции Федеральное государственное унитарное предприятие «Российские сети вещания и оповещения» (ФГУП РСВО) предлагает решение по построению узлов управления комплексной безопасностью на базе **Универсального программно-аппаратного комплекса (УПАК РСВО)**.

УПАК РСВО – интеллектуальная система полного цикла управления системами, силами и средствами, которая объединяет на программно-аппаратном уровне подсистемы и решения, используемые в создании комплексной системы безопасности. Комплекс создан на базе собственного программного обеспечения, объединяет системы связи, мониторинга, анализа, прогнозирования и имеет свою уникальную разработанную **подсистему комплексного информирования и оповещения**.

Узел управления комплексной безопасностью – это совокупность программно- технических средств, модулей различного назначения, автоматизированных систем работающих совместно по единому плану, направленных на выполнение одной или нескольких задач решаемых в интересах обеспечения комплексной безопасности объектов военной инфраструктуры.

Основные принципы противодействия угрозам заложенные в узле управления комплексной безопасностью

Принцип ***создания в узле управления системы исследования прогнозных сценариев.***

Принцип ***упреждения и своевременного выявления уязвимостей.***

Принцип ***комплексного подхода к оценке обстановки охватывающей все подсистемы обеспечивающие безопасность.***

Основные задачи решаемые программно-аппаратным комплексом управления комплексной безопасностью

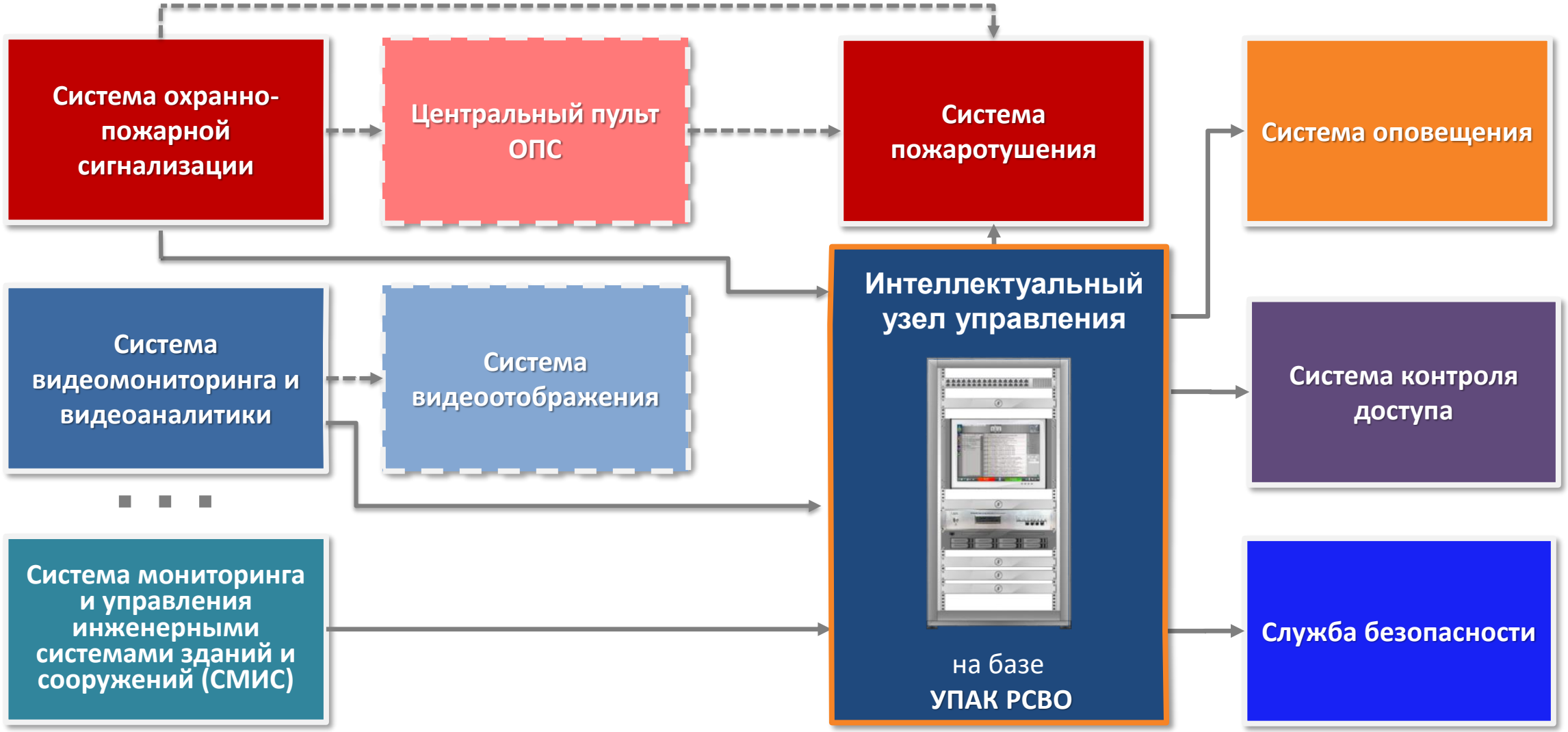
Программно-аппаратный комплекс управления системой комплексной безопасностью разработан С ЦЕЛЬЮ автоматизации функций и процесса управления комплексной системой безопасности на объектах военной инфраструктуры в различных режимах боевой готовности.

Обеспечение функционирования разнородных сил и средств комплексной безопасности по единому плану (замыслу), систематизация потоков информации от различных информационных систем в единый информационный контур как существующих, так и перспективных при подготовке и проведения мероприятий обеспечения безопасности объектов различной инфраструктуры.

Выявление уязвимостей, оценка состояния системы комплексной безопасности в реальном режиме времени, прогнозирования сценариев развития ситуации, разработка систем управления базами данных, математических моделей и информационно-расчетных задач, формирование обоснованных вариантов решений, представление структурированных аналитических отчетов, докладов, справок, высокой степени информативности, визуализация данных.

Подготовка и реализация управленческих решений в различных режимах.

Система комплексной безопасности ТЦ на базе Универсального программно-аппаратного комплекса (УПАК) РСВО

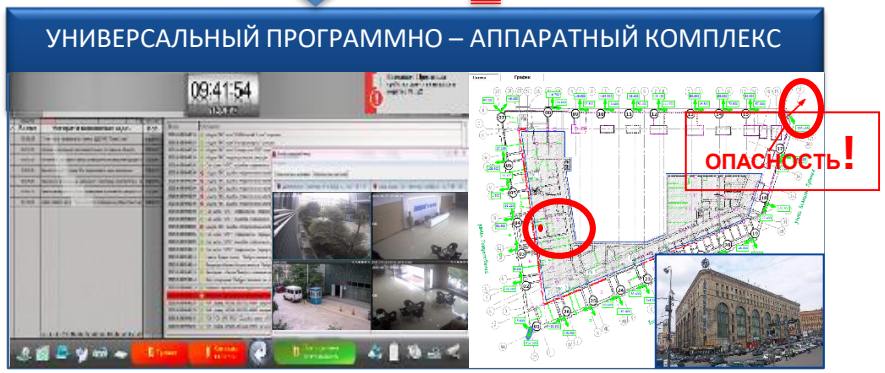


Универсальный программно-аппаратный комплекс РСВО – это интеллектуальная платформа, представляющая собой совокупность функциональных узлов (устройств) и специального программного обеспечения

Система комплексной безопасности промышленного объекта на базе Универсального программно-аппаратного комплекса (УПАК) РСВО

УПАК во взаимодействии с дежурной сменой определяет работу исполнительных систем и службы безопасности

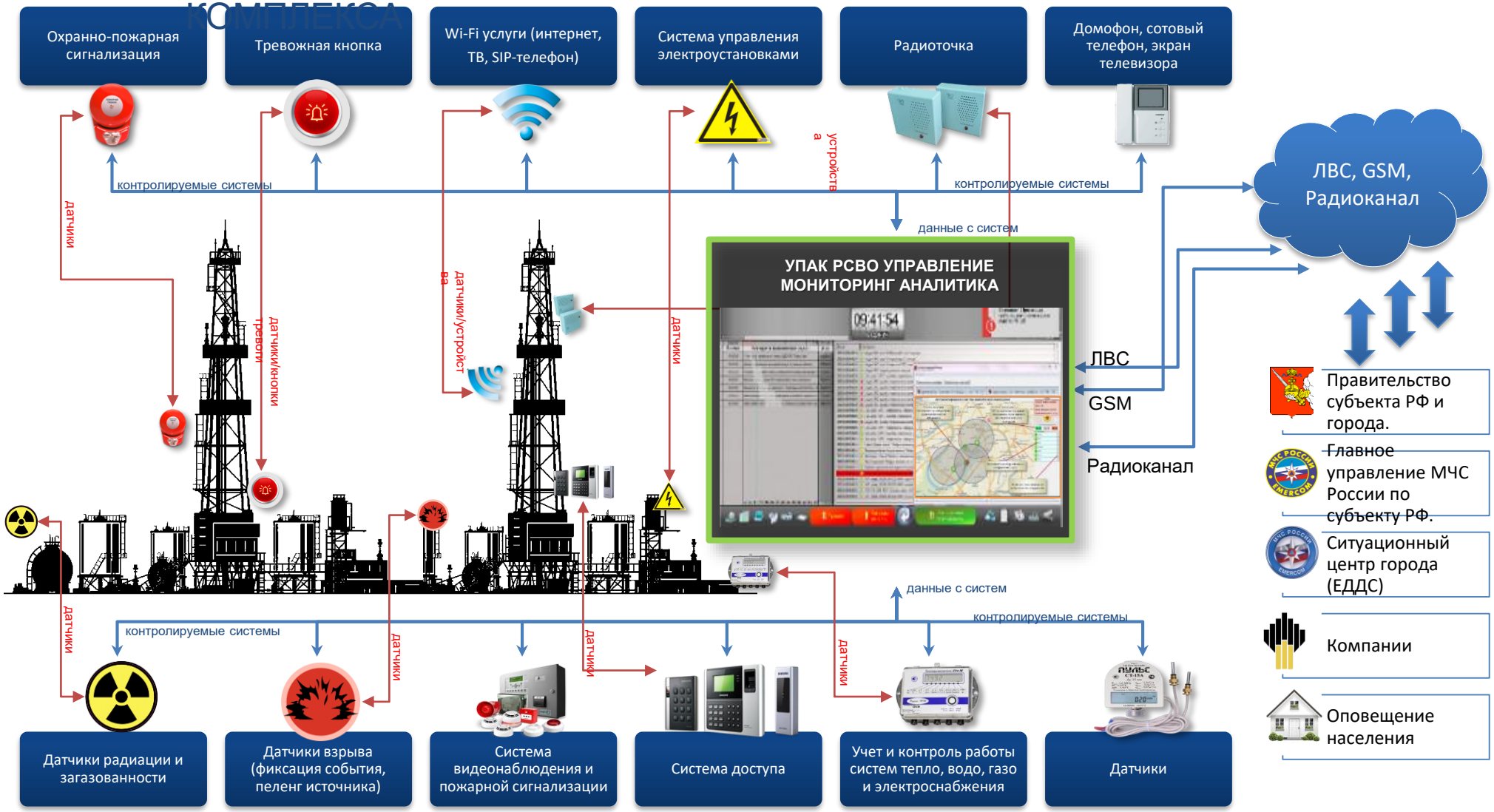
ЦЕЛИ, ДОСТИГАЕМЫЕ УНИВЕРСАЛЬНЫМ ПРОГРАММНО-АППАРАТНЫМ КОМПЛЕКСОМ УПАК РСВО



- Сокращение времени реагирования на различные ЧС и аварии
- Использование системы в условиях нескольких тревог, в повседневной деятельности и в ЧС
- Оценка защищенности объектов и территорий по совокупности всех параметров
- Сокращение человеческих и материальных потерь на начальных этапах ЧС и аварий
- Контроль, моделирование, прогнозирование, поддержка принятия решений, управление силами и средствами
- Информирование по всем доступным каналам связи лиц, принимающих решения, комплексное оповещение населения
- Межведомственное взаимодействие, доведение сигналов и команд управления до подчиненных структур
- Платформа интеллектуального анализа данных
- Интеграция установленных систем
- Противодействие киберпреступности

МОНИТОРИНГ, ИНФОРМИРОВАНИЕ, ОПОВЕЩЕНИЕ И УПРАВЛЕНИЕ

НА ПРИМЕРЕ ОБЪЕКТОВ ПОВЫШЕННОЙ ОПАСНОСТИ ПОСТРОЕНИЕ КОМПЛЕКСА



УПАК РСВО – интеллектуальная платформа

Специальное программное обеспечение УПАК – это программный продукт, полностью разработанный в РСВО. Использованы компоненты с открытым исходным кодом. Язык программирования – C++. Фреймворк - Qt. Существует реализация для ОС Astra Linux. Разработано сопряжения с ГИС КБ «Панорама».

ASTRALINUX® common edition

C++ Qt

PostgreSQL

КБ ПАНОРАМА

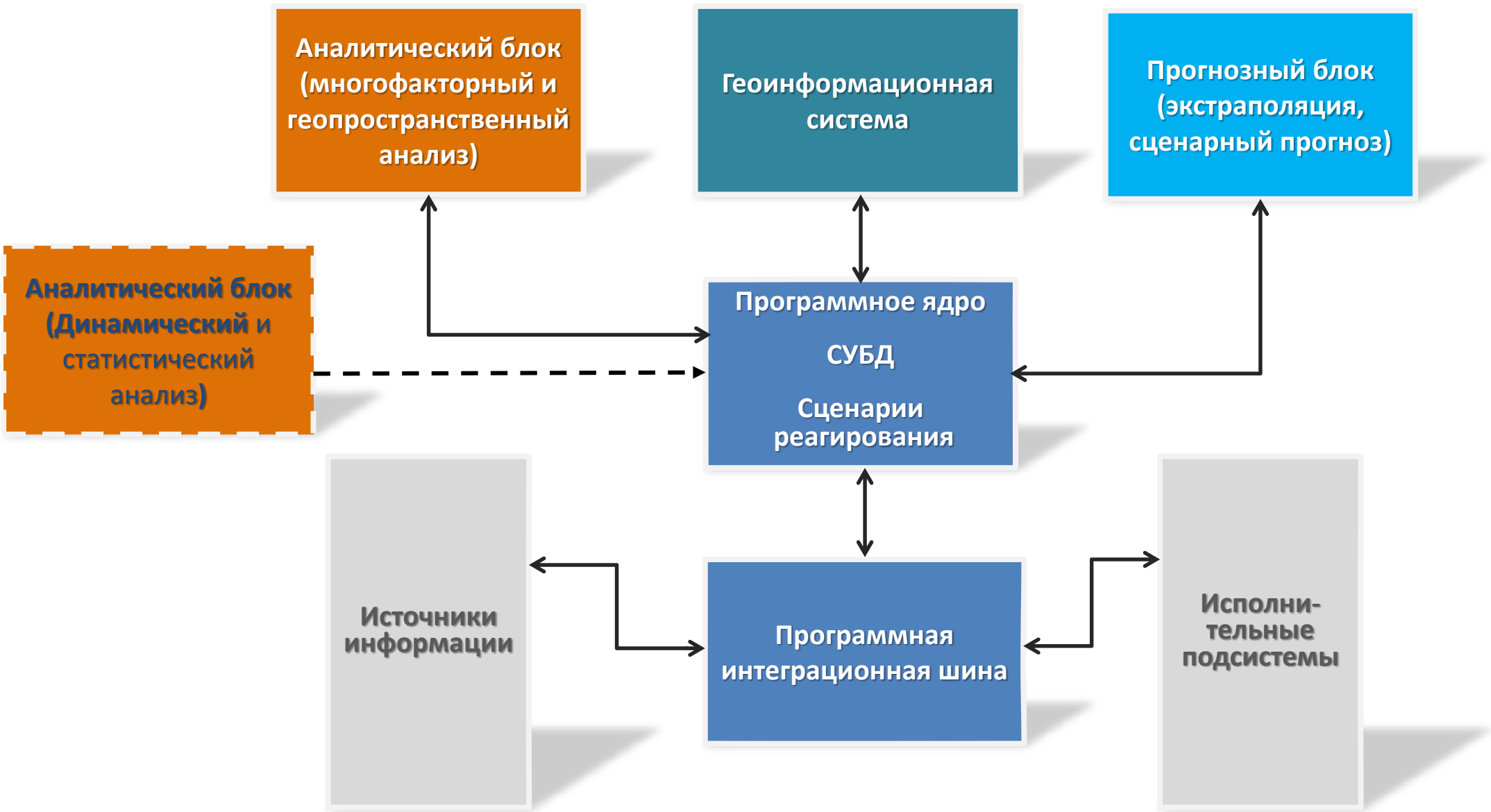
Основные достоинства УПАК РСВО

Комплекс обеспечивает поддержку принятия решения в кризисных ситуациях, в условиях **ограниченного времени и недостатка квалифицированных кадров**.

Анализ результатов применения УПАК РСВО показал, что он обеспечивает:

- снижение времени реагирования на угрозы;
- снижение вероятности ошибок и роли «человеческого фактора»;
- снижение потенциального ущерба;
- повышение уровня безопасности;
- повышение эффективности управления объектами инфраструктуры.

Основные элементы интеллектуального узла управления УПАК



Методы анализа временных рядов

Одна из основных задач систем комплексной безопасности – оперативное и достоверное обнаружение угроз.

В роли признаков угроз могут выступать, в том числе, потоки случайных событий, представленные в виде временных рядов.

В случае стандартных ситуаций, случайный процесс, как правило стационарен, при появлении же угрозы происходит скачок значений статистических признаков, что нарушает стационарность исследуемого процесса.

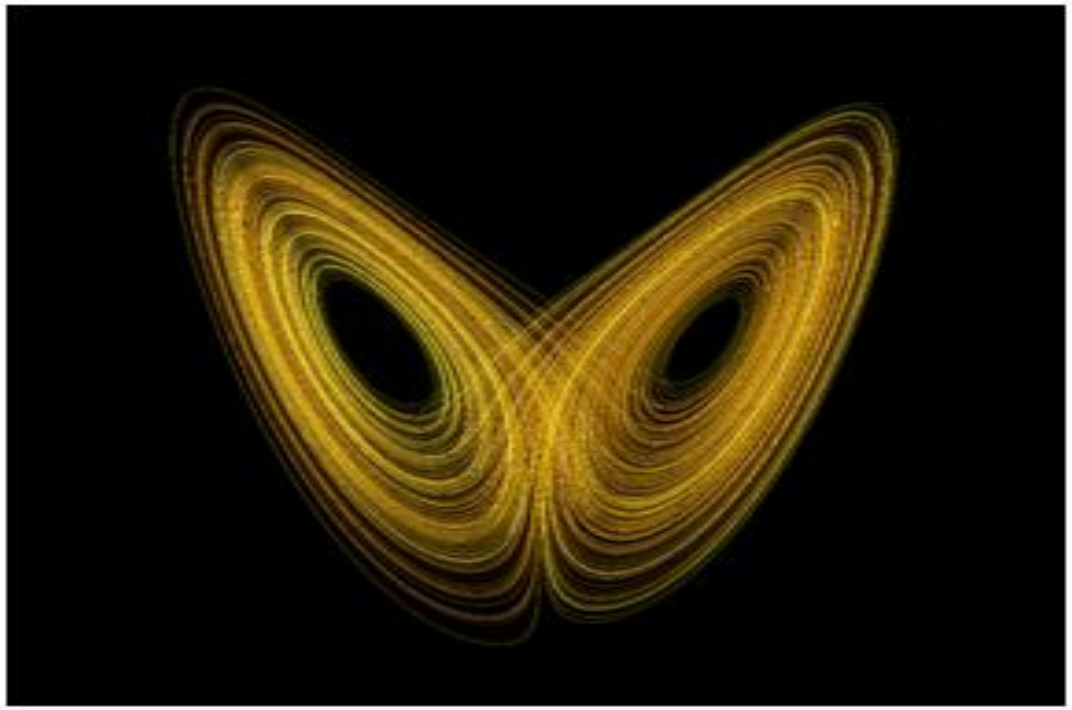
Проведен анализ существующих подходов, позволяющих обнаружить изменение состояния объекта, признаки которого представлены в виде временного ряда:

1. Метод корреляционной размерности.
2. Метод корреляционной энтропии.
3. Метод автокорреляционной функции.
4. Метод средней взаимной информации.
5. Метод на основе расчета показателя Херста.

Результаты проведенных экспериментов показали, что ни один из представленных подходов не позволяет оперативно обнаружить изменение характеристик временного ряда, свидетельствующее о событии угрозы.

Это привело к необходимости поиска иных подходов к решению данной проблемы, в том числе с использованием теории хаоса.

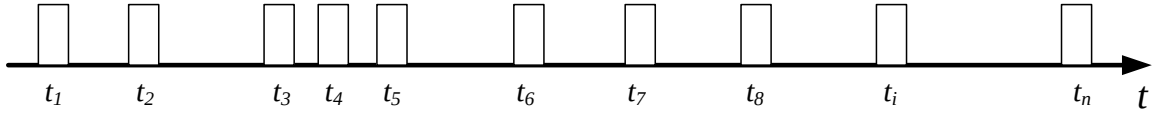
Фазовый портрет странного аттрактора Лоренца



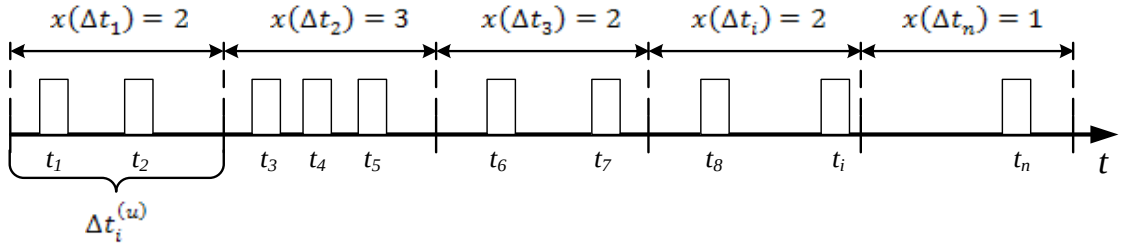
Математический аппарат теории хаоса позволяет описывать состояние исследуемых систем в виде фазовых портретов, формируемых фазовыми траекториями.

Примером является странный аттрактор Лоренца, описывающий графически решения системы дифференциальных уравнений.

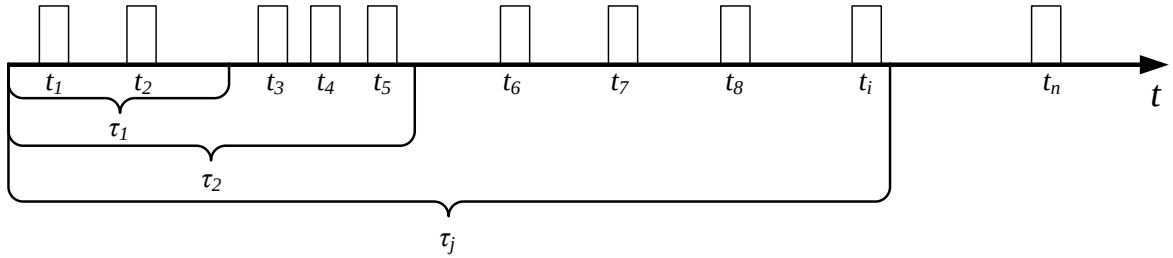
Аналогом такого подхода для дискретных динамических систем являются разностные уравнения.



Поток событий, представленный в виде временного ряда

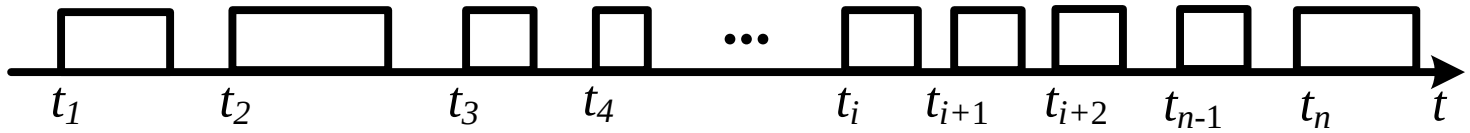


Порядок формирования интервального ряда с интервалом $\Delta t_i^{(u)}$



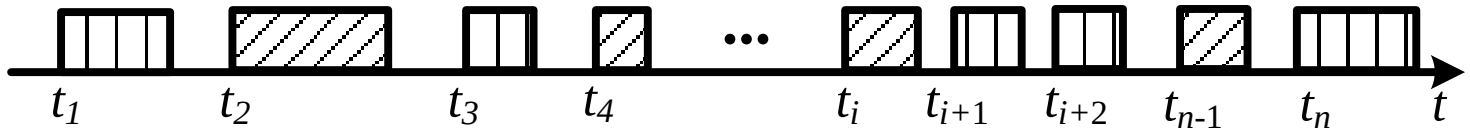
Пример выбора интервалов различной длительности

Примеры вариантов отбора моментов событий



а)

Поток моментов событий по времени $T_{\{n\}} = (t_1, t_2, \dots, t_i, \dots, t_n)$



б)

Поток моментов событий по ансамблю $A_{\{n-1\}} = (t_2, t_4, \dots, t_i, \dots, t_{n-1})$.

Варианты формирования динамических переменных

При формировании двумерного фазового портрета по осям абсцисс и ординат откладываются, так называемые **динамические переменные**, от правильного выбора которых зависит информативность полученного изображения и степень его отличия от формы фазовых портретов для иных ситуаций

Простейшим вариантом формирования динамических переменных является их представление в виде разностного уравнения 1-го порядка

$$\Delta y_i = N_{i+1} - N_i \qquad (1)$$

Возможно вычисление разности количества моментов запросов между удаленными интервалами со смещением *l*.

$$\Delta y(k) = N_{i+1} - N_i \qquad (2)$$

Для формирования разностных уравнений 2-го порядка производится формирование разность $\Delta^2 y(k)$ от разности значений соседних интервалов $\Delta x(k)$.

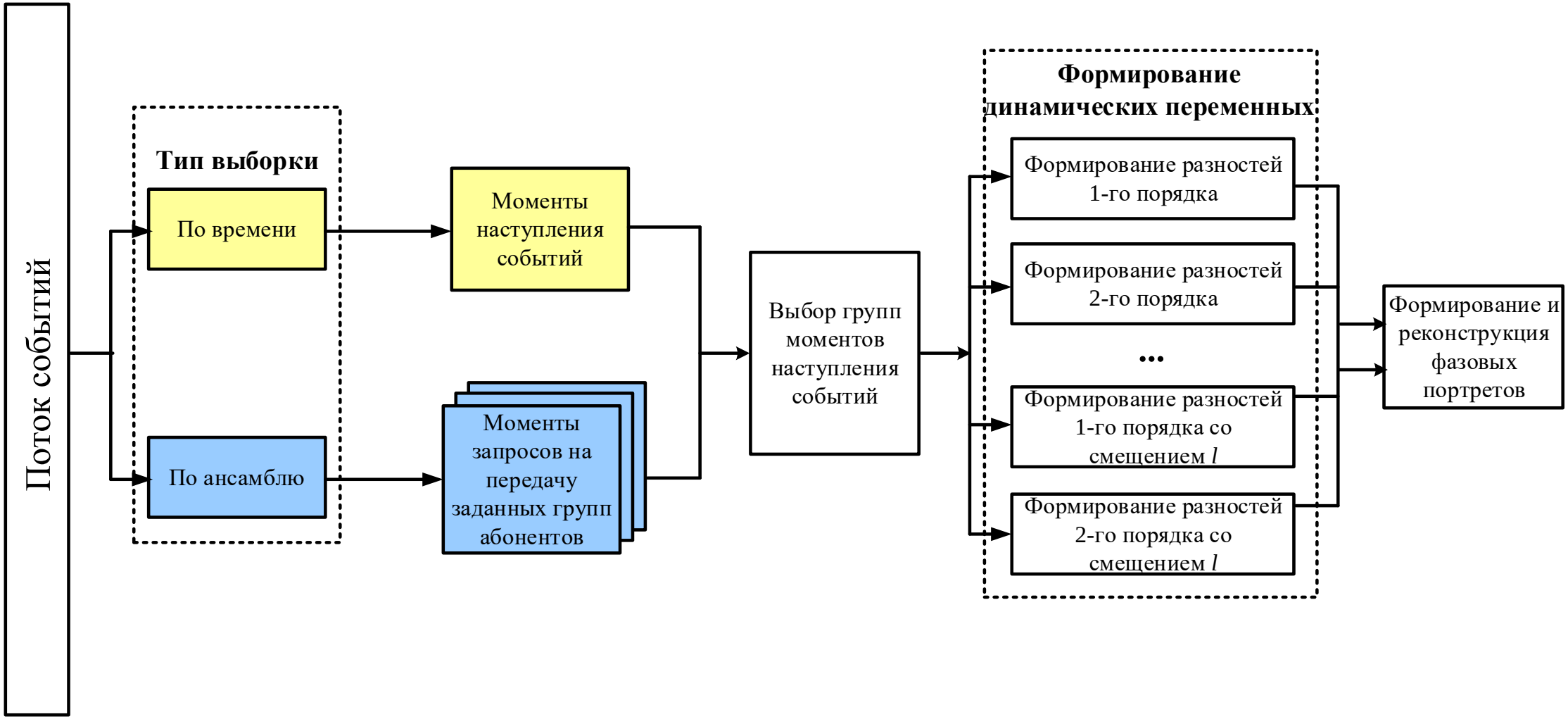
$$\Delta^2 y_i = \Delta y_{i+1} - \Delta y_i \qquad (3)$$

или

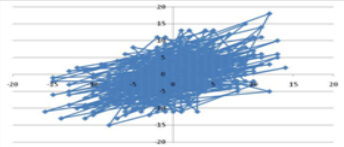
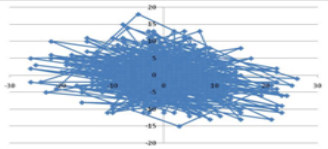
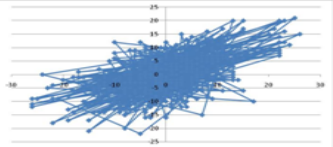
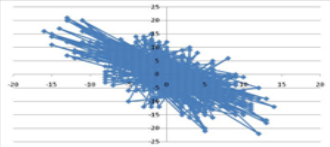
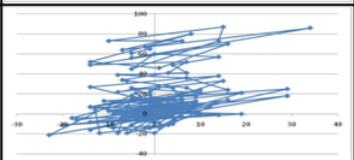
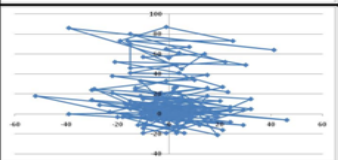
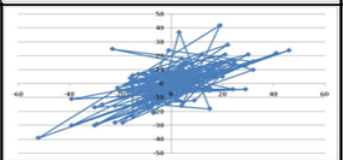
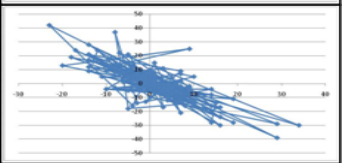
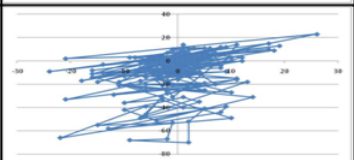
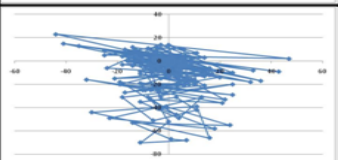
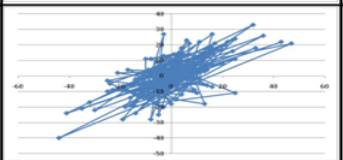
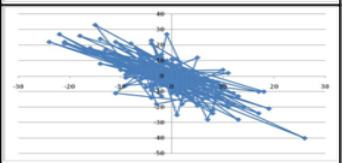
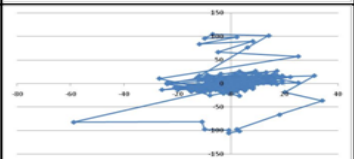
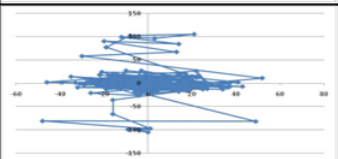
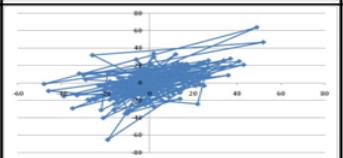
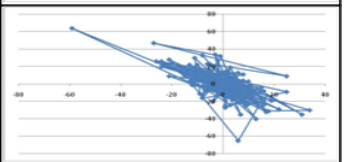
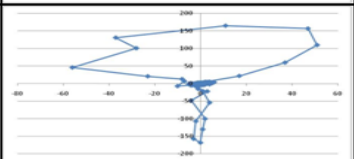
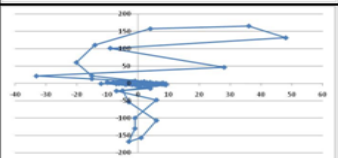
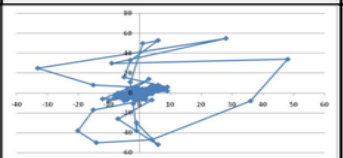
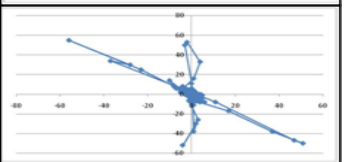
$$\Delta^2 y^*(k) = \Delta y^*(k+1) - \Delta y^*(k). \qquad (4)$$

Из достаточно большого количества вариантов пар динамических переменных выбираются те, на основе которых формируются наиболее информативные фазовые портреты.

Порядок выбора динамических переменных для распознавания состояний объектов угроз



Фазовые портреты, сформированные на основе различных пар динамических переменных

№ п/п	Возможные ситуации, возникающие в сети	Фазовый портрет			
		Пара динамических переменных $\Delta x(k)$ и $\Delta_{(20)}x'(k)$	Пара динамических переменных $\Delta^2 x(k)$ и $\Delta_{(20)}x'(k)$	Пара динамических переменных $\Delta^2 x(k)$ и $\Delta^2_{(20)}x'(k)$	Пара динамических переменных $\Delta x(k)$ и $\Delta^2_{(40)}x'(k)$
1	Сеть с квазипостоянной интенсивности				
2	Сеть с возрастанием интенсивности по сигмоиде				
3	Сеть с убыванием интенсивности по сигмоиде				
4	Сеть с аномальным увеличением интенсивности				
5	Сеть с аномальным уменьшением интенсивности				

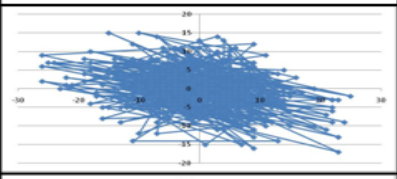
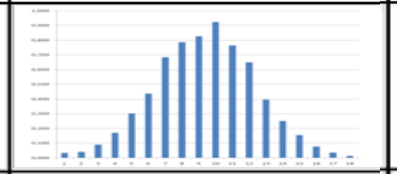
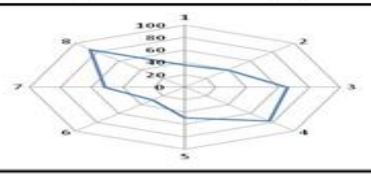
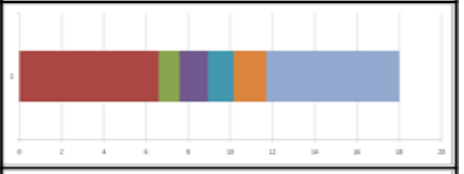
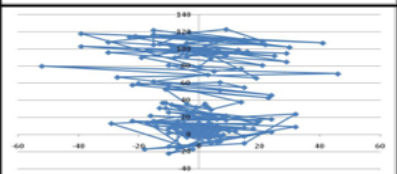
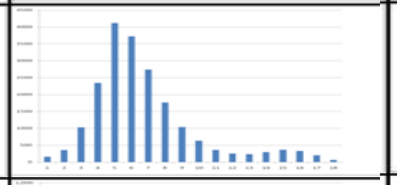
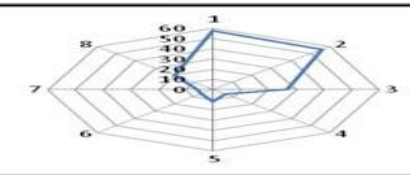
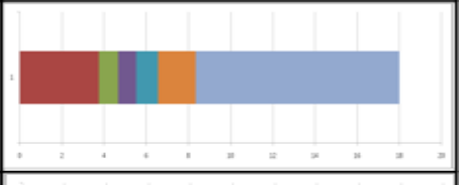
В таблице приведены фазовые портреты для потоков событий с различными законами изменения интенсивности для различных пар динамических переменных.

Варианты реконструкции фазовых портретов

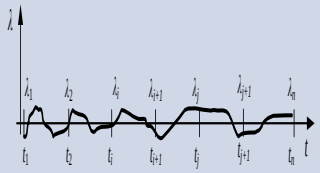
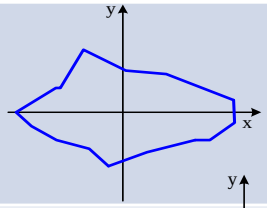
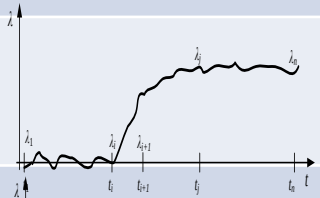
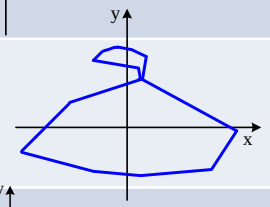
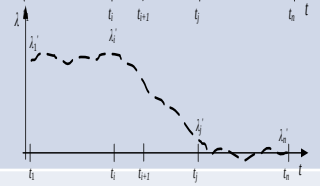
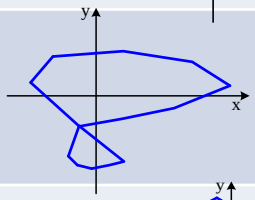
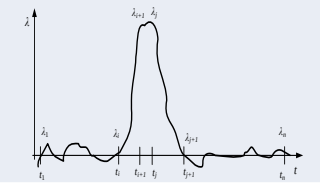
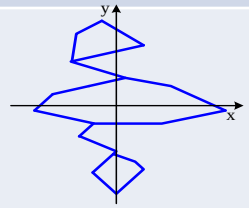
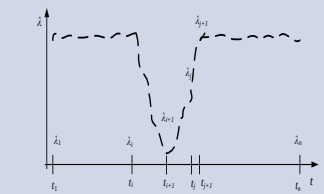
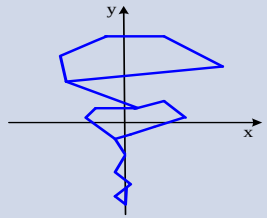
Хаотичный характер фазовых портретов вызывает определенные проблемы при их распознавании, поэтому было предложено провести реконструкцию портретов.

Предложено три варианта реконструкции:

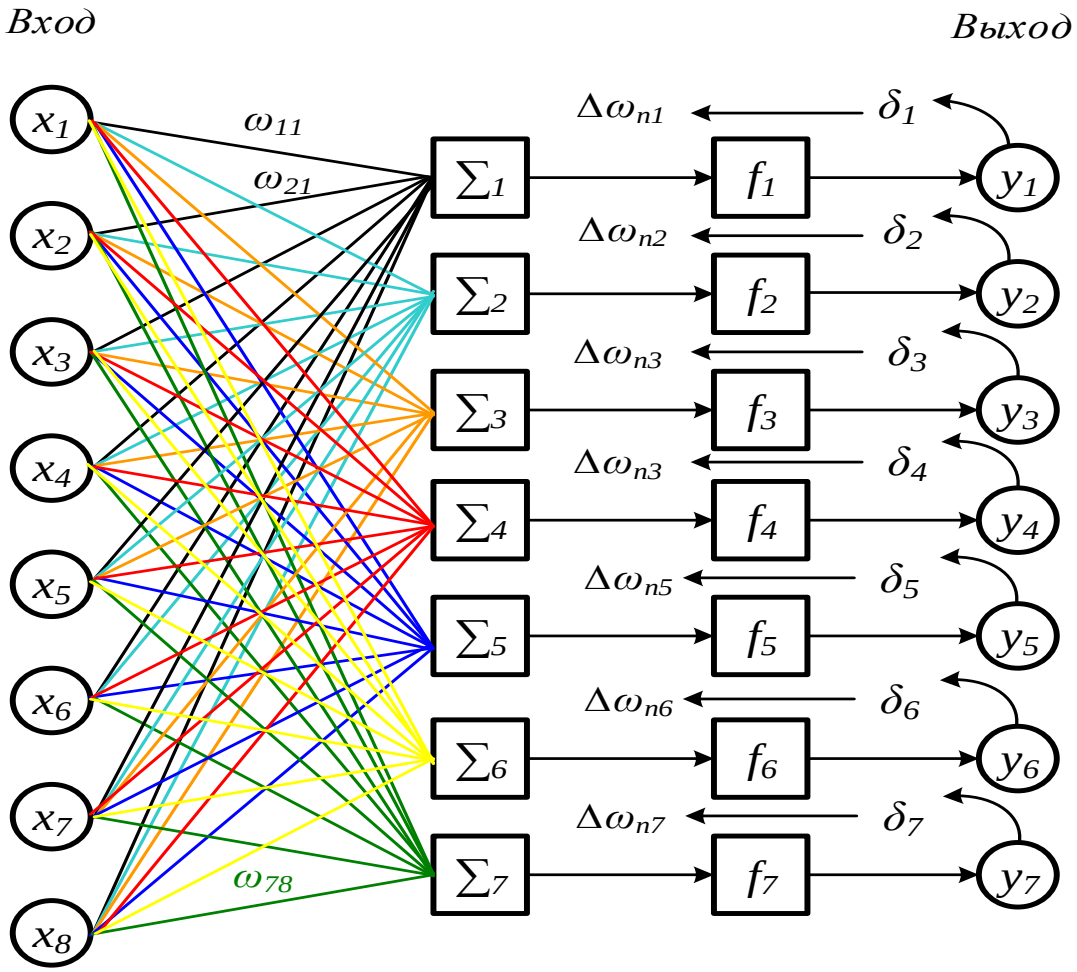
- на основе гистограмм;
- на основе подсчета фазовых точек в заданных секторах;
- на основе квантилей распределений.

№ п/п	Возможные ситуации, возникающие в сети	Фазовый портрет	Реконструированный фазовый портрет	Реконструированный фазовый портрет	Реконструированный фазовый портрет
1	Сеть с квазипостоянной интенсивности				
2	Сеть с возрастанием интенсивности по сигмоиде				

Основные состояния объектов и соответствующие им законы изменения интенсивности потока событий

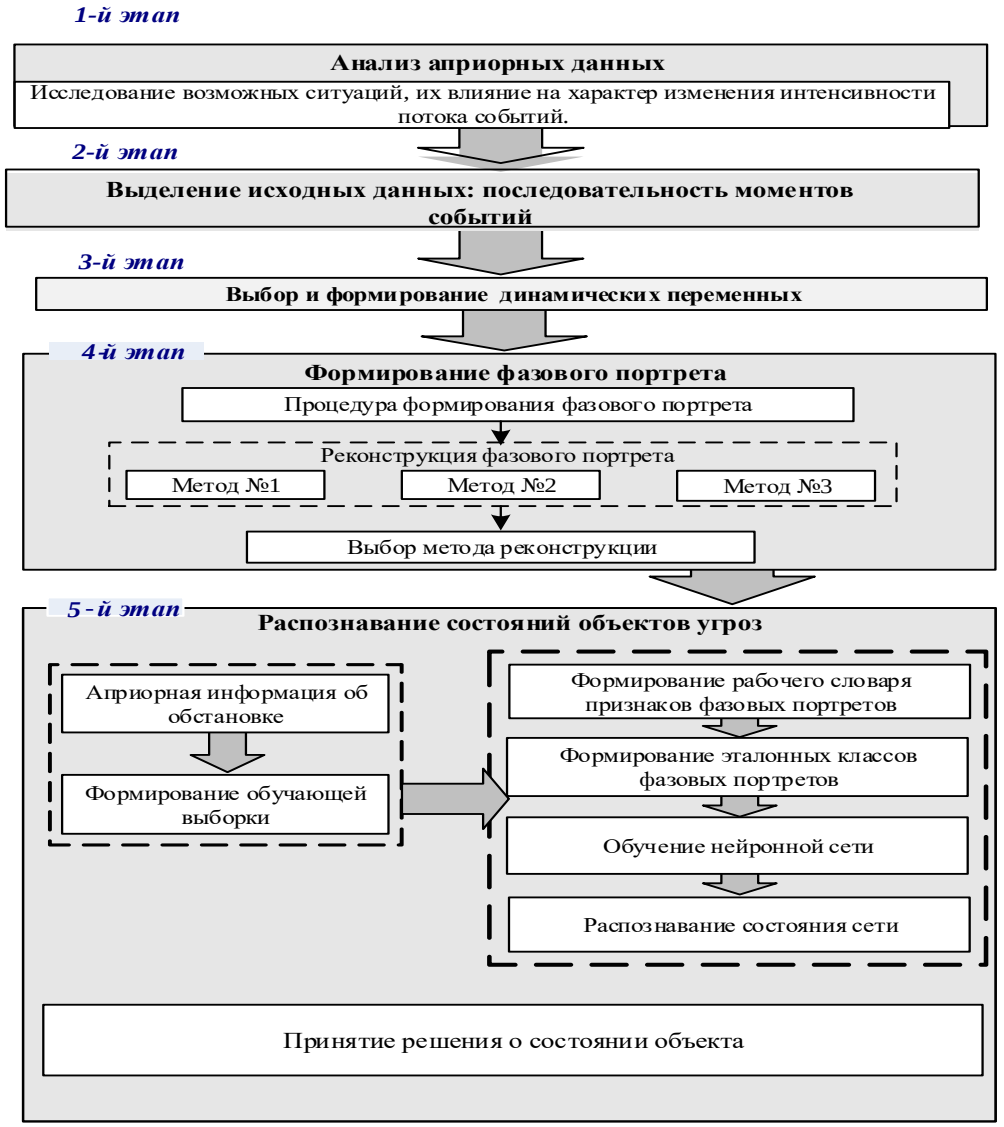
№ п/п	Основные состояния объектов	Вид закона изменения интенсивности потока запросов	Сформированный фазовый портрет
1	Квазипостоянная интенсивность		
2	Возрастание интенсивности		
3	Убывание интенсивности		
4	Аномальный всплеск интенсивности		
5	Аномальный спад интенсивности		

Структурная схема нейронной сети с обратным распространением ошибки для распознавания состояний объектов



На входе – значение квантилей (октилей), являющихся результатом реконструкции фазового портрета, на выходе – вид состояния объекта угрозы.

Блок-схема методики распознавания состояний объектов угроз



Российские сети вещания и оповещения

Спасибо за внимание!

ФГУП РСВО
105094, г. Москва, ул. Семеновский вал, д. 4
Телефон: +7 (499) 639-00-00, 8 (800) 250-59-95
Факс: +7 (499) 639-00-80
E-mail: info@rsvo.ru