

*Д.Р. Мерзлякова*

## **ИСПОЛЬЗОВАНИЕ ТЕОРИИ РЕШЕНИЯ ИЗОБРЕТАТЕЛЬСКИХ ЗАДАЧ ДЛЯ ОБЕСПЕЧЕНИЯ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ И ТЕХНОЛОГИЙ СЕЙФНЕТ НАЦИОНАЛЬНОЙ ТЕХНОЛОГИЧЕСКОЙ ИНИЦИАТИВЫ**

Представлен прикладной аспект использования ТРИЗ в целях обеспечения техносферной безопасности и технологий Сейфнет Национальной технологической инициативы. Представлены возможности цифровых технологий для проведения “диверсионного анализа” на основе ТРИЗ. Представлены технологии Сейфнет как цифровое развитие экономики в области безопасности.

*Ключевые слова:* национальная технологическая инициатива, технологии Сейфнет, ТРИЗ, цифровые технологии, цифровая экономика, техносферная безопасность, диверсионный анализ.

В восьмидесятые годы было начато использование ТРИЗ для прогнозирования и предотвращения всевозможных нежелательных ситуаций и явлений, в том числе: преступлений, ошибок, производственного брака, нарушений функционирования технических систем, аварий, катастроф (в том числе экологических) и т.п. Методология, получившая название "диверсионный анализ", предусматривает на первом этапе "изобретение" с помощью ТРИЗ возможно большего числа различных нежелательных ситуаций и явлений (фактически речь идет об изобретении диверсий - отсюда и название метода), а на втором - решение задач, обеспечивающих предотвращение этих "диверсий". Сегодня диверсионный анализ (прогноз) "принят на вооружение" всеми службами обеспечения безопасности, начиная с Комитета Глобальной Безопасности ООН и Интерпола и кончая ассоциациями защиты потребителей. Во всяком случае, ни один закон не будет сегодня принят, ни один проект не начнет осуществляться и ни один товар не поступит в продажу, если по нему не проведен диверсионный прогноз.

Службы диверсионного прогноза снизили число опасностей, подстерегающих людей, но изредка нежелательные происшествия, стихийные бедствия и аварии все-таки происходят. И здесь ТРИЗ позволяет в условиях дефицита времени и ресурсов быстро и эффективно решать творческие задачи, направленные на локализацию аварии, спасение людей и т.п.

Рассмотрим понятие диверсионного прогноза и анализа более подробно. В чём же заключается этот метод? "Диверсионный анализ" – это метод прогнозирования возможных нежелательных явлений, в т.ч.: чрезвычайных ситуаций, аварий, катастроф (в т.ч. экологических),

стихийных бедствий, преступлений и т.п., а также выявления причин уже случившихся происшествий. Он состоит из двух основных этапов.

**Этап первый:** на нём происходит преобразование вопросов типа, “какие чрезвычайные ситуации и нежелательные явления возможны в данном объекте”, или “почему возникла данная чрезвычайная ситуация” в вопросы типа, “как испортить данный объект, как обеспечить возникновение наибольшего количества наиболее опасных нежелательных явлений”, либо “как реализовать в данном объекте именно ту чрезвычайную ситуацию, которая возникла”. Всё это напоминает разработку диверсий, в результате чего возникают изобретательские задачи, требующие решения с помощью методов технического творчества.

**Этап второй.** На нём решаются задачи по предотвращению спрогнозированных “диверсий”. Таким образом “диверсионный анализ” включает предварительно выполняемые операции:

- формулирование “диверсионной задачи”;
- анализ известных способов создания чрезвычайных ситуаций, вредных и нежелательных явлений;
- паспортизацию и проверку возможностей использования для “диверсии” имеющихся ресурсов;
- поиск возможных нежелательных эффектов в информационных фондах и с помощью методов технического творчества;
- поиск возможностей усиления и “маскировки” нежелательных эффектов;
- анализ выявленных нежелательных эффектов и возможностей их усиления;
- поиск возможностей устранения нежелательных эффектов.

В “диверсионном анализе” используются специальные информационные фонды:

- типовые способы создания нежелательных явлений и их результаты;
- типовые опасные зоны на технических объектах;
- ресурсы, способные обеспечить вредное воздействие;
- типовые ошибки при создании технических систем;
- способы усиления и «маскировки» нежелательных явлений;
- способы предотвращения нежелательных явлений и борьбы с последствиями.

Такой подход в дальнейшем влечёт за собой использование сценарного анализа, который, как способ проверки различных предложений о будущем включает в себя построение двух или трех правдоподобных сценариев, разработку для каждого из них адекватной стратегии, оценку вероятности осуществления сценариев и оценку результирующих стратегий.

Иногда сценарии полезно строить на базе возможных результатов: оптимистического, пессимистического и наиболее вероятного. Пессимистичный сценарий нужен, чтобы проверить существующие предположения и планы. Оптимальное число сценариев – два, три...

Для ускорения процесса разработки сценариев развития и выбора стратегии необходима четкая систематизация существующих рисков [1].

Всё вышеперечисленное будет в значительной степени способствовать развитию профессионального риск-мышления, т.к. для “грамотно спланированной диверсии” необходимы профессиональные знания в области функционирования объекта, и его слабых точек, синергетического воздействия чрезвычайных ситуаций и т.д.

Для проведения “диверсионного анализа” можно использовать, в том числе и цифровые технологии, например компьютерную программу ЭФФЕКТЫ 200.

Программу ЭФФЕКТЫ 200 можно использовать:

- при разработке *концепций* новых устройств и технологий вне зависимости от области их применения;
- для выявления *причин отказов и поломок* различных технических устройств;
- для определения *последствий* тех или иных естественных и технических процессов;
- для разработки расчетных *моделей* устройств и технологий.

Данная методика может быть использована и для обеспечения техносферной безопасности. Техносферная безопасность – это свойство объекта, выраженное в его способности противостоять техносферным опасностям (негативным факторам техносферных опасностей). Обеспечение техносферной безопасности – создание благоприятных для человека условий существования в преобразуемой человеком биосфере – техносфере. На управленческом уровне сегодня реализуется ряд систем для обеспечения безопасности человека в техносфере (безопасность труда, защита в ЧС, пожарная защита и др.). Они имеют общие цели и задачи, поэтому в перспективе могут быть сведены в общую систему «обеспечения безопасности техносферы» [2; 3].

Для обеспечения техносферной безопасности могут быть использованы и технологии Национальной технологической инициативы по направлению Сейфнет.

Прогнозировать развитие отраслей экономики призвана Национальная технологическая инициатива (НТИ). Это государственная программа мер по поддержке развития в России перспективных отраслей, которые в течение следующих 20 лет могут стать основой мировой экономики [2].

НТИ предполагает развитие следующих технологий: системы данных; развитие искусственного интеллекта; системы распределенного реестра; квантовые технологии; энергетика; новые производственные технологии; сенсорика и компоненты робототехники; технологии беспроводной связи; технологии управления свойствами биологических объектов, нейротехнологии, технологии виртуальной и дополненной реальности.

Данные технологии развивают следующие рынки НТИ: рынок энергетики – Энерджинет, рынок производства и доставки еды – Фуднет, обеспечение персональной безопасности – Сейфнет, система персональной

медицины и здравоохранения – Хелфнет, производство беспилотных летательных аппаратов – Аэронет, производство морского транспорта без экипажа – Маринет, производство автотранспорта без водителя – Автонет, распределенные системы финансов и валюты – Финнет, искусственные распределённые компоненты психики и сознания – Нейронет.

Согласно НТИ Сейфнет включает в себя несколько основных направлений разработок: устройства, применяемые для обеспечения безопасности, прикладные системы для решения задач безопасности, безопасность платформ управления и приложений, индустриальные интеграционные услуги, безопасность сетей и пр. [2]. Перечисленный спектр позволяет прогнозировать востребованность как технологий Сейфнет, так и специалистов их разрабатывающих и реализуемых.

Таким образом, методика ТРИЗ предназначена для решения проблем, связанных с обеспечением безопасности: прогнозирования возможных чрезвычайных ситуаций, аварий, катастроф и других нежелательных явлений; своевременного выявления "факторов риска" и "предвестников аварии"; выработки конкретных технических и организационных решений, направленных на предотвращение спрогнозированных нежелательных явлений и т.п. Методика основана на применении теории решения изобретательских задач (ТРИЗ) и "диверсионного анализа", она не заменяет существующие анти-аварийные методы, подходы и мероприятия, а дополняет их современными методами решения творческих задач.

## СПИСОК ЛИТЕРАТУРЫ

1. Афанасьев В.М., Миназетдинов Т.Ф. Формирование риск-мышления у специалистов в области техносферной безопасности // В сборнике докладов Всероссийской научно-практической конференции с международным участием: Новые технологии, материалы и оборудование Российской авиакосмической отрасли. - 2016. - С. 791-795.
2. Бондаренко О. А. Концепция дорожной карты Сейфнет // Проблемы развития современного предпринимательства. Ставрополь: Секвойя, 2018. – С. 14-19.
3. Закирова Р.Р., Мерзлякова Д.Р., Свинцова Н.Ф. Исследование и реализация систем управления безопасного производства на объектах экономики при обучении магистров направления подготовки «Техносферная безопасность» // В сборнике: ДАЛЬНЕВОСТОЧНАЯ ВЕСНА - 2018 Материалы 16-й Международной научно-практической конференции по проблемам экологии и безопасности. - Комсомольск-на-Амуре, 2018. - С. 20-21.
4. Производственный травматизм. Несчастный случай на производстве [электронный ресурс]. - [https://meduniver.com/Medical/gigiena\\_truda/142.html](https://meduniver.com/Medical/gigiena_truda/142.html), 27.04.2018
5. Ревенков А. В., Резчикова Е. В. Теория и практика решения задач: учебное пособие. - М.: Форум, 2018. – 128 с.

6. Шамина О. Б. Теория решения изобретательских задач. Конспект лекций. Томск. Изд – во: Томского политехнического университета, 2012. – 244 с.

Мерзлякова Дина Рафаиловна

кандидат психологических наук, доцент, кафедра безопасности

жизнедеятельности

Удмуртский государственный университет

E-mail: [dinamerzlyakova26@gmail.com](mailto:dinamerzlyakova26@gmail.com)