ОТ СТРАТЕГИИ К ПРАКТИКЕ УПРАВЛЕНИЯ РИСКОМ

А. Д. Еремин, *кандидат философ. наук,* ***В. Г. Ялозо***

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров

1. Стратегии управления рисками

Объект и угроза являются ключевыми характеристиками, которые должны быть включены в процесс управления риском, однако, необходимо отметить, что система безопасности должна быть объектоцентрируема, т.е. без существования объекта не существует и угроз объекту. Определение пространства угроз объекту может быть получено только через объект. В противном случае, алармистские фантазии могут сделать пространство угроз объекту бесконечным и «раздеть страну», в желании обеспечить безопасность обществу и государству.

Угрозы находятся в динамике, они постоянно изменяются, да и сам объект во времени проходит различные жизненные циклы. Исторически сложившаяся практика обеспечения безопасности, как правило, базируется на том, что требования безопасности определяются, разрабатываются и утверждаются после того, как произойдет какой-нибудь инцидент с объектом, т.е. требования безопасности базируются на приобретенном опыте эксплуатации объекта, а безопасность объекта акцентирована на ликвидации последствий. Такой подход не вызывает беспокойства, когда фактически динамика угроз не наблюдается, когда ущербы не существенны. Если же динамика угроз возрастает, ущербы могут быть громадными, такая практика в обеспечении безопасности недопустима. Возникает вопрос: «Как в процессе управления риском оптимально распределить ресурсы, обеспечивающие безопасность, чтобы достигнуть приемлемого риска?». Хотя наш тезис об объектоцентрированности систем обеспечения безопасности предполагает начинать с объекта, но это необходимо делать при управлении риском конкретного объекта, а при системном подходе рассмотрения аспектов управления риском, лучше начать с угроз.

Рис. 1. Структура угроз

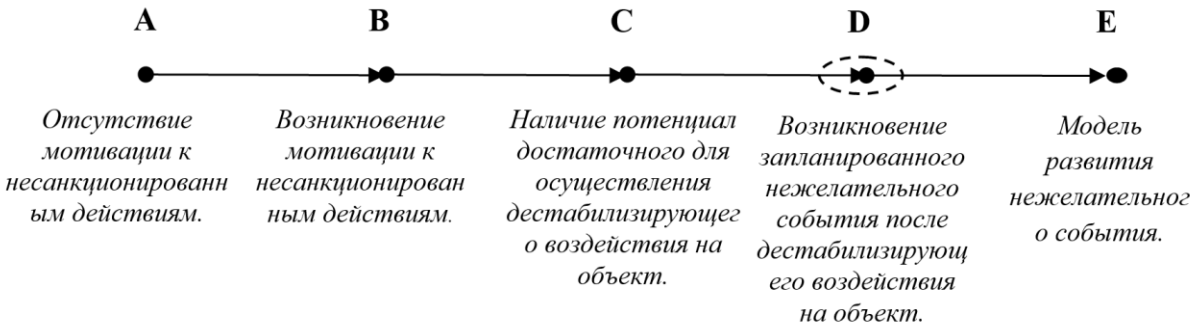

Рис. 2. Фазы развития и реализации угрозы «действия людей»

По нашему мнению, угрозы являются базовым компонентом системы безопасности и их классификация может быть представлена следующей структурой:

Каждую угрозу можно оценивать:

- по степени неопределенности, которая существует в процессе анализа ее возникновения и развития;
- по динамике увеличения потенциала угрозы во времени и пространстве;
- по возможным сценариям реализации угрозы по отношению к объекту.

Наиболее сложными являются угрозы, относящиеся к классу «действия людей». Особенно, «дурной неопределенностью» обладают угрозы «умышленные действия людей». Имеет смысл, по нашему мнению, отдельно остановиться и рассмотреть фазы развития и реализации этой угрозы.

Фазы: «**AB**» и «**BC**» – будут составлять этап подготовки к реализации дестабилизирующего воздействия на объект. Фаза: «**CD**» – осуществление дестабилизирующего воздействия по отношению к объекту. Фаза: «**DE**» – последствия дестабилизирующего воздействия. Наиболее значимой точкой в процессе развития и реализации угрозы является точка-репер «**D**». Данная точка определяет возникновение запланированного предполагаемыми злоумышленниками нежелательного события, т.е. если это событие возникло, тогда можно считать, что угроза по отношению к объекту реализована.

Как видно из схемы реализации угрозы, поле деятельности по управлению риском очень широкое и не сводится только к ликвидации последствий чрезвычайной ситуации, которая может возникнуть на объекте. На каждой фазе возникновения, развития и реализации угрозы необходимо управлять риском. Суть управления сводится к задаче – как оптимально распределить ресурсы (которые не бесконечны), чтобы добиться максимально снижения риска?

В процессе управления риском должен присутствовать объект. Он, также как и угроза, проходит фазы развития и на каждой фазе он, в определенной степени, чувствителен к возможной угрозе. В процессе жизненного цикла объекта могут быть выделены следующие фазы:

- предпроектный этап (разработка концепции и ТЭО, прохождение экспертиз);
- проектирование и конструирование;
- строительно-монтажные и пусконаладочные работы;
- эксплуатация и вывод из эксплуатации (утилизация).

Управление риском на этапах развития объекта должно включать в себя оценку чувствительности объекта к возможным угрозам и внесение коррективов: в проект, конструкцию, создание объекта (строительство) – с целью снижения чувствительности объекта к возможным угрозам. Если будет создан высокочувствительный объект к возможным угрозам, тогда на этапе его эксплуатации, потребуется на много больше ресурсов для поддержания приемлемого риска. В конечном итоге, управления риском будут включать в себя выполнение следующих задач:

• минимизация возможностей возникновения и развития угроз;

• минимизация чувствительности объекта к угрозам;

• максимизация защищенности объект;

• максимизация смягчения последствий, в случае реализации угрозы.

При управлении риском важную роль играю выбранные стратегии управления риском:

• уменьшение риска;

• ограничение риска;

• уклонение от риска;

• передача риска;

• страхование риска.

•

Уменьшение риска. При этой стратегии ресурсы, обеспечивающие безопасность, направляются на этап ликвидации последствий, которые могут наступить после реализации угрозы объекту. Самая неэффективная и затратная стратегия.

Ограничение риска. Суть ограничения риска, это создание физической защиты объект, т.е. контроль и ограничение доступа на объект. В некоторых случаях при проектировании объекта можно достигать таких ограничений в доступе, которые по эффективности могут превосходить, надстраиваемую физическую защиту на объекте. Затратив ресурсы на этапе проектирования объекта, впоследствии, можно не тратить ресурсы на создание и функционирование физической защиты объекта.

Уклонение от риска. Простой подход, заключающийся в том, что просто не выполнять рискованных задача и не совершать рискованных действий.

Передача риска. Передать выполнение рискованных задач тому, у кого риск меньше при выполнении этих задач.

Обеспечение безопасности строится на различных принципах и моделях безопасности. Можно выделить три типичные модели управления безопасностью:

• программное управление;

• программно-адаптивное управление;

• управление по схеме «предиктор – корректор».

Программное управление:

• разрабатывается определенная программа безопасности, которая потом реализуется в процессе функционирования системы безопасности;

• данная программа адекватна ситуации в сфере безопасности на момент разработки программы;

• в процессе выполнения программы состояние объекта и состояние угроз объекту не контролируется, т.е. обратная связь, отражающая состояние безопасности отсутствует;

• уровень качества управления зависит от того, насколько программа соответствует реальным условиям;

• гибкость управления отсутствует.

Программно-адаптивное управление:

• при выполнении программы контролируется функционирование объекта и состояние его структуры, учитываются и возможные угрозы объекту, т.е. существует обратная связь, отражающая по контрольным параметрам состояние безопасности объекта с учетом внешней среды и состояния объекта;

• в данной модели со временем накапливается ошибка по рассогласованию относительно контрольных параметров (например: изменение угроз), если они не корректируются в процессе управления;

• инерция в сфере принятия решений, что приводит к запаздыванию принятия решений по распределению ресурсов для обеспечения безопасности объекта (имеется фазовый сдвиг между возмущением и компенсирующим воздействием на это возмущение).

Таблица 1

Модели управления риском и задачи безопасности

Задачи безопасности	**Программное управление**	**Программно-адаптивное управление**	**Предиктор-корректор**
Прогноз изменения вне внешней среды (угрозы)	*Не выполняется*	*Не выполняется*	*Мониторинг внешних угроз с определением динамики их развития*
Прогноз изменения внутренней среды объекта (уязвимость объекта)	*Не выполняется*	*Не выполняется*	*Мониторинг внутренних угроз с определением динамики их развития*
Оценка состояния внешней среды	*Не выполняется*	*Выполняется на основе реализации угроз в прошлом*	*Определение потенциала внешних угроз*
Оценка состояния объекта	*Не выполняется*	*Выполняется по критериям с учетом реализации угроз в прошлом*	*Оценка уязвимости объекта на основе потенциала и динамики развития внешних и внутренних угроз*
Реагирование на угрозу	*Реагирование на угрозу в процессе ее реализации*	*Реагирование на угрозу в процессе ее реализации*	*Распределение ресурсов безопасности с учетом динамики развития угроз и уязвимости объекта с целью реагирования на угрозу в будущем*
Реагирование на последствия после реализации угрозы	*Ликвидация последствий реализации угрозы*	*Ликвидация последствий реализации угрозы*	*Ликвидация последствий реализации угрозы*

Предиктор-корректор:

- управление базируется на информации о текущем и прошлых состояниях среды и объекта с учетом прогнозирования тенденций и изменений, которые могут привести к отклонениям от принятого допустимого риска;
- система безопасности реагирует не только на уже свершившиеся отклонения, но и на отклонения, которые только имеют тенденцию к осуществлению в будущем.

2. Методология управления рисками

Технические системы становятся все более сложными, возрастает количество элементов и уровней иерархии конструкции. В инженерно-технической деятельности нельзя избежать объективно существующей неопределенности свойств конструкции и характеристик процессов индустриального производства (характеристик материалов и размеров, параметров процессов и т. д.), которая компенсируется допусками. Эта неизбежная погрешность (неопределенность) традиционно компенсируется коэффициентами запаса, но в условиях рыночной экономики здесь заложено концептуальное противоречие. Рыночная конкуренция требует сокращения до минимума всех коэффициентов запаса, а товар (изделие) в идеале должен превратиться в «*прах*» с минимумом отходов на следующий же день после окончания срока гарантии.

Выход предложен в концепции допустимого риска. Неизбежный допуск (погрешность) должен обосновываться и устанавливаться на проектном этапе для всех остальных этапов жизненного цикла изделия (включая эксплуатацию), а ошибки пер-

сонала должны исключаться за счет требований к компетенции персонала. При этом становится возможным отделить два типа неопределенности (вероятности) – допустимые неопределенности (риски) в природных и техногенных процессах от ошибок человека. В настоящее время методология оценки допустимого уровня рисков при разработке изделия (технологии, производства) нормируется научно-техническим сообществом, а ответственность за принятие конкретного решения в рассматриваемых проектных и запроектных авариях лежит в основном лично на проектировщике, что делает его позицию слабо защищенной от претензий общества (зачастую справедливых) о некомпетентности, субъективизме, коррупционности. При этом обостряется роль человеческого фактора в безопасности. Поэтому принятое понятие о допустимом уровне риска, оставляющее неопределенность в степени субъективности проектировщика не достаточно для снятия проблемы человеческого фактора при проектировании.

Возможность дальнейшего продвижения в решении названной проблемы видится в уточнении понятия риска. В Федеральном законе «*О техническом регулировании*» понятие риска введено как допустимая вероятность ущерба с учетом тяжести его последствий. Исходя из данного подхода, события, по уровням тяжести последствий от ущерба от их реализации, могут быть разделены на зоны ответственности:

- эксплуатационные затраты предприятия;
- область коммерческого страхования;
- зона рисков отраслевой ответственности;
- уровни риска, относимые к ответственности государства.

Смягчить субъективность принятия проектных решений можно за счет законодательного установления государством уровня предельно допустимого риска, который нельзя превышать при проработке каких-либо проектных решений. Совместными решениями государства, производственного (отраслевого) и страхового сообществ устанавливается граница между областями эксплуатационных затрат, коммерческого страхования и отраслевых рисков. На основе такого понимания риска можно построить инструментарий оптимизации рисков при проектировании предприятия, а также при его эксплуатации. Для этого представим[1] риски в форме функционала (1), позволяющего производить оптимизацию интегрального риска на основе поиска экстремумов по его существенным частным составляющим:

$$R = R\,(W, Y) \ldots\ldots\ldots\ldots . \quad (1)$$

где: R – риск от реализации единичного события в заданный период времени;
W – вероятность причинения вреда объектам защиты от рассматриваемого события;
Y – ущерб, определяющий тяжесть вреда для объекта защиты от реализации события.

Управление рисками осуществляется за счёт целенаправленного изменения вероятности и/или потенциального ущерба конкретных событий до достижения по всем источникам риска оптимальности в интеграле функционала R = R (W, Y, Z, t) как состояния предприятия с минимальными потенциальными потерями. Предлагаемый подход позволит установить четкие границы полномочий и ответственности проектировщика в проектном решении при допускаемом уровне природных и техногенных рисков и, соответственно, разделить риски на зоны ответственности проектировщика и эксплуатационных служб, конкретизировать влияние человеческого фактора на безопасность предприятия в форме ошибок при проектировании или при его эксплуатации.

[1] Подробнее см.: *Еремин А.Д.* Управление техногенными рисками как система / Экологическая и промышленная безопасность: Сборник материалов 3 сессии школы-семинара. – Саров: РФЯЦ-ВНИИЭФ, 2004. С. 49-61.

Если подвести черту под излагаемым материалом, тогда можно с определенной долей уверенности констатировать: **необходимым условием** эффективного управления риском объектов является управление безопасностью на основе модели «предиктор-корректор», а **достаточные условия** включают в себя следующие тезисы:

1. Угрозы субъективны по форме и объективны по содержанию. Выделение угроз происходит на основе интересов, действующих субъектов. Структура интересов субъектов включает в себя следующие уровни интересов: личные, корпоративные, системные. В системах безопасности должны доминировать системные интересы субъектов, а не корпоративные и личные. В противном случае, система безопасности, построенная на личных и корпоративных интересах, со временем приведет к развалу всей системы безопасности.

2. Система безопасности строится на основе принципа «объектоцентрированности» – нет объекта, нет угроз объекту.

3. Степень чувствительности объекта к возможным угрозам определяется на этапах проектирования, конструирования и создания объекта. На этапах конструирования и проектирования затраты на выполнения задач намного меньше, чем затраты, которые будут необходимы для обеспечения безопасности объекта на протяжении его жизненного цикла (затраты на функционирование физической защиты объекта).

4. Физическая защита объекта разрабатывается только на основе анализа возможных угроз. В противном случае невозможно определить адекватность физической защиты относительно безопасности. Физическая защита будет либо недостаточной, либо избыточной. В этих случаях объективный уровень допустимого риска не может быть определен.

5. Угрозы и уязвимость объекта учитываются при утилизации и ликвидации объекта, т.к. на этом этапе могут реализовываться угрозы по отношению к объекту. На данном этапе могут наступить более тяжелые последствия после реализации угроз, чем на этапе функционирования объекта;

Управление рисками осуществляется за счёт целенаправленного изменения вероятности и/или потенциального ущерба конкретных событий до достижения по всем источникам риска оптимальности в интеграле функционала $R = R(W, Y, Z, t)$ как состояния объекта защиты с минимальными потенциальными потерями.

Список литературы

1. *Еремин А. Д.* Управление техногенными рисками как система / Экологическая и промышленная безопасность: Сборник материалов III сессии школы-семинара. – Саров: РФЯЦ-ВНИИЭФ, 2004. С. 49–61.