

ИНФОРМАЦИОННАЯ БАЗА ПРОЦЕССА УПРАВЛЕНИЯ РИСКОМ

А. С. Оголихин

e-mail: andrew@bgd.tu-chel.ac.ru

Южно-Уральский государственный университет, г. Челябинск, Россия

Риск – количественная мера безопасности (опасности), в первую очередь позволяет специалисту оценить вероятность и возможные последствия нарушения работоспособности, с целью своевременного внесения соответствующих корректив, какого-либо из элементов сложной технической системы (промышленного предприятия), будь то установка, агрегат, процесс или даже человек, под воздействием как внутренних (нарушение трудовой дисциплины, износ оборудования и т.п.), так и внешних (природные явления, диверсии и т.п.) факторов. Для системы эти факторы – источники (реципиенты), объективно существующие и всегда присутствующие при формировании опасной ситуации, не что иное как достигшие определенной частоты и интенсивности возмущающие воздействия, оказывающие влияние на соответствие заданным процессам функционирования элементов системы и их устойчивость.

Основной трудностью при разработке информационного обеспечения процесса управления риском следует считать то, что одна и та же информация, отображающая процессы развития и возникновения опасных ситуаций, их взаимосвязь с производственными процессами, дает различный результат при рассмотрении с разных точек пространства и времени. Информация динамична и взаимосвязана по уровням и видам производственного процесса.

Если говорить об управлении безопасностью (риском) промышленного предприятия (частная задача в управлении сложным объектом) на основе информационных технологий, то необходимо четко представлять, что под информацией понимаются не любые сообщения, которыми обмениваются люди или передают их по техническим каналам связи, а лишь такие, которые уменьшают степень неопределенности у получателя. Неопределенность существует тогда, когда из-за неполноты информации необходим выбор одной из двух или большего числа возможностей. Такие процессы, в свою очередь, характерны при осуществлении функций связи и управления. Поэтому в данном случае будет иметь место подход с позиций вероятностного варианта математической теории информации [1, 2].

В тоже время говорить о работоспособности какой-либо системы управления можно лишь после того, как для нее разработана структура информационной базы, модель рассматриваемой предметной области (построение базы знаний управления риском на производственном объекте), обеспечена информационная совместимость элементов системы и, на основании этого, определен временной интервал реакции системы на происходящие в объекте управления изменения [3, 4].

При прочих равных условиях, как то: профессиональная пригодность и материальное обеспечение, в данной конкретной ситуации на вероятность принятия человеком правильного решения и совершения безошибочного поступка, в первую очередь, влияет качество и количество имеющейся у него на данный момент информации [5].

Современный уровень развития научных знаний в области информатики, к сожалению, не позволяет однозначно, численными методами охарактеризовать качество имеющейся информации. Все существующие методы такой оценки являются субъективными, относительными и ограниченными требованиями текущего момента [5]. Поэтому, общепринято считать более качественной ту информацию, которая характеризуется меньшим объемом и, при множестве возможных вариантов (альтернатив) решения поставленной задачи, позволяет выбрать наиболее верное и рациональное решение.

Так как процесс управления риском, как и всякий процесс управления, связан с процедурой принятия решения, т.е. с выбором одного из многих вариантов развития событий в сложившейся на данный момент ситуации, то необходимым условием своевременной и адекватной реакции субъекта управления на изменения в объекте является:

- наличие у субъекта управления (сотрудника службы охраны труда) объемов заранее запасенной и систематизированной информации, достаточно полно характеризующей

объект управления и окружающую его среду, а так же справочной, нормативно-методической информации по анализу риска;

- возможность корректировки информации в созданных базах данных;
- обеспечение субъекта управления необходимыми технологиями обработки информации, т.е. наличие алгоритмов сбора, хранения и поиска необходимой информации.

На основании вышесказанного, кажется возможным свести создание системы управления безопасностью (риском) на предприятии к организации на нем распределенной системы сбора и обмена данных, причем, учитывая потенциально возможные объемы информации, имеющей отношение к безопасности крупного промышленного объекта, эта система должна быть реализована на основе современных информационных технологий, в частности, с применением компьютерных сетей и передового программного обеспечения в области создания баз данных с максимально ориентированным на пользователя интерфейсом.

В связи с этим, ключевым этапом на пути создания системы управления риском становится разработка структуры ее информационной базы. Структуру создаваемой информационной базы должны составлять элементы, нацеленные на накопление и использование информации, содержащейся в банках данных по анализу риска (вид и структура этих банков подробно рассмотрены в [6]), для комплексного анализа безопасности производства. На рис.1 и 2 эти элементы названы “модулями”, что соответствует применяемой в информатике терминологии.

Сегодня в структурах информационных баз такого рода можно выделить три разновидности элементов-модулей. Первая из них – это модули 1 и 8 (рис. 2), в том или ином виде обязательные для информационного обеспечения деятельности любой службы (не только охраны труда), сотрудники которой активно работают с документацией. Вторая – модули со 2-го по 6-ой, составляют ядро информационного обеспечения служб охраны труда отечественных промышленных предприятий в ходе выполнения их сотрудниками своих основных, традиционных служебных обязанностей, независимо от того, выполняется на предприятии анализ риска или нет. Третий вид структурных элементов может быть представлен только одним модулем, на рис. 2 он обозначен как “Модуль “Анализ риска””. Фактически в нем содержатся шаблоны для проведения анализа риска, поэтому структура информационного взаимодействия этого модуля с другими элементами информационной базы определяется спецификой исходных данных, необходимых для информационной поддержки проводимых процедур анализа риска.

Основным преимуществом, а также доказательством правомочности именно такого подхода к разделению функций между компонентами, составляющими информационную базу и, как следствие, к построению ее структурной схемы, является то, что в этом случае создаваемое информационное обеспечение позволит найти комплексное решение задачи повышения уровня безопасности производственных процессов.

Так как, по существу, такую информационную базу будет составлять набор взаимодополняющих друг друга информационных моделей конкретного промышленного предприятия, посредством которых производство отображается как система “человек – машина – среда” с подсистемами “человек – безопасность производства” (модули 2 и 3), “машина – безопасность производства” (модули 4 и 5) и “среда – безопасность производства”, что на сегодняшний день признано наиболее правильным.

Учет влияния окружающей среды (природной, нормативно-правовой и т.д.) на безопасность производства частичного осуществления моделями, заложенными в модули 2 ... 5. Так же достаточные для анализа этой подсистемы объемы нормативно-правовой, административной информации содержатся в модуле 1. Необходимые процедуры объединения моделей всех трех подсистем осуществляются в два этапа: предварительного, в форме ретроспективного взгляда на события (модуль 6) и окончательного, в форме анализа риска как комплексного количественного показателя безопасности всей системы (модуль 7).

Следовательно, при таком структурном исполнении создаваемая информационная база будет являться своеобразным носителем, синтезатором моделей обеспечения промышленной

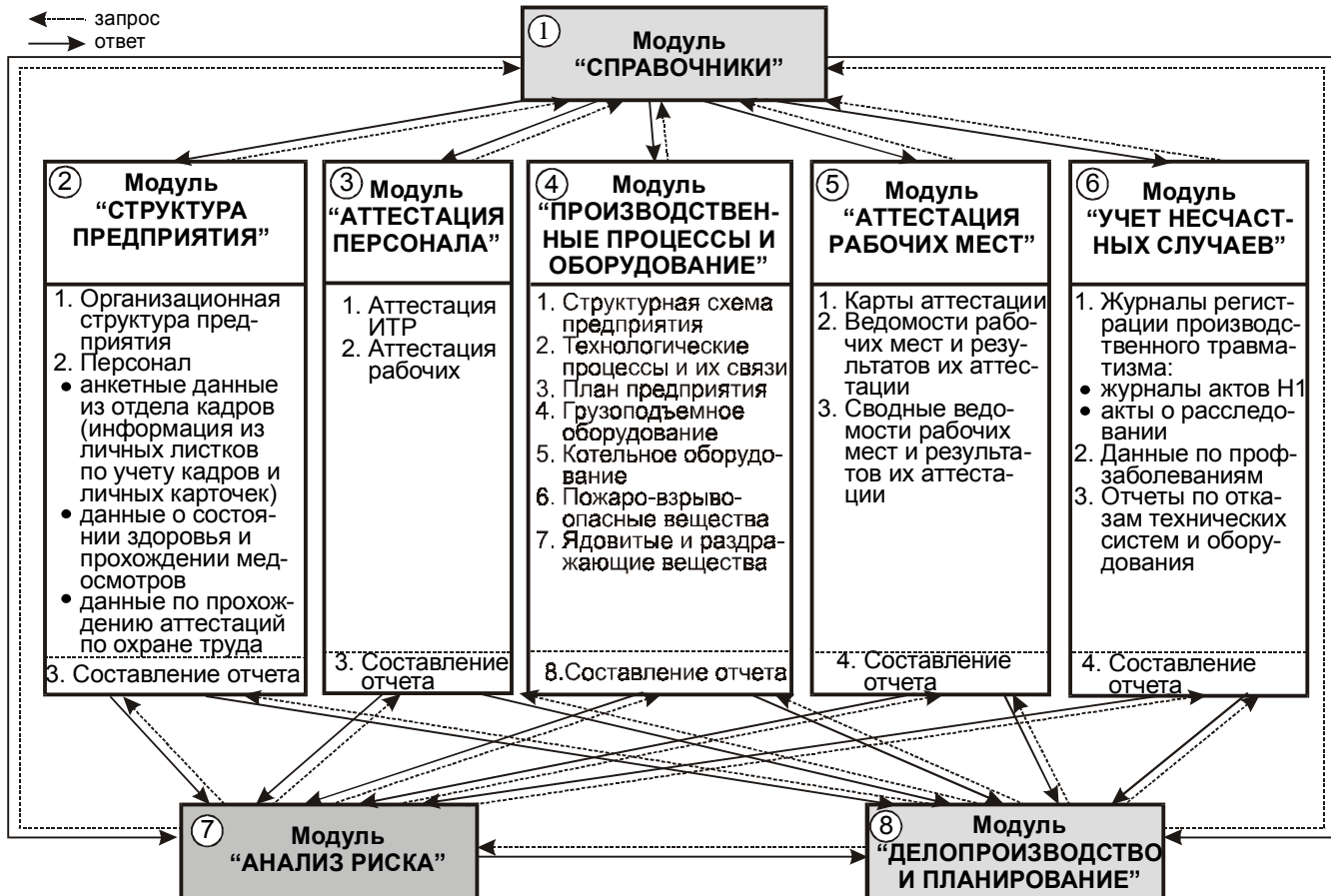


Рис. 1. Структура информационной базы процесса управления риском



Рис. 2. Модули "Справочники", "Делопроизводство и планирование" и "Анализ риска"

безопасности (моделей рассматриваемой в работе предметной области) в структуре информационного обеспечения системы управления риском на предприятии.

Время реакции системы управления риском на предприятии на изменения в объекте управления, при условии сформированных банков данных, в первую очередь будет зависеть от времени необходимого для проведения анализа риска сотрудниками службы охраны труда по той или иной, оптимальной для каждого конкретного случая, методике. Очевидно, что время такого анализа зависит от большого количества трудно учитываемых факторов, а именно опыта и числа исполнителей, характера объекта, требуемой точности и т.п.

В таблице 1, составленной на основании материалов источников [6, 7], приведены достаточно грубые значения необходимых затрат времени для основных методов анализа риска (считается, что анализ проводит группа из 3-х аналитиков).

Данные виды анализа применяются для принципиально разных условий и объектов, имеют различные сложность и исходную информацию, следовательно, они не могут сравниваться по скорости проведения.

Кроме того, в данном случае, вообще не совсем корректно ставить вопрос о времени реакции системы управления. В ходе анализа риска, основной процедуры управления, фактически определяются вероятность отказа того или иного элемента системы, а так же величина возможного ущерба. Концепция приемлемого риска изначально допускает возможность такого отказа в любой момент времени. Это означает, что всегда объективно существует вероятность неблагоприятного события (несчастного случая, аварии) и реализоваться это событие может раньше, чем в состоянии его выявить и предотвратить (снизить вероятность реализации) система управления риском.

Таблица 1

Время проведения анализа риска основными методами

	Методы анализа риска	Время анализа
1	Анализ дерева отказов	От 1 дня до 2 недель
2	Анализ дерева событий	От 1 дня до 2 недель
3	Анализ причинно-следственных связей	1...2 недели
4	Анализ человеческого фактора	1...2 недели
5	Анализ состояний отказов и их взаимодействия (FMEA)	От 1 дня до 2 недель
6	Исследование риска эксплуатации (HAZOP)	От 1 дня до 2 недель

Тем не менее, очевиден тот факт, что период существования (эксплуатации) большинства компонентов производства (персонал, технологическое оборудование, сооружения и т.п.) значительно больше двух недель, максимального по оценкам экспертов, срока необходимого для любого из методов анализа риска. Так же мировая практика [6, 7] свидетельствует, что затраты на проведение анализа риска существенно ниже возможных потерь, как экономических, так и социальных от несчастных случаев.

Вследствие этих причин, проведена ли оценка бысродействия системы управления риском или нет особой роли не играет, важным является лишь обеспечение ее элементами заданной точности анализа риска.

ЗАКЛЮЧЕНИЕ

Таким образом, определены основные условия эффективного функционирования системы управления безопасностью на промышленном предприятии основанной на концепции приемлемого риска (системы управления риском).

Для разработки структуры информационной базы процесса управления риском в работе выполнен анализ основных типов банков данных, необходимых для проведения анализа риска, анализ организационной структуры отечественных промышленных предприятий, а так же места в ней службы охраны труда.

Разрабатываемую в работе систему управления риском следует рассматривать как дополнение к уже существующей на промышленном предприятии системе управления, как новую, органично интегрированную часть его организационной структуры.

Помимо этого, предложены основные принципы построения информационного обеспечения для системы управления риском на предприятии, что и позволило разработать

принципиальную схему его информационной базы, с использованием существующих моделей обеспечения промышленной безопасности, показаны невозможность и отсутствие необходимости оценки быстрого действия этой системы.

ЛИТЕРАТУРА

1. Азгальдов Э. Г. Дескрипторный словарь по информатике / Науч. ред. А. И. Черный; ВИНТИ. – М: ВИНТИ, 1991. – 164 с.
2. Горский Ю. М. Системно-информационный анализ процессов управления / Отв. ред. В. А. Веников; АН СССР, Сиб. отд-ние, Сиб. энерг. ин-т. – Новосибирск: Наука, 1988. – 322 с.
3. Петров Е. Н. Производственная информатика. – М.: Изд-во ВЗПИ, 1990. – 178 с.
4. Абдуллаев А. А., Алиев Р. А., Уланов Г. М. Принципы построения автоматизированных систем управления промышленными предприятиями с непрерывным характером производства. Под ред. акад. Б. Н. Петрова. – М.: Энергия, 1975. – 440 с.
5. Бауэр Ф. Л. Информатика: Задачи и решения / Пер. с нем. М. К. Валиева и В. К. Сабельфельда; Под ред. А. П. Ершова. – М: Мир, 1978. – 355 с.
6. Хенли Э., Кумамото Х. Надежность технических систем и оценка риска: Пер. с англ. – М.: Машиностроение, 1984. – 528 с.
7. Harms-Ringdahl, L. Safety Analysis: Principles and Practice in Occupational Safety. Elsevier applied science, London, 1993.