ЗАЩИТА В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

УДК 614.8.008

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ОЦЕНКИ РИСКОВ ВОЗНИКНОВЕНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Артёмова А.Ю., к.э.н.,
доцент кафедры управления и организации деятельности в сфере гражданской зашиты,
Институт гражданской защиты Донбасса,
ГВУЗ «Донецкий национальный технический университет»

В статье изучены характеристики методологической базы управления рисками для определения основных методов, применимых для оценки риска чрезвычайных ситуаций. Представлено рассмотрение сущности риска как основного понятия теории и практики безопасности. Изучена концепция риск-ориентированного подхода как основа управления безопасностью объекта. Сформулирована общая стратегия управления безопасностью, которая базируется на соответствующих определениях риска, обеспечивающих практичность сравнения реальных уровней риска с целями, его значимость и наглядность. В результате выработана общая схема управления рисками предприятия на основе методик, наиболее приемлемых для оценки риска чрезвычайных ситуаций.

Ключевые слова: *опасность, безопасность, оценка риска, чрезвычайные ситуации, приемлемый риск, технократическая концепция, концепции риск ориентированного подхода, алгоритм управления риском.*

Постановка проблемы и ее связь с актуальными научными и практическими исследованиями. Безусловным аспектом существования любой системы или организации, особенно ярко выраженным на современном этапе развития мирового сообщества, является рисковая составляющая. В классических теориях риска утверждается, и небезосновательно, что риск – это яркая характеристика степени развитости общества. Стремительные темпы развития социумов, технических, информационно-коммуникационных и других видов систем и их трансформация приводят, соответственно, к возрастающему в геометрической прогрессии рисковому уровню всего окружающего нас пространства, и, в частности, увеличивающемуся риску возникновения чрезвычайных ситуаций. Система безопасности любого региона в целом или отдельного предприятия предусматривает анализ, планирование, прогнозирование развития возможных чрезвычайных ситуаций под влиянием различных факторов, их кумулятивного, транстерриториального и других эффектов. Это определяет необходимость оценки риска возникновения чрезвычайных ситуаций, их последствий и методов снижения риска для повышения уровня безопасности любых объектов, территорий.

Цель статьи – изучение современного инструментария управления безопасностью объектов на основе изучения характерных методологических особенностей системы оценки рисков возникновения чрезвычайных ситуаций.

Изложение основного материала исследования. Беспрецедентный рост числа аварий и катастроф в конце XX века, зафиксированный всеми важнейшими мировыми информационно-статистическими институтами, привел к необходимости коренного пересмотра принципов обеспечения безопасности. Как следствие, в промышленно развитых странах возникло новое важнейшее понятие в методологии оценки риска – концепция «приемлемого риска». Согласно выдвинутой концепции, опасности могут быть чрезмерными (недопустимыми) и приемлемыми (допустимыми). В целом такая стратегия реализовывается на практике в виде комплекса процедур по оценке и управлению рисками. Американская версия методологии дополнена распространением информации о рисках для обеспечения гласности на всех предусмотренных этапах. Оценка риска – это совокупность регулярных процедур анализа риска, идентификации источников возникновения риска, определения возможных масштабов последствий проявления факторов риска и определения роли каждого источника в общем профиле риска конкретного объекта. Основная стратегическая цель управления риском – снижение его уровня до приемлемого. Многообразие применяемых в практике методов управления риском представлено, на наш взгляд, четырьмя типами: методы уклонения от риска; методы локализации риска; методы распределения риска; методы компенсации риска.

Риск – основное понятие теории и практики безопасности. В соответствии с современным законодательством уровень безопасности определяется риском. Специалисты по безопасности предприятий должны быть компетентными во многих вопросах теории определения риска [1]. Формирование специалиста XXI столетия требует глубоких знаний методологии анализа риска сложных систем «человек – машина – окружающая среда» как современного инструментария управления безопасностью. Научный кругозор будущего специалиста как базис безопасности, знание методологии управления риском формируется в учреждениях высшего образования. Специальное образование является необходимым условием профилактики, предотвращения, предупреждения чрезвычайных ситуаций. Передовые сообщества настойчиво ведут поиски наилучших методов анализа и управление риском социально-экологических систем. Уже более 30 лет в развитых странах при принятии решений используются различные методы расчета риска. Создана

международная информационная сеть обмена данными по анализу рисков, выпускаются ежемесячные журналы, с информацией о риск-ориентированных методах расчетов [2]. Сказанное касается прежде всего потенциально опасных объектов (ПОО), АС в том числе. Разработано множество программ (расчетных кодов) по расчету рисков. Один из наиболее распространенных – код IRRAS (SAPHIRE), описанный в учебном пособии для специальности «атомная энергетика» [1]. Приведем коротко содержание основных понятий. Первое, и главное, понятийный аппарат относительно безопасности. Почему именно риск определяет уровень безопасности? Ранее во всех документах по безопасности, в законах в том числе, безопасность определяли как состояние защищенности человека, общества, окружающей среды. Но категория «состояние» может иметь только качественные уровни для сравнения: удовлетворительное – неудовлетворительное, высокий – низкий и т.д., а этого недостаточно для современного общества. Конечно, можно создать качественные шкалы для сравнения с дополнительными степенями качества, но в таком случае становится необходимым и словесное описание каждой степени сравнения. Для большого множества состояний разных по природе опасностей получаем неразрешимую задачу по реальному определению этого «состояния». Вот почему при необходимости детального описания опасностей человечество отказалось от такого (качественного) определения еще во второй половине прошлого века (начало 70-х гг.). Появилась необходимость более детальной классификации состояния безопасности, которая отображает бесконечное множество возможных состояний – количественное, числовое определение. Определение безопасности как допустимого риска предполагает возможность количественных и прогнозных расчетных значений опасностей. Действительно, риск как случайная величина имеет значение от 0 до 100 %, или единицы. Нуль отображает отсутствие риска, единица – достоверный, неизбежный риск. В диапазоне от 0 до 1 находится бесконечное множество чисел, существует возможность их натурального сравнения – вот причина перехода на новое определение.

В современном законодательстве принято такое определение: риск – количественная мера опасности, которая определяется функцией двух переменных – вероятности нежелательного события и ущерба от него. Мерой риска в обществе часто становится цена жизни человека (U = 1). Так, события, в результате которых один несчастный случай со смертельным исходом происходит на один миллион людей, обычно не замечаются в обществе (вероятность возникновения $P(t) = 10^{-6}$) – малый риск, а события, которые имеют частоту летального исхода $P(t) = 10^{-3}$ – очень большой риск, расцениваются как несчастные случаи. Раньше риск часто определялся как вероятность этого постулированного события (смерти), т.е. предполагалось, что риск – это относительная величина, которая всегда меньше единицы. Соответственно современным представлениям, риск – размерная величина, которая зависит от вероятности негативного (нежелательного) события и размеров его последствий. Наиболее просто риск можно измерять той же величиной, что и опасный фактор нежелательного события, т.е. летальными случаями. Другим общим измерением величины риска (как убытка) для всех нежелательных событий, служат деньги – прямые, непосредственные потери или затраты на устранение негативных последствий нежелательного события, умноженные на вероятность этого события. В таком виде имеем, на первый взгляд, противоречие с тем, что сказано выше – измерения риска числами, иногда большими единицы. На самом деле противоречия нет, в этом случае получаем стоимость рисков, которые также можно сравнивать, например, для опасностей разных предприятий или для разных опасных ситуаций одного предприятия. В государственном регулировании безопасности чаще используется первая единица измерения риска, международные организации (ВОЗ) устанавливают рекомендованные максимальные значения допустимого риска на уровне 5 на 10 000 человек в год ($5*10^{-4}$). Концепция управления безопасностью на основе определений риска имеет название риск-ориентированного подхода (РОП).

Основу концепции риск-ориентированного подхода в вопросах управления безопасностью составляет сравнение текущего уровня риска с допустимым, а методологией риск-ориентированного подхода служит вероятностный анализ безопасности (ВАБ). Результаты ВАБ могут быть использованы для определения значимости различных факторов, которые делают вклад в аварию, или для вывода относительно рисков, которые создают ПОО.

В последнем случае общепринято, чтобы решение о приемлемости риска базировалось на трех основных принципах.

1. Существуют уровни риска для отдельных лиц или общества в целом в связи с использованием технологий, которые не следует допускать безотносительно к их полезности. Такие уровни часто называют границами приемлемости.

2. Даже при риске меньше указанного уровня безопасность не может считаться абсолютной, и знания о том, как ее улучшить, никогда нельзя считать полными. Соответствующие действия включают постоянное стремление к снижению риска при условии, что усилие по достижению этих улучшений не являются необоснованно высокими.

3. На уровнях, существенно более низких в сравнении с границей приемлемости, риск настолько низкий, что его следует считать пренебрежимо малым для того, чтобы избежать ненужных затрат ресурсов, которые отвлекают внимание от важных проблем безопасности, которые могут привести к большему риску иного типа. Такой соответственно низкий уровень иногда называют минимальной границей.

Реализация этих принципов требует формулирования целей безопасности, которые базируются на соответствующих определениях риска, обеспечивающих практичность сравнения реальных уровней риска с целями, его значимость и наглядность. В качестве примера необходимости применения расчетов ВАБ в работе [3] приводится ссылка на проект Чернобыльской станции до аварии в 1986 г. Этот проект допускал

возникновение неконтролируемого переходного процесса с разрушением всех барьеров безопасности вследствие неправильного функционирования одной системы, а именно, системы управления реактивностью. Таким образом, если бы вероятностные оценки были сделаны, то рассчитанная вероятность тяжелых последствий зависела бы почти исключительно от таких величин, как отказ по общей причине системы управления или человеческая ошибка, т.е. авария в таком виде не могла бы состояться, благодаря своевременно принятым мерам.

Обозначим общепринятые определения сферы безопасности.

Риск определяется произведением вероятности возникновения возможного ущерба на ожидаемый размер ущерба.

Безопасность представляет собой приемлемый уровень риска относительно выгод, полученных из деятельности (активности) объекта, который подвергается риску.

Существуют две общих интерпретации вероятности.

Частотная вероятность (относительная частота или эмпирический подход), когда вероятность случая (события А) определенная формулой:

$$P(A) = \lim_{n..} (X/n), \quad (1)$$

где X – число случаев (событий «А»), которые реализовались из числа «n» повторенных испытаний.

Для фиксированного «n», величина P(A) – относительное частотное появление случая (события) «А». Итак, увеличение числа испытаний «n» улучшает оценку вероятности P(A).

Субъективный подход (подход «степени убеждения») определяет вероятность P(A) как величину неопределенности степени убеждения, что каждый «Субъект» имеет относительно случая (события) «А». Например, на основании знания симметрии для монеты, которая подбрасывается, можно предположить что, вероятность выпадения решки (верхней части) при подбрасывании – 0.5. Субъективный метод требует, чтобы вероятность была назначена способом, который согласуется с убеждением.

Надежность (*англ*. Reliability) – R – вероятность того, что система сработает удовлетворительно (т.е. безопасно) за соответствующий (определенный) период времени (24 часа или количество циклов) и в установленных условиях работы. Это определение соответствует международным стандартам и не совпадает с ДСТУ 2870.

Потенциально опасный объект – это объект, на котором могут использоваться или изготавливаются, перерабатываются, сохраняются или транспортируются опасные вещества, биологические препараты, а также другие объекты, которые при определенных обстоятельствах могут создать реальную угрозу возникновения аварии.

Случайной величиной X называется величина, которая характеризуется упорядоченным набором X = (X1, X2, …) действительных чисел (возможных значений) X1, X2, ... Каждому из этих возможных значений приписывается соответствующая вероятность реализации этого значения p1, p2, ... – распределение вероятности величины X.

Случайный процесс – это случайная функция x(t) от независимой переменной t. Каждое испытание дает определенную функцию X(t), что называется реализацией процесса или выборочной функцией. Случайный процесс можно рассматривать или как совокупность реализаций процесса X(t) или как совокупность случайных величин, которые зависят от параметра t.

Неопределенность случайной величины характеризует рассеивание значений случайной величины, которые наблюдаются вокруг ее среднего значения. Для нормального симметричного распределения случайной величины рассеяния описывается дисперсией D(y) и стандартным отклонением. Неопределенность значений связана с природой процесса, который исследуется, позволяет судить о статистических закономерностях процесса и не связана с ошибками измерений.

Изучим характеристики неопределенности. На практике, при вычислениях без использования специальных программ, используют статистические данные точечных значений вероятностей, упуская данные о типе распределения вероятностей исходных данных и их неопределенностях.

Рассмотрим значение знания факторов, которые характеризуют точность (неопределенность) статистических данных. Случайные величины с большей дисперсией как бы более размыты возле средних значений, диапазон значений их области существования более широкий, максимальные и минимальные значения более отдалены друг от друга. Отметим, что геометрически стандартное отклонение совпадает с расстоянием от среднего значения до точек перегиба кривой. Для случайной величины Y с нормальным распределением вероятности наблюдения обычно рассматривают три значения границ доверительного интервала ... 1; ... 2.; ... 3.; в эти интервалы попадает следующая часть значений соответственно: 0,683, 0,955, 0,997. Для приведенного примера и доверительной вероятности P = 95 % (диапазон … 2.) соответствующие доверительные интервалы будут: (0,0001; 0,0003) для 1 = 0,00005, (преимущество) (0; 0,0004) для 2 = 0,0001, (-0,0004; 0,0008) для 3 = 0,0003. Иными словами, с вероятностью 95 % случайная величина Y будет находиться в этих интервалах. Отметим, что в последнем случае, при 3 = 0,0003, ширина доверительного интервала превышает среднее значение случайной величины в шесть раз, т.е. данные с меньшими неопределенностями имеют большее преимущество, первоочередность. Кроме того, нижняя граница последнего интервала выходит за пределы допустимых значений – принимает отрицательное значение. На практике это означает, что интервал возможного значения переменной расширяется от нуля до четырехкратного значения.

Нормальное распределение играет очень важную роль в математической статистике. Оно описывает случайные величины, которые имеют лишь общие свойства: непрерывность значений, равновероятность симметричных относительно отклонений, большая вероятность малых отклонений от среднеквадратического отклонения.

Доверительный интервал – характеристика неопределенности или несовершенства в описании случайной величины, которая базируется на данном эмпирическом материале. В пределах доверительного интервала с заданной доверительной вероятностью можно найти значение величины, которая исследуется.

Далее рассмотрим в целом алгоритм управления риском.

В начале статьи упоминалось о концепции общего управления безопасностью – концепции риск-ориентированного подхода (РОП). В Украине эта концепция управления разработана много лет назад, но внедрена только в ядерной отрасли, на наш взгляд, по общим причинам политической нестабильности и безответственности. В концепции управления рисками изложены семь основных принципов государственного управления безопасностью в рыночных условиях: 1) приемлемости; 2) превентивности (предотвращение); 3) минимизации (АЛАРА); 4) полноты; 5) адресности (кто создает риск, тот и платит); 6) целесообразного значения приемлемых уровней; 7) информирование (декларирование). Эти семь принципов в развитых странах действительно обеспечивают надлежащей уровень безопасности.

Приведем краткое объяснение этих принципов.

1. Принцип приемлемости риска, состоит в определении и достижении в государстве социально, экономически, технически и политически обоснованных нормативных значений рисков для населения, окружающей природной среды и объектов экономики.

2. Принцип превентивности предусматривает максимально возможное и заблаговременное выявления опасных значений параметров состояния или процесса и инициирующих событий, которые создают угрозу возникновения чрезвычайных ситуаций, и применение конкретных мероприятий, направленных на нейтрализацию этой угрозы и/или смягчения ее последствий.

3. Принцип минимизации риска, согласно которому риск чрезвычайной ситуации необходимо снижать настолько, насколько это возможно, добиваться достижения разумного компромисса между уровнем безопасности и размером затрат на ее обеспечение. Принцип минимизации риска еще известен как принцип АЛАРА: «Всякий риск должен быть снижен настолько, насколько это практически достижимо или же до уровня, который настолько низок, насколько это разумно достижимо».

4. Принцип полноты, соответственно которому риск для жизнедеятельности человека или функционирование любого объекта является интегральной величиной, которая должна определяться с учетом всех угроз возникновения аварий и/или чрезвычайных ситуаций с учетом человеческого фактора.

5. Принцип адресности, который заключается в том, что риском должен управлять тот, кто его создает.

6. Принцип выбора целесообразного значения риска, соответственно которому субъект управления риском обеспечивает в пределах от минимального до предельно допустимого такое значение риска, которое он считает целесообразным, исходя из имеющихся у него экономических, технических и материальных ресурсов и существующих социальных и политических условий; субъект хозяйствования, выбирая целесообразное значение риска, гарантирует определенный уровень безопасности для населения и уплату страховых выплат, если авария произошла.

7. Принцип обязательности информирования, который заключается в том, что каждый субъект управления риском обязанный регулярно предоставлять органам государственной власти и местного самоуправления реальные значения рисков.

Выводы и перспективы дальнейших исследований. Управление рисками чрезвычайных ситуаций техногенного и природного характера должно рассматриваться как неотъемлемая часть государственной политики национальной безопасности и социально-экономического развития государства, одной из важнейших функций всех органов исполнительной власти и субъектов хозяйствования всех форм собственности и может осуществляться на основе указанных выше принципов, аккумулируя лучшие достижения человечества во всех областях производства.

Цель управления риском при осуществлении деятельности потенциально опасного объекта и АЭС можно определить как обеспечение безопасности персонала, населения и окружающей природной среды путем установления и поддержания приемлемого уровня риска при использовании оптимальным образом с максимальной эффективностью имеющихся материальных ресурсов.

Таким образом, управление рисками – это деятельность, связанная с идентификацией, анализом рисков и принятием решений, направленных на минимизацию отрицательных последствий наступления исходных событий (явлений) и/или уменьшение вероятности их реализации до приемлемых значений. В общем случае процесс управления рисками при осуществлении деятельности на объекте включает выполнение шести процедур и постоянный мониторинг и контроль:

1) планирование управления рисками;
2) идентификация рисков;
3) качественная оценка рисков;
4) количественная оценка рисков;
5) планирование реагирования на риски;

6) реализация принятого решения;

7) мониторинг и контроль.

Планирование управления рисками – это процесс принятия решений по применению методологии РОП для конкретной деятельности.

Исходя из вышесказанного, этот процесс может включать в себя:

- организацию на объекте специального подразделения (группы управления рисками), ответственного за оценку и управление рисками;
- выбор методики оценки рисков;
- определение источников данных для идентификации рисков;
- определение интервала времени для анализа ситуации (аварии).

Очень важным является определение допустимых (приемлемых) уровней риска, которые определяются на основе действующего законодательства.

Идентификация рисков определяет, какие риски могут повлиять на рассматриваемый вид деятельности. Характеристики этих рисков должны быть оформлены документально. Идентификация рисков должна проводиться регулярно на протяжении всей деятельности объекта. Специализированное подразделение должно привлекать к работам по идентификации рисков всех участников процесса: проектировщиков, эксплуатационников, специалистов других подразделений и независимых экспертов. Идентификация рисков организовывается как итерационный процесс. Первые расчеты потенциального риска выполняют проектировщики. В процессе деятельности объекта, с учетом опыта эксплуатации, уточняются данные по надежности систем и оборудования, процедурам управления, ошибкам персонала и делается перерасчет рисков для объекта. Для формирования объективной оценки в завершающей стадии процесса оценки могут принимать участие независимые эксперты. Пример идентификации рисков (для радиационных рисков) изложен в государственном нормативном документе НРБУ-97/Д-2000 (Украина).

Качественная оценка рисков – это процесс качественного анализа результатов идентификации, а также определение событий, которые вносят наибольший вклад в общий риск и требуют принятия мер по снижению риска. Качественная оценка определяет степень важности риска и составных его событий. Целесообразно создать банк данных рисков всей деятельности на объекте, основанный на систематизированных данных, в том числе данных по влиянию рисков на персонал. На этом этапе возможно определение факторов наибольшего влияния, которое создаст предпосылки управления.

Количественная оценка рисков определяет значение вероятности возникновения рисков и влияния их последствий на деятельность, которая помогает принимать оптимальные решения и избегать неопределенности (в смысле управления) при этом. Количественная оценка рисков предусматривает выполнение предыдущих процессов, это завершающий этап задачи определения рисков. Важный этап качественного анализа систем заключается в представлении условий невыполнения функций системы в виде так называемого множества минимальных сечений. Набор минимальных сечений системы однозначно определен ее деревом отказов и может быть получен при использовании специальных алгоритмов выбора минимальных сечений, который составляет наиболее важную задачу расчетного кода. Заметим, что при расчете точечной вероятности нежелательного события с помощью ДО вручную или с помощью калькулятора мы не получаем набора минимальных сечений системы, т.е. теряем чрезвычайно важную информацию для управления риском. Действительно, если известно, какие события оказывают наибольшее влияние на риск, то задача управления сводится к тому, чтобы уменьшить влияние этих событий любым способом. Если это невозможно, или слишком дорого, то необходимо создавать специальные системы безопасности, назначением которых являются ограничения отрицательного действия нежелательного события, или прекращение опасного процесса на каком-то промежуточном этапе. Количественные данные по базисным событиям влияют на важность самого минимального сечения – его процентный вклад в вероятность отказов системы.

Планирование реагирования на риски – это разработка методов и технологий снижения отрицательных последствий рисков. Качественное, научно обоснованное планирование возможно при условии выполнения всех предыдущих этапов процесса соответственно. Стратегия планирования должна отвечать типам рисков, их величине и значимости, наличию ресурсов и временных параметров. В наиболее опасных случаях целесообразно предусматривать несколько вариантов реагирования на риски.

Планирование должно осуществляться в соответствии со специальной методикой, которая учитывает специфику объекта, действующие на нем правила и инструкции.

Реализация принятого решения осуществляется как заключительный этап всей работы по управлению рисками на основе предыдущего планирования. Это могут быть действия, которые должны быть выполнены немедленно, или на протяжении какого-то непродолжительного срока, или долгосрочные мероприятия, которые нуждаются в значительных материальных ресурсах. В некоторых случаях реализация принятого решения контролируется государственными надзорными органами – инспекциями. В случае если объект создает угрозу, которая превышает принятые уровни риска, нужно осуществлять мероприятия модернизации технологий, или оборудования или вообще прекращать его деятельность.

Мониторинг и контроль параметров проводятся с целью проверки соблюдения требований установленных норм. Мониторинг и контроль должны осуществляться специализированным подразделением объекта. При этом постоянно контролируется процесс идентификации рисков, выполнение плана реагирования на риски, оценка эффективности мер по снижению рисков, величина остаточного риска и его приемлемость.

Качественный контроль выполнения деятельности дает информацию, которая оказывает содействие принятию эффективных решений по предотвращению новых рисков или смягчение последствий. Контроль может инициировать выбор альтернативных стратегий, принятие изменений, перепланирование проекта для достижения базового плана.

При организации управления риском, разработке предложений относительно принятия управленческих решений для обеспечения наглядности, удобства проведения оперативных расчетов риска целесообразно наносить на карты информацию о зонах риска на объекте. Под зонами риска понимают помещение и территории, которые ограничены изолиниями, которым отвечают определенные уровни риска. Установление зон риска имеет важное практическое значение. Особенно велика роль этих зон при анализе, оценке обстановки и принятии решения в аварийных условиях.

Для целей мониторинга и проверки соблюдения норм предусматривается необходимое оборудование и внедряются соответствующие процедуры проверки. Указанное оборудование надлежащим образом обслуживается и испытывается, а также калибруется с надлежащей периодичностью на основе эталонов, которые отвечают национальным или международным стандартам.

Все оговоренные процессуальные моменты стратегической деятельности руководства любым объектом в свете оценки рисков возникновения чрезвычайных ситуаций являются основой и содержанием управления безопасностью его функционирования.

Библиографический список

1. Бегун, В.В. Вероятностный анализ безопасности атомных станций [Текст] / В.В. Бегун, О.В. Горбунов и др. – Киев: НТТУ КПИ, 2000. – 558 с.
2. Risk Excellence Notes. U.S. Department of Energy. Argonne, 2000.
3. Вероятностный анализ безопасности №75 – INSAG – 7. Доклад международной консультативной группы по ядерной безопасности: серия изданий по безопасности МАГАТЭ – Вена: МАГАТЭ, 1994. –147 с.

bgdicz_artyomova@mail.ru
Рецензент к.т.н., доц. М.Б.Старостенко

HAZARD EXPECTATION BASED SAFETY AND HEALTH CARE CONTROL APPROACHES FOR EMERGENCY CASES

Dr. **A.Y. Artyomova,** Ph.D. (Econ.),
IGZD, DonNTU

In this article we study characteristics methodological base of risk management to identify the main methods applied to assess the risk of emergencies. Presents a consideration of the notion of risk as the main concepts of the theory and practice of security. Studied the concept of a risk - based approach as a basis for safety management of the facility. Formulated the overall strategy for safety management based on the relevant definitions of risk, ensuring the practicality of comparing actual risk levels with the purpose, its significance, and clarity. As a result of a General scheme of enterprise risk management on the basis of the techniques most appropriate to assess the risk of emergencies.

Keywords: *hazard, safety, risk assessment, emergency, reasonable risk, technocratic concept, the concept of risk-oriented approach, the algorithm of risk management.*