Министерство развития информационных технологий и коммуникаций республики Узбекистан Ташкентский университет информационных технологий имени Мухаммада аль-Хорезми

Кафедра: «Информационной безопасности»

Практическая работа №1

Тема: **Методы оценки рисков**

Группа 221-20

Выполнил: Абдушарипов А

Проверил: Абдуллаев Д

Ташкент 2021

Практическая работа №1

Тема: «Методы оценки рисков»

Всей деятельности организации соответствует риск. Менеджмент риска помогает в принятии решений в условиях неопределенности и возможности возникновения событий или обстоятельств (плановых и непредвиденных), воздействующих на достижение целей организации. **Риск** (в контексте безопасности) – это вероятность причинения ущерба и возможные последствия.

Управление информационными рисками (IRM - Information Risk Management) представляет собой процесс выявления и оценки рисков, снижения их до приемлемого уровня, а также внедрения адекватных механизмов для поддержания этого уровня. *Стопроцентной защиты не существует.* Каждая система имеет уязвимости и подвержена угрозам. Необходимо выявлять эти угрозы, оценивать вероятность их реализации и ущерб, к которому это может привести. Затем нужно предпринимать правильные шаги для снижения общего уровня риска всего окружения до уровня, считающегося в компании приемлемым.

Риски могут иметь различные формы, не обязательно связанные с компьютерами. С точки зрения информационной безопасности, существует несколько видов рисков, которые компания должна понимать и учитывать.

Ниже представлен список основных категорий:

- **Физический ущерб**. Пожар, затопление, вандализм, отсутствие электроэнергии, стихийные бедствия.
- **Действия человека**. Случайные или намеренные действия или бездействие, которые могут нарушить работу компании.
- **Неисправность оборудования**. Неработоспособность систем или периферийных устройств.
- **Внутренние и внешние атаки**. Хакинг, крекинг и проведение атак.
- **Неправильное использование данных.** Предоставление совместного доступа к конфиденциальной информации компании, мошенничество, шпионаж, кражи.
- **Утрата данных.** Преднамеренное или непреднамеренное уничтожение информации.
- **Ошибки приложений.** Ошибки в вычислениях, ошибки ввода информации, переполнения буфера.

Анализ рисков, который на самом деле представляет собой инструмент для управления рисками, является методом выявления уязвимостей и угроз, оценки возможного воздействия, что позволяет выбирать адекватные защитные меры именно для тех систем и процессов, в которых они необходимы.

Анализ рисков имеет четыре основные цели:

- Идентификация активов и их ценности для компании
- Идентификация угроз и уязвимостей
- Количественная оценка вероятности и влияния на бизнес этих потенциальных угроз
- Обеспечение экономического баланса между ущербом от воздействия угроз и стоимостью контрмер

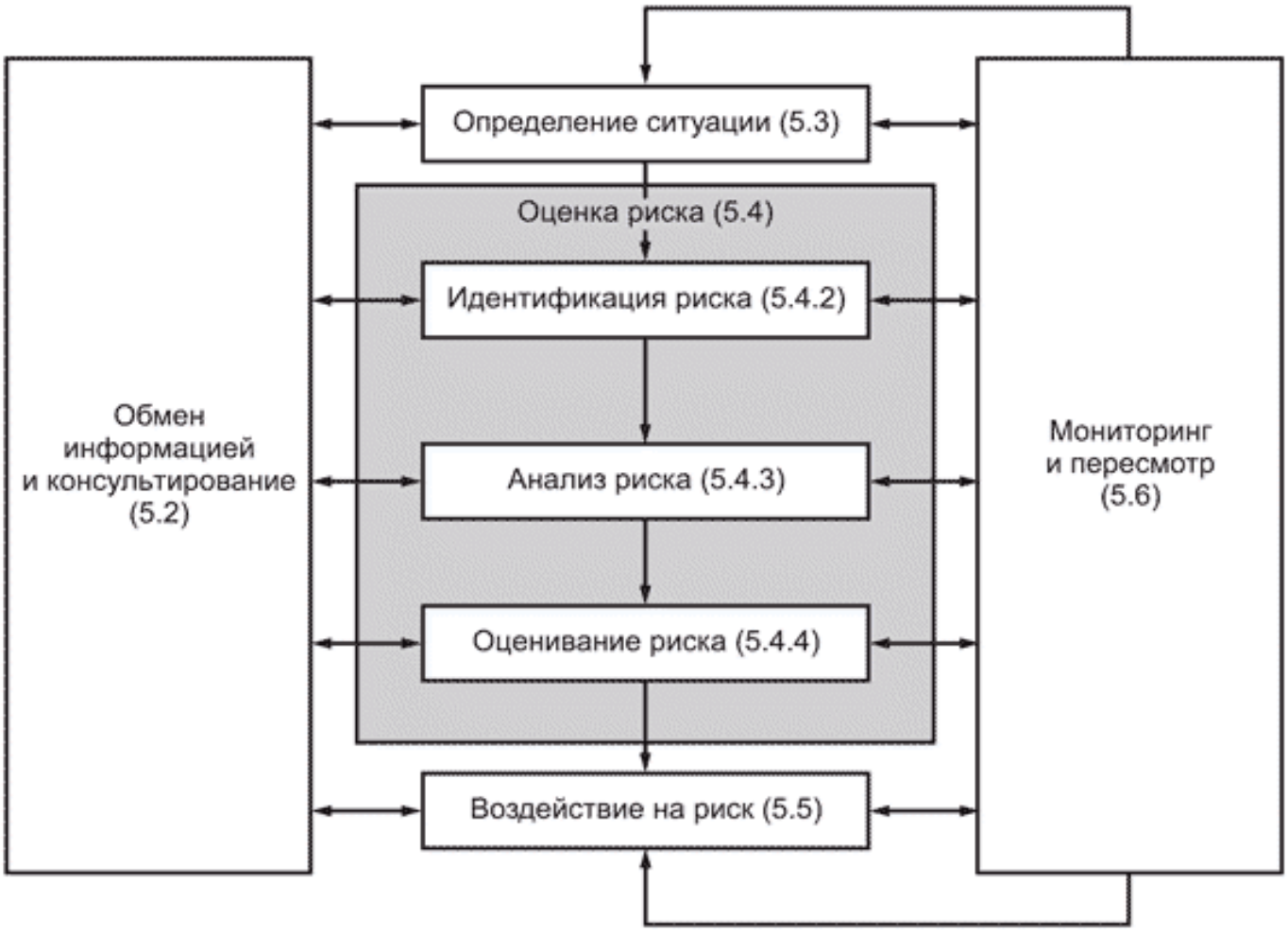
Анализ рисков позволяет сравнить годовую стоимость защитных мер с потенциальным ущербом. Годовая стоимость защитных мер не должна превышать потенциальный годовой ущерб. Также, анализ рисков позволяет связать программу безопасности с целями и требованиями бизнеса компании, что крайне важно для успеха и в том, и в другом.

- **Риск** –влияние неопределенности на цели.
- **Цель** – это то, чего мы желаем достичь в процессе той или иной деятельности. В последнем примере целью абитуриента является поступление в университет.
- **Неопределенность** – состояние, даже частичное, нехватки информации, связанной с пониманием события или знанием о нем, его последствий, или вероятности. В последнем примере, абитуриенту неизвестно, поступит он или нет, и каковы в точности будут последствия поступления или непоступления.
- **Влияние** – это отклонение от желаемого или ожидаемого, положительное или отрицательное. В последнем примере, предположим, расчитывает поступить на «контракт». Отрицательным отклонением от ожидаемого будет являеться непоступление, а положительным – поступление на «бюджет».

Риск часто выражается в форме комбинации последствий события, и связанной с ним вероятности возникновения.

Менеджмент риска включает применение логических и системных методов для:

- обмена информацией и консультаций в области риска;
- установления области применения при идентификации, анализе, оценке и обработке риска, соответствующего любой деятельности, процессу, функции или продукции;
- мониторинга и анализа риска;
- регистрации полученных результатов и составления отчетности.



Оценка риска. Оценка риска является частью процесса менеджмента риска и представляет собой структурированный процесс, в рамках которого идентифицируют способы достижения поставленных целей, проводят анализ последствий и вероятности возникновения опасных событий для принятия решения о необходимости обработки риска.

Оценка риска позволяет ответить на следующие основные вопросы:

- какие события могут произойти и их причина (идентификация опасных событий);
- каковы последствия этих событий;
- какова вероятность их возникновения;
- какие факторы могут сократить неблагоприятные последствия или уменьшить вероятность возникновения опасных ситуаций.

Кроме того, оценка риска помогает ответить на вопрос: является уровень риска приемлемым, или требуется его дальнейшая обработка?

Основной **целью оценки риска** является представление на основе объективных свидетельств информации, необходимой для принятия обоснованного решения относительно способов обработки риска.

Оценка риска обеспечивает:

- понимание потенциальных опасностей и воздействия их последствий на достижение установленных целей организации;
- получение информации, необходимой для принятия решений;
- понимание опасности и ее источников;
- идентификацию ключевых факторов, формирующих риск, уязвимых мест организации и ее систем;
- возможность сравнения риска с риском альтернативных организаций, технологий, методов и процессов;
- обмен информацией о риске и неопределенностях;
- информацию, необходимую для ранжирования риска;
- предотвращение новых инцидентов на основе исследования последствий произошедших инцидентов;
- выбор способов обработки риска;
- соответствие правовым и обязательным требованиям;
- получение информации, необходимой для обоснованного решения о принятии риска в соответствии с установленными критериями;
- оценку риска на всех стадиях жизненного цикла продукции.

Идентификация риска. Идентификация риска - это процесс определения элементов риска, составления их перечня и описания каждого из элементов риска.

Целью идентификации риска является составление перечня источников риска и событий, которые могут повлиять на достижение каждой из установленных целей организации или сделать выполнение этих целей невозможным. После идентификации риска организация должна идентифицировать существенные особенности проекта, персонал, процессы, системы и средства управления. Процесс идентификации риска включает в себя идентификацию причин и источников опасных событий, ситуаций, обстоятельств или риска, которые могут оказать существенное воздействие на достижение целей организации, и характер этих воздействий.

Анализ риска. Анализ риска включает в себя анализ и исследование информации о риске. Анализ риска обеспечивает входные данные процесса общей оценки риска, помогает в принятии решений относительно необходимости обработки риска, а также помогает выбрать соответствующие стратегии и методы обработки риска.

Анализ риска включает анализ вероятности и последствий идентифицированных опасных событий с учетом наличия и эффективности применяемых способов управления. Данные о вероятности событий и их последствиях используют для определения уровня риска.

Анализ риска включает анализ источников опасных событий, их положительных и отрицательных последствий и вероятностей появления этих событий.

При этом должны быть идентифицированы факторы, влияющие на вероятность события и его последствия. Событие может иметь множественные последствия и может влиять на различные цели.

Также должны быть учтены результаты применения и эффективность существующих методов управления.

Выбор метода оценки рисков.

Методы оценки риска выбирают на основе:

- цели исследования;
- ответственности принимаемых решений;
- типа и диапазона анализируемого риска;
- возможных последствий опасного события;
- степени необходимых экспертиз, человеческих и других ресурсов;
- доступности информации и данных;
- потребности в модификации/обновлении оценки риска;
- обязательных и договорных требований.

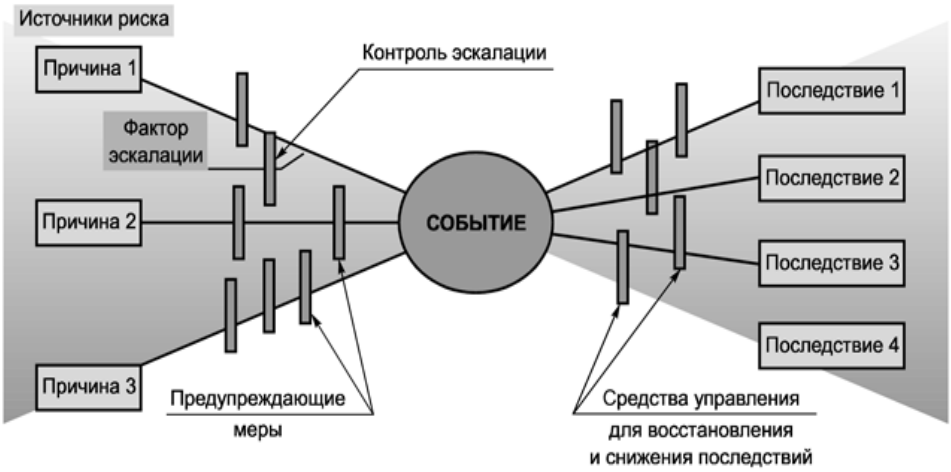
На выбор метода оценки риска влияют различные факторы, такие как **доступность ресурсов**, **характер и степень неопределенности** данных и информации, сложность метода.

На выбор метода оценки риска влияют следующие **факторы доступности ресурсов:**

- практический опыт, навыки и возможности группы оценки риска;
- ограничения по времени и другие ресурсы организации;
- доступный бюджет, если необходимы внешние ресурсы.

Характер и степень неопределенности информации включают в себя понимание качества, количества и полноты информации о рассматриваемом риске. **Понимание** включает в себя осознание достаточности полученной информации о риске, его источниках и причинах, его последствиях для достижения установленных целей. **Неопределенность** может быть связана с неопределенностью данных и недостатком достоверных данных.

АНАЛИЗ "ГАЛСТУК-БАБОЧКА"



АНАЛИЗ «ГАЛСТУК-БАБОЧКА»

Данный метод представляет собой графическое описание и анализ развития исследуемого нежелательного события от причин до последствий. Основное внимание в данном методе уделяется контрмерам против исследуемого события и причин, которые к нему приводят.

Выполнение данного метода можно выделить следующие этапы:

1. Определение события для анализа в центре диаграммы.
2. Составление перечня причин, которые могут привести к исследуемому событию.
3. Анализ механизма развития ситуации до исследуемого события
4. Можно описать факторы, которые могут привести к эскалации события и его последствий.
5. Отображение барьеров, которые помешают причинам развиться до события, т.н. предупреждающие меры. Также можно отобразить барьеры для факторов эскалации (см. п. 4)
6. Составление перечня последствий, к которым может привести исследуемое событие
7. Отображение барьеров, которые помешают изучаемому событию развиться до последствия.

По выполнению анализа «галстук-бабочка» мы получаем простую диаграмму, наглядно демонстрирующую основные пути опасных событий и барьеры, направленные на предотвращение или смягчение нежелательных последствий, или же усиление и ускорение ожидаемых событий (в том случае, если исследуемое событие является положительным).

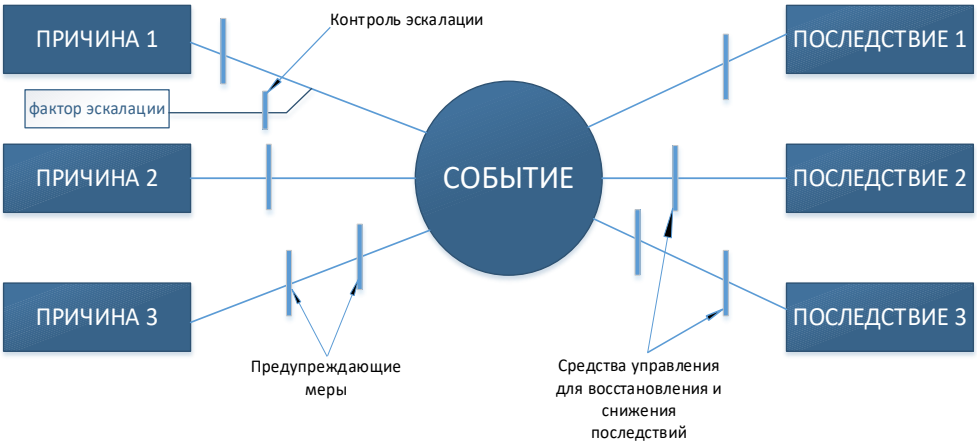


Рис 1.5. Пример диаграммы «галстук-бабочка»

АНАЛИЗ ДЕРЕВА НЕИСПРАВНОСТЕЙ

Анализ дерева неисправностей используется для идентификации и анализа факторов, которые могут привести к нежелательному событию, т.н. конечному событию. Исследуемые факторы выставляются в последовательность, в которой они могут произойти, и связываются логически. Этими факторами могут быть события, связанные со сбоями или отказами компонентов различного оборудования, например, компьютера, программного обеспечения, ошибками сотрудников или другими событиями, которые могут привести к нежелательному событию.

Для применения данного метода требуется хорошее знание исследуемой системы, как она может выйти из строя, и понимание того, что может привести к нежелательному событию. Может быть очень полезным построение детальной схемы дерева неисправностей. Кроме того, возможно подсчитать вероятность исследуемого нежелательного события. Для этого необходимы сведения о вероятности всех событий, описанных в дереве неисправностей.

Выполнение данного метода можно выделить следующие этапы:

1. Определить конечное событие, которое нужно исследовать
2. Нахождение возможных причин, приводящих к конечному событию, начиная с конечного события
3. Анализ обозначенных причин, с целью определения конкретных событий или отказов, которые могут привести к обозначенным причинам.
4. Последовательный анализ причин следующего уровня, и так далее, пока анализ не станет нецелесообразным.
5. Оценка вероятности начальных событий, и последующий расчет вероятности конечного события.

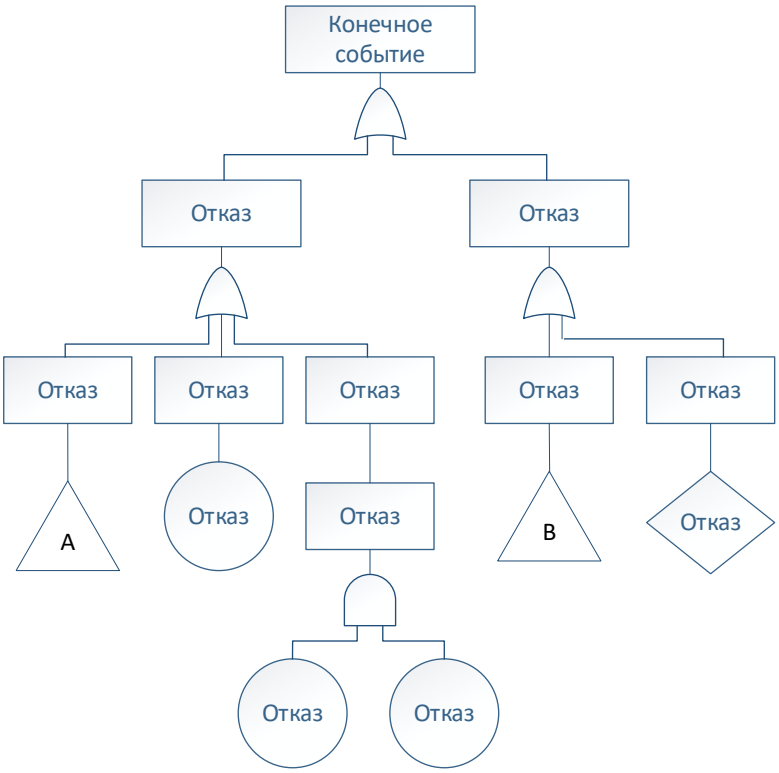


Рис 1.6. Пример диаграммы «анализ дерева неисправностей»

Анализ дерева неисправностей дает наглядное представление путей возникновения исследуемого конечного события и взаимосвязанных ситуаций, когда может одновременно произойти более одного события. Также можно оценить вероятность конечного события.

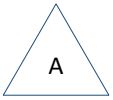
Логический элемент «И» - событие произойдет, если все события на входе произойдут

Логический элемент «ИЛИ» - событие произойдет, если хотя бы одно событие на входе произойдет

Базовое событие - дальнейший анализ нецелесообразен

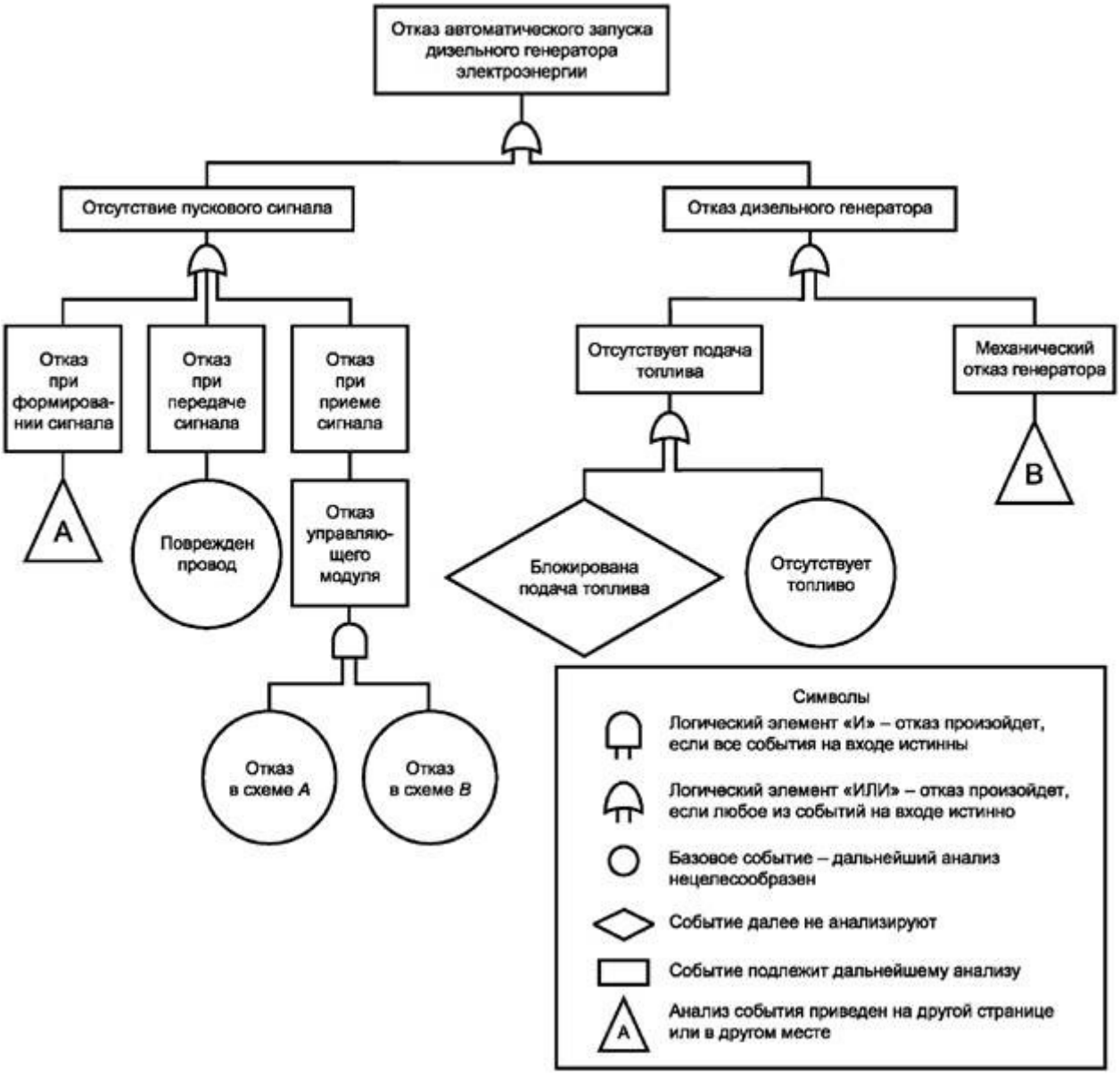
Событие не анализируют

Событие подлежит дальнейшему анализу

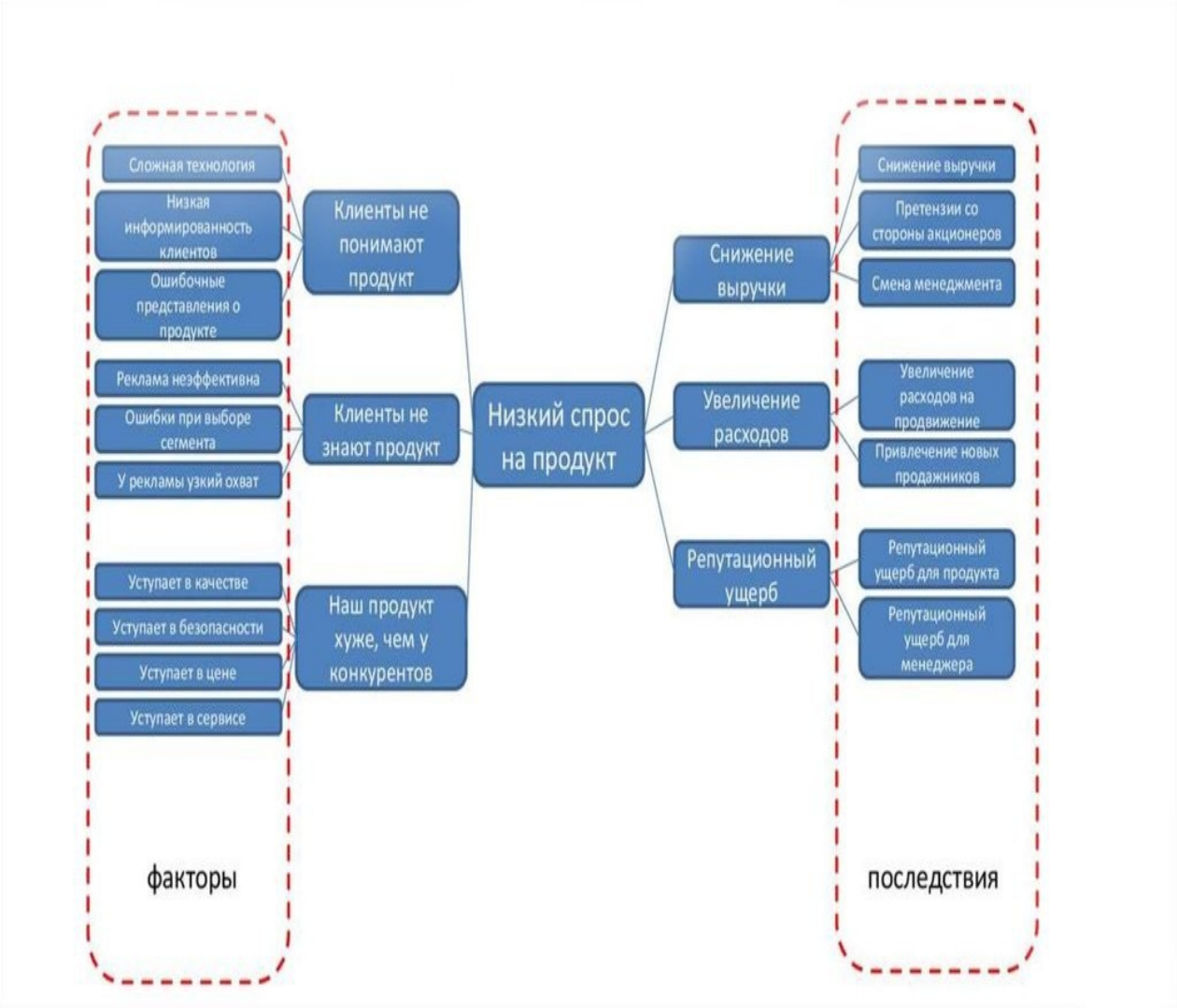
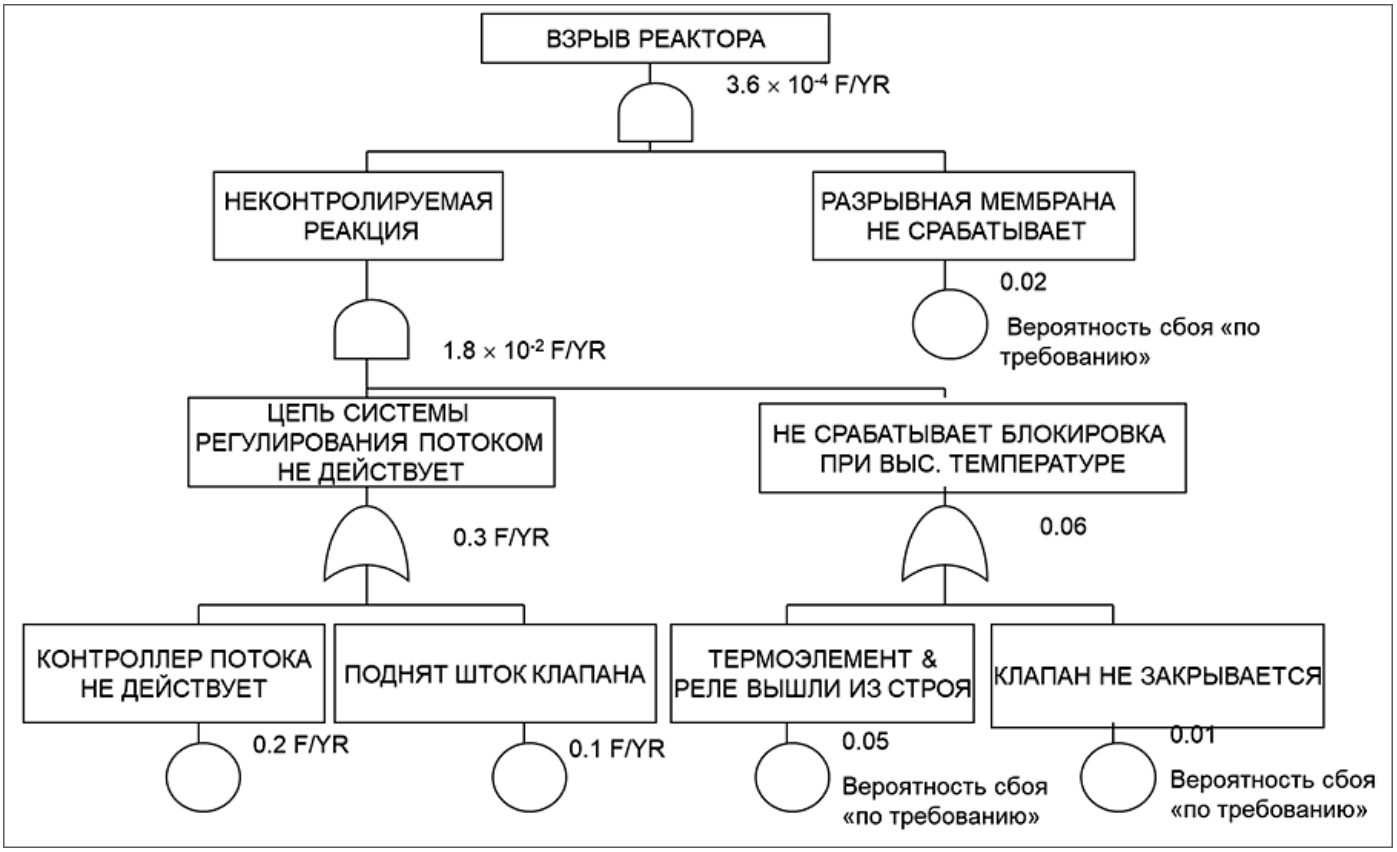


Перенос – анализ события приведен на другой странице или в другом месте

Рис 1.7. Символьные обозначения анализа дерева неисправностей



ПРИМЕР ДЕКОМПОЗИЦИИ РИСКА – ПАДЕНИЕ СПРОСА НИЖЕ ПЛАНА НА ПРИЧИНЫ И ПОСЛЕДСТВИЯ



АНАЛИЗ ДЕРЕВА НЕИСПРАВНОСТЕЙ