

С.Ю. Бутузов

**МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ БЫСТРОДЕЙСТВУЮЩИХ
АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ
СИСТЕМ ИНТЕГРАЛЬНОЙ БЕЗОПАСНОСТИ
ВЫСОКОРИСКОВЫХ ОБЪЕКТОВ**

Аннотация. Представлены методологические основы проектирования и оценки устойчивого функционирования автоматизированных информационно-управляющих систем (АИУС) интегральной безопасности высокорисковых объектов. Показано, что в качестве показателя качества и надёжности функционирования АИУС может являться величина и характер изменения информационной энтропии, зависящей от ряда физико-технических и информационных параметров системы. Особое внимание уделено проектированию подсистемы детектирования и сброса избыточного давления, возникающего при ЧС, обусловленных взрывами, как составляющей, обеспечивающей физическую устойчивость объекта.

Современный этап развития промышленного производства в Российской Федерации характеризуется усложнением технологических процессов. В настоящий момент времени активно развиваются такие отрасли промышленности как нефтеперерабатывающая, газовая, химическая, деревообрабатывающая, металлургическая и др. Предприятия данных отраслей промышленности относятся к высокорисковым объектам [1], на которых возможно возникновения техногенных чрезвычайных ситуаций (ЧС). По статистическим данным, ежегодно прирост техногенных ЧС составляет 30-35%. Основными причинами их возникновения являются:

- износ технологического оборудования;
- промышленный запуск неотработанных технологий;
- недостаточный квалификационный уровень персонала промышленного предприятия.

Повышение безопасности в техносфере может быть достигнуто за счёт обновления технологического оборудования высокорисковых объектов. Однако на это требуются существенные финансовые затраты, а также наличие необходимого промышленного потенциала, обеспечивающего производство нового технологического оборудования. Поэтому такой способ повышения техносферной безопасности в настоящее время нереализуем.

Реально повысить уровень обеспечения безопасности при возникновении техногенных ЧС возможно за счёт создания и внедрения на объектах *быстродействующих* автоматизированных информационно-управляющих систем (АИУС) интегральной безопасности высокорисковых объектов.

В настоящее время АИУС обеспечения безопасности высокорисковых объектов [1] формируются, используя принцип комплексного построения систем. При этом в неё включается большое количество (до 50-ти) подсистем, например, таких как:

- управление доступом на объект;
- защита от террористических действий;
- обеспечение пожаро- и взрывобезопасности;
- радиационная безопасность;

- химическая безопасность;
- экологической безопасности;
- и другие необходимые системы,

которые в аппаратном плане создаются по *дискретному* принципу. При этом анализ поступающей информации лицом, обеспечивающим безопасность объекта, осуществляется последовательно, исходя из установленной очереди поступления сообщений от подсистем. В этом случае при возникновении чрезвычайной ситуации система оперативно не может обеспечить безопасность промышленного персонала и технологического оборудования.

В случае возникновения чрезвычайных ситуаций, связанных с взрывами на высокорисковом объекте, определяющим становится такой фактор, как время реагирования на возникновение избыточного давления. Обеспечить безопасность при данных ЧС могут только быстродействующие автоматизированные информационно-управляющие системы обеспечения безопасности объектов.

Для повышения быстродействия автоматизированных информационно-управляющих систем интегральной безопасности научно обоснована [1] возможность их создания на единой программно-аппаратной и информационной базе. В таких системах, получивших название интегрированных, анализ информации, поступающих от подсистем, осуществляется в комплексе, одновременно от нескольких (в предельном случае, всех) подсистем.

Также при таком построении при необходимости информационный ресурс одной подсистемы или всех может быть перенаправлен для повышения эффективности функционирования другой подсистемы. Например, при воздействии избыточной освещённости на видеосистему подсистема управления доступом на объект на экране монитора перестаёт формировать контрастное изображение. Это происходит из-за того, что недостаточно мощности компьютерной составляющей АИУС для формирования контрастного изображения. Поэтому для его формирования необходимо увеличить производительность данной подсистемы за счёт дополнительного использования мощностей других подсистем. Такое перераспределение мощностей подсистем возможно только при построении их по интегральному принципу.

Однако, в работах [1,2], посвященных применению АИУС, отсутствуют научные основы проектирования, обеспечение надёжности и устойчивости функционирования таких систем. Решение данных проблем возможно на основе разработки специальных методов моделирования работы систем. Созданию методологических основ, включающих в себя данные методы и принципы построения отдельных элементов систем, а также действия персонала, обеспечивающего безопасность высокорискового объекта, посвящена настоящая работа.

Общий принцип построения *быстродействующей* АИУС обеспечения интегральной безопасности высокорискового объекта представлен в[3]. В её структуре предусмотрено наличие двух обязательных составляющих обеспечения безопасности: автоматической и автоматизированной систем. Система автоматического управления позволяет повысить устойчивость функционирования АИУС при возникновении ЧС, связанных со взрывами. Оно достигается за

счёт использования исполнительных элементов, имеющих физико-технические характеристики, существенно превышающие характеристики существующих элементов [5]. При дефлаграционном взрыве время срабатывания системы автоматического управления детектирование избыточного давления не должно превышать 0,1 мкс [6]. Таким образом, физическая устойчивость АИУС определяется данным параметром.

Устойчивое функционирование подсистем является одним из основных вопросов обеспечения интегральной безопасности высокорисковых объектов, которое необходимо уметь моделировать. При проектировании АИУС интегральной безопасности высокорисковых объектов необходимо использовать фрактальный принцип построения подсистем, что позволяет повысить её функциональную надёжность при дестабилизирующих факторах различного характера [4].

Моделирование работы сложных систем, к которым можно отнести и АИУС интегральной безопасности высокорисковых объектов, является эффективным методом их исследования. Такие системы характеризуются тем, что детерминированный характер, наблюдаемый при функционировании, сочетается со стохастической природой их отдельных элементов. Т. е. в системах можно выделить два уровня: микроуровень, где связи между элементами квазислучайные, и макроуровень, на котором связи между параметрами состояния чётко заданы. Взаимодействие между уровнями и(или) характер преобразования элементов на микроуровне зависит от конкретного вида связей. Для АИУС обеспечения интегральной безопасности высокорисковых объектов данной характеристикой является энтропия S информационных потоков системы [7]. Т.е. энтропия может выступать в качестве величины, характеризующей АИУС обеспечения интегральной безопасности высокорискового объекта. При превышении некоторой критической величины энтропии $S_{кр}$ система будет либо функционировать неустойчиво, либо полностью отказывать ($S > S_{кр}$).

Для случая построения автоматизированной системы по *дискретному* принципу она будет определяться как:

$$S_o = - \sum_{i=1}^n p_i \log_2 p_i \quad (1)$$

где S_o – энтропия дискретной автоматизированной информационно-управляющей системы обеспечения безопасности;

p_i – вероятность появления сигнала в i -том канале системы, включающей n подсистем.

Для АИУС, созданной по *интегральному* принципу, максимум информационной энтропии определяется как:

$$S_{um} = n \log_2 n \quad (2)$$

По разности величин информационных энтропий ΔS можно судить о том, какой принцип построения АИУС является более предпочтительным.

$$\Delta S = S_o - S_{um} = - \sum_{i=1}^n p_i \log_2 p_i - n \log_2 n > 0 \quad (3)$$

Из анализа выражения (3) следует, что более предпочтительной является построение АИУС по интегральному принципу. Данный вывод следует из условия минимизации энтропии системы ($S_o > S_{\min}$).

В случае, когда из n подсистем не задействованы m ($n > m$), то формула для расчёта энтропии, очевидно, приобретает вид:

$$S_{\min} = (n - m) \log_2 (n - m) \quad (4)$$

Из (4) следует, что при возникновении ЧС, например, обусловленных взрывами на объекте, функциональная стабильность АИУС обеспечивается за счёт отключения подсистем, которые не являются критичными и не используются в такой момент времени для обеспечения безопасности промышленного оборудования и технологического персонала объекта. Такие подсистемы должны быть определены заранее, чтобы при возникновении ЧС в автоматическом режиме могли быть отключены.

Определяя производную по времени выражения (1) и приравниваю её к нулю, получаем:

$$\begin{aligned} \frac{dS}{dt} &= - \sum_{i=1}^n \left(\frac{dp_i}{dt} \cdot \log_2 p_i + p_i \cdot \frac{d}{dt} (\log_2 p_i) \right) = - \sum_{i=1}^n \left(\frac{dp_i}{dt} \cdot \log_2 p_i + \frac{p_i}{p_i \cdot \ln 2} \right) = \\ &= - \sum_{i=1}^n \left(\frac{dp_i}{dt} \cdot \log_2 p_i + \frac{1}{\ln 2} \right) = 0 \end{aligned} \quad (5)$$

т.е. $\frac{dp_i}{dt} > 0$

Следовательно, степень неопределённости информационной составляющей в автоматизированной информационно-управляющей системе возрастает во времени, а, следовательно, возрастает информационная энтропия системы.

Характер изменения энтропии может быть различен (рис. 1). Линейный характер изменения энтропии (зависимость 2) характеризует удовлетворительную степень интеграции АИУС. В случае, если характер отличен от линейного (зависимости 1,3), то можно сделать вывод, что система функционирует неустойчиво, и при воздействии дестабилизирующих факторов различного характера может быть выведена из строя.

Для того, чтобы АИУС устойчиво функционировала необходимо, чтобы энтропия системы находилась на постоянном уровне, или (что даже более предпочтительно) во времени снижалась. Решением данной задачи может быть: использование более высокопроизводительных компьютерных систем, оптимизация построения специализированных баз данных АИУС, периодичность обновления информации в них и т.д. Также снижению энтропии способствует программно-аппаратная оптимизация подсистем АИУС интегральной безопасности высокорисковых объектов [3].

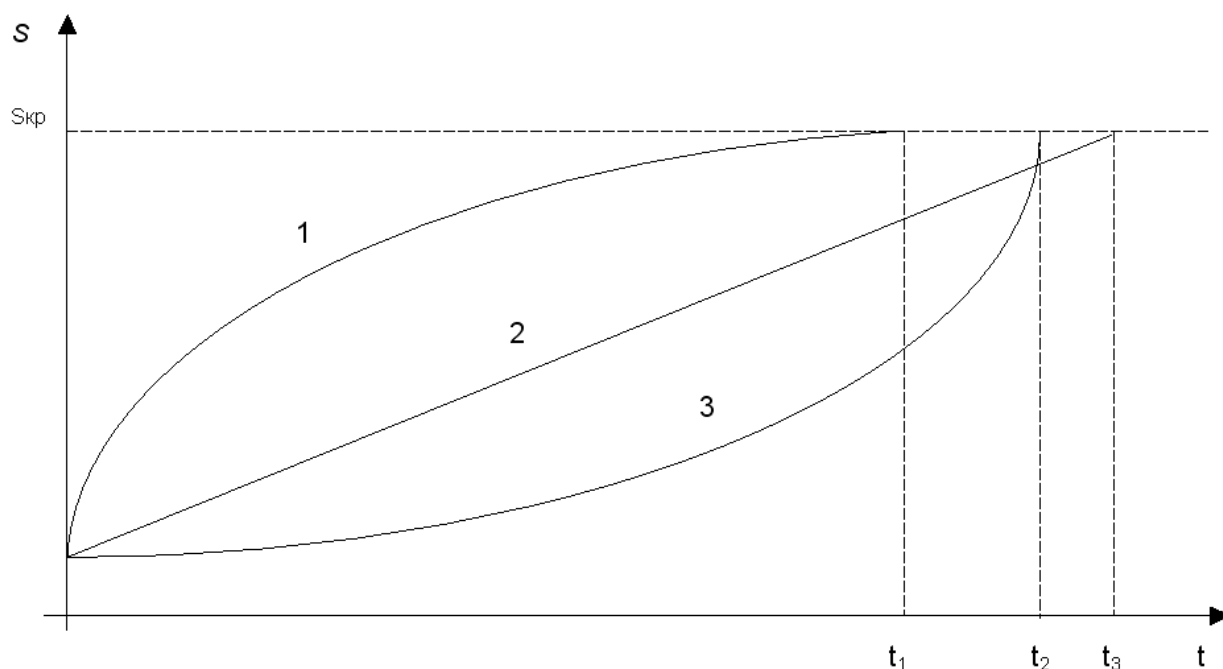


Рис. 1. Зависимости изменения энтропии АИУС интегральной безопасности высокорискового объекта во времени.

Примером интеграции подсистемы обеспечения безопасности является автоматизированная информационно-управляющая подсистема управления эвакуацией (УЭ) технологического персонала (рис. 2).

Данная подсистема в качестве составляющих нижнего уровня включает в себя инфракрасные (ИК-) датчики, расположенные по периметру производственных площадей и внутри технологических помещений объекта. Они предназначены для измерения температуры в различных локальных участках территории предприятия.

Контроллер системы ИК-датчиков обрабатывает поступающую первичную измерительную информацию и в режиме реального времени формирует на пульте управления оператора технологического процесса график распределение температуры на территории предприятия.

В случае возникновения ЧС лица, принимающие решения (ЛПР), имеют перед собой полную картину, характеризующую возможность организации безопасной эвакуации персонала из производственных корпусов и с территории объекта.

В этом случае автоматизированная система поддержки принятия решения по безопасному управлению эвакуацией предлагает ЛПР на выбор наиболее безопасные пути выхода с территории предприятия. Направления выбранных путей эвакуации указывается на специальных информационных табло, устанавливаемых на предприятии. Видеоинформация также должна сопровождаться аудио сообщениями.

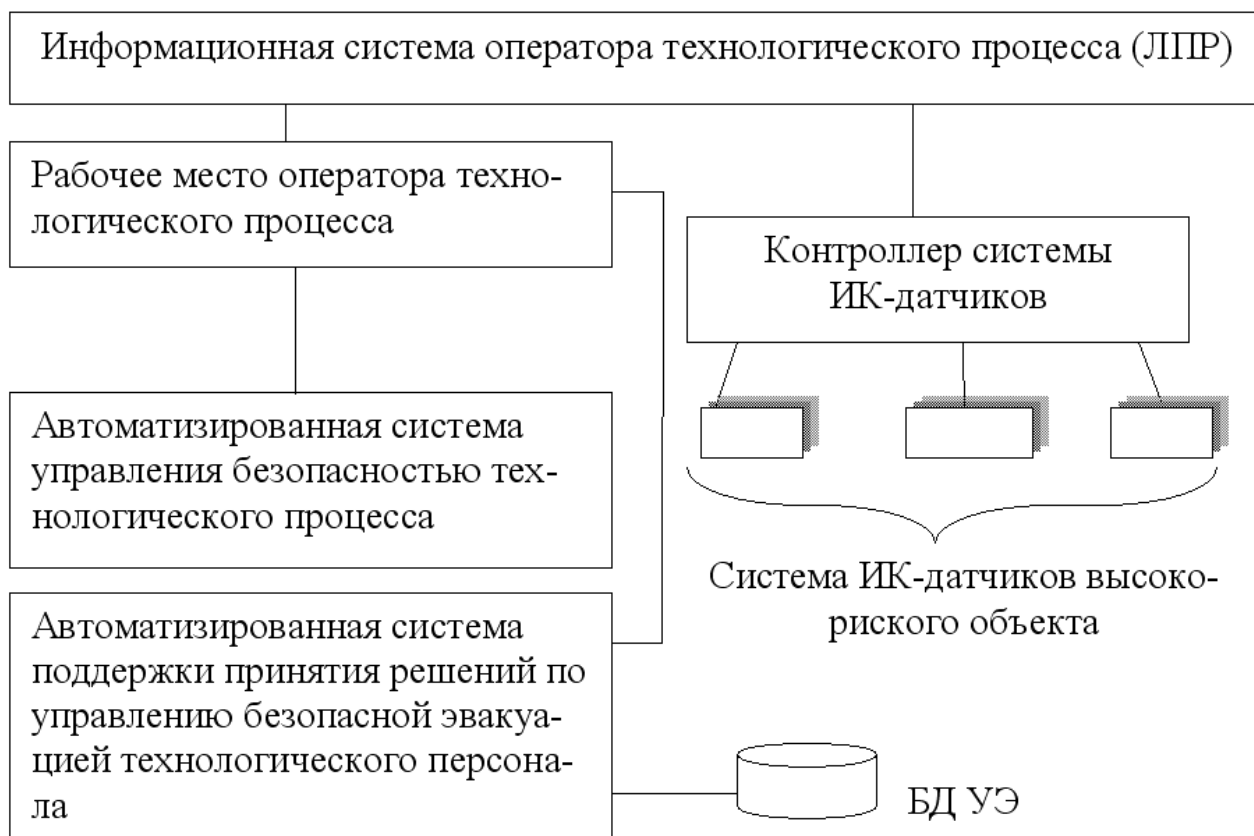


Рис. 2. Распределение информационных потоков в системе АИУС интегральной безопасности – система УЭ технологического персонала.

Процесс выбора оптимального решения опирается на информацию, содержащуюся в базе данных автоматизированной системы поддержки принятия решения по управлению безопасной эвакуацией технологического персонала при ЧС, которые включают в себя:

- возможные пути эвакуации, разработанных на основе прогностических моделей развития ЧС различного характера;
- расчётной динамики распределения температуры по территории предприятия в реальных масштабах времени.

Выбор путей эвакуации ЛПР следует осуществлять с учётом реальной обстановки, которая отражается на информационной панели.

Таким образом может быть интегрирована любая из подсистем обеспечения безопасности в АИУС интегральной безопасности высокорисковых объектов.

Представленные методологические основы проектирования и оценки надёжности АИУС интегральной безопасности высокорисковых объектов позволяют моделировать процесс функционирования и обеспечения безопасности при возникновении ЧС техногенного характера.

Литература

1. Топольский Н.Г., Блудчий Н.П. Основы обеспечения интегральной безопасности высокорисковых объектов. – М.: МИПБ МВД России, 1998.
2. Топольский Н. Г., Блудчий Н. П., Мосягин А. Б. Интегральная безопасность промышленно-технических объектов // Безопасность жизнедеятельности, №8, 2001.

3. Бутузов С. Ю. Энтропийный метод определения эффективности функционирования информационных каналов автоматизированных комплексных систем безопасности промышленных предприятий // Вестник Санкт-Петербургского университета ГПС МЧС России, №1-2 (11-12), 2006 – С.-П.: С.-П. университет ГПС МЧС России, 2006.
4. Бутузов С. Ю. Устойчивость функционирования каналов передачи информации автоматизированных комплексных систем безопасности // Там же.
5. Топольский Н. Г., Бутузов С. Ю., Членов А. Н. Тепловой пожарный извещатель // Патент на изобретение №2181505 МПК⁷ G08B17/06. - М.: ФИПС, 2001.
6. Ударные волны и экстремальные состояния вещества // Под ред.. Фортова В. Е. - М.: Наука, 2000.
7. А. Дж. Вильсон. Энтропийные методы моделирования сложных систем. – М.: Наука, ГИФМЛ, 1978.