УДК 004.8

О НЕКОТОРЫХ ФУНКЦИЯХ “SAFETY MANAGEMENT SYSTEM”, ПРИМЕНИМЫХ ДЛЯ ИДЕНТИФИКАЦИИ ОПАСНОСТЕЙ И УЯЗВИМОСТЕЙ НА ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТАХ

Е.А. Сакрутина
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: consoft@ipu.ru

Ключевые слова: идентификация опасностей и уязвимостей, риски, safety management system

Аннотация: В статье рассмотрены важные функции системы “Safety management system” в части своевременной идентификации опасностей и уязвимостей. Внедрение таких систем в энергетике повысит безопасность функционирования объектов энергетической сферы.

1. Введение

В условиях интенсивного развития и внедрения информационных технологий уделяется особое внимание вопросам обеспечения безопасности критически важных объектов, к которым относятся крупные гидротехнические сооружения, объекты энергетики (в том числе и атомной), вредные химические производства, транспортные узлы и т.п. [1-6]. Выведение таких объектов из штатных ситуаций может привести к тяжелым последствиям. Совокупность критически важных объектов входит в состав объектов критической информационной инфраструктуры. Для успешной реализации мероприятий защиты критической информационной инфраструктуры необходимо решение ряда задач, часть из которых связана с созданием системы мониторинга угроз безопасности. Главной целью создания системы мониторинга угроз безопасности является снижение до минимального уровня риска воздействия и минимизации возникающего ущерба. Одним из решений является создание информационно-аналитической системы “Safety management system” [7-12], которая осуществляет мониторинг безопасности на основе системных закономерностей.

Развитие информационно-аналитической системы “Safety management system” в энергетике, в том числе и атомной, осуществляется в направлении достижения высокого уровня качества и доходности и характеризуется ростом технической оснащенности и сложности процессов.

Высокие требования по безопасности и экономичности определяют необходимость использования и совершенствования автоматизированных средств и систем диагностирования, своевременно обнаруживающих дефекты (угрозы, факторы опасности) в технологических процессах с целью предотвращения последствий от них и снижения потерь (временных, материальных, финансовых и других ресурсов). Под дефектами по-

нимаются несоответствия предписанным технологиям, которые обусловлены различными объективными и субъективными причинами.

Применяемые в энергетике методы контроля и диагностики, в основном направленные на повышение безопасности и обеспечение работоспособности техники, недостаточно ориентированы на обнаружение дефектов в сферах деятельности, которые обеспечивают доходность. Анализ объектов в широком смысле показывает, что известные методы диагностирования оказываются неэффективными для обнаружения дефектов в процессах, и необходимы новые подходы, включающие разработку методов идентификации факторов опасности.

2. Свойства “Safety Management System” в энергетике

Повышение уровня безопасности всегда было одним из основных приоритетов для энергетических объектов. Тем не менее, в связи с развитием традиционной энергетики и наличием вероятности увеличения числа инцидентов разного рода в международном сообществе присутствует мнение, что традиционных реагирующих подходов снижения риска до приемлемого уровня может быть недостаточно. В последние годы, системные причины многих инцидентов в энергетике привели к существенному повышению интереса к процедурам идентификации и управления рисками, а также к разработке и развитию систем управления безопасностью в энергетике, которые имеют три основные характеристики:

- системность – меры по управлению безопасности будут осуществляться в соответствии с разработанной Программой безопасности и последовательно применяться;
- проактивность – подход, при котором основной акцент делается на профилактике путем выявления опасных факторов и принятия мер по уменьшению риска, прежде чем произойдет какое-либо опасное событие и окажет неблагоприятное влияние на состояние безопасности;
- четкость – меры по управлению безопасностью должны быть задокументированными, наглядными и осуществляться отдельно от других видов управленческой деятельности.

В работах, посвященных системам управления безопасностью [13-16], строятся прогнозы влияния различных факторов на безопасность на основе аппроксимации статистических данных и экспертных оценок, но при этом не проводится непосредственного математического моделирования организационных механизмов.

Функционирование системы управления безопасностью в энергетике должно представлять собой замкнутый цикл последовательно выполняемых операций: выявление фактора риска, оценка степени опасности выявленных факторов риска, выработка вариантов действий по локализации факторов риска, информирование органов управления и поддержка принятия решения, анализ эффективности принятых мер. На рис. 1 представлена схема оценки состояния безопасности на основе факторного анализа, где применятся методология PDCA (the Deming's Shewhart cycle) для постоянного улучшения безопасности. The Deming's Shewhart cycle является важной составляющей успешного функционирования системы управления безопасностью.

Общекорпоративный подход к безопасности предназначен для осуществления постоянного совершенствования системы безопасности и преследует следующие основные цели:

- оперативно и постоянно снижают остаточный риск системы (см. рис. 2, которая выдвигает на первый план 2 связанных типа событий - инцидентов и уязвимости -

и совместную область, охватываемых политикой безопасности на основе концепции использования или дрейфа реализации);

- оценка фактической применимости и реальной эффективности политики безопасности, с целью ее постоянного совершенствования.

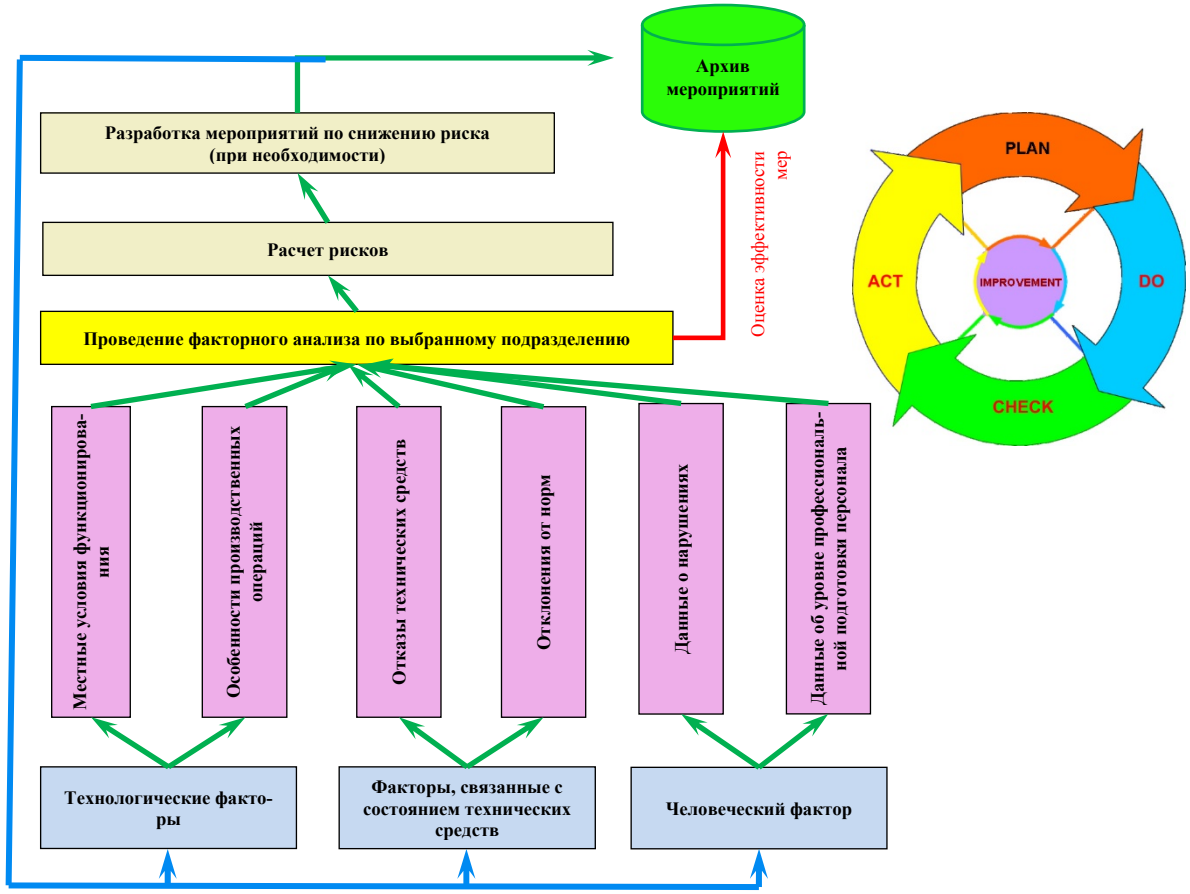

Рис. 1. Оценка состояния безопасности на основе факторного анализа.

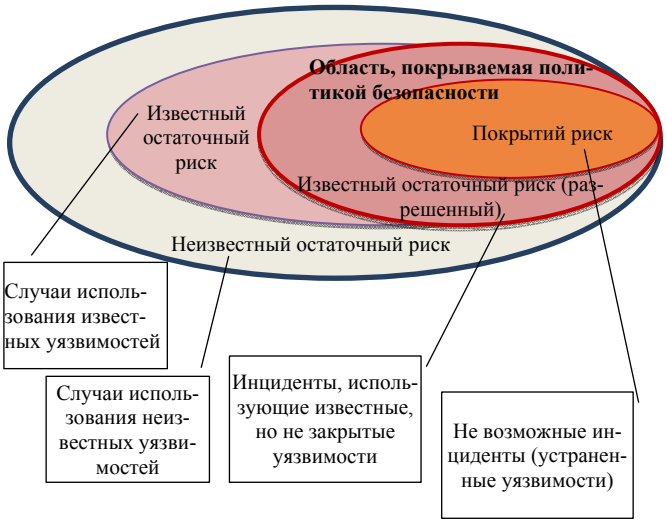

Рис. 2. Соотношение остаточных рисков.

Управление рисками безопасности в энергетической системе должно быть непрерывным процессом, охватывающим весь энергетический объект, и осуществляться всеми сотрудниками на всех уровнях организации, а также должно быть нацелено на выявление потенциально опасных событий, влияющих на безопасность. Управление рисками безопасности не является линейным процессом, в котором один компонент оказывает влияние на следующий. Управление рисками безопасности является многонаправленным циклически процессом, в котором практически все компоненты могут воздействовать и воздействую друг на друга. Существует прямая взаимосвязь между целями организации и компонентами процесса управления рисками, представляющими собой действия, необходимые для их достижения. Данная взаимосвязь представлена на трехмерной матрице (см. рис. 3).

Рис. 3. Взаимосвязь между целями и компонентами процесса управления рисками.

3. Идентификация опасностей и используемые методы

Событие – это происшествие, инцидент или авария, имеющие внутренний или внешний источник по отношению к организации, и оказывающие влияние на достижение поставленных целей. Влияние событий может быть положительным, отрицательным или смешанным. События, отрицательно влияющие на деятельность организации, представляют собой риски.

Риск может быть определен как потенциальный ущерб, включая небезопасные действия и/или условия, которые могут закончиться особыми ситуациями любой классификации. Риск является конкретизирующим понятием опасности и рассматривается как степень опасности события и частоты возникновения события (вероятности события, абсолютного количества инцидентов разного рода). Определение рисков в отношении

безопасности – это начальная стадия управления рисками, на которой проводится идентификация опасностей и их анализ.

Цель идентификации опасности и процесса анализа риска состоит в том, чтобы упростить разработку управленческих решений для предотвращения возможных рисков.

По своему характеру методы выявления опасных факторов могут быть реализованы с помощью следующих стратегий:

Ретроактивная – стратегия предусматривает реагирование на события/происшествия путем принятия мер, направленных на предотвращение их повторения в будущем. Ретроактивная стратегия предусматривает получение и анализ данных по происшествиям, инцидентам, отказам техники, событиям и т.д.

Проактивная – стратегия, при которой основной акцент делается на выявление опасных факторов и принятие мер по их устранению, прежде чем произойдет какое-либо событие, способное отрицательно отразиться на показателях безопасности. При реализации этой стратегии проводится активный сбор информации из различных источников. Риск возникновения происшествий может быть сведен к минимальному путем выявления уязвимых мест, прежде чем они себя проявят.

Прогностическая – стратегия, основанная на выявлении потенциальных факторов опасности в предстоящей производственной деятельности и разработке мер по недопущению их проявления. По своей сути прогностические системы сбора данных о безопасности являются статистическими системами, собирающими и анализирующими значительный объем оперативных данных, которые сами по себе важного значения не имеют. Далее полученные данные объединяются с данными ретроактивных и проактивных систем сбора информации о безопасности.

Оценивание уровня безопасности осуществляется на основе формирования индексов оценки ситуации с учетом подразделений, ответственных за возникновение событий, прогнозируемых видов происшествий и количества факторов, влияющих на эти события.

4. Оценка рисков безопасности

Целью и основным результатом анализа и оценки рисков является разработка корректирующих и/или предупреждающих мероприятий для поддержания на приемлемом уровне рисков потенциальных последствий воздействия факторов опасности.

Наиболее информативным анализом параметров работы объекта энергетики в области обеспечения безопасности является многомерный принцип обработки статистических данных с использованием экспертных заключений. Опасности в системе управления рисками документируются и контролируются. Объем и содержание функции идентификации опасности охватывает всю производственную деятельность, при этом сбор данных производится как по ретроактивным, так и по проактивным и прогностическим схемам.

Для определения эффекта применения процесса управления риском и правильности превентивных мероприятий должен проводиться постоянный мониторинг рисков.

Возникновение особой ситуации есть не что иное, как проявление рисков и опасностей. Для проведения многомерного анализа системы необходимо иметь представление о виде особой ситуации, таким образом, чтобы события можно было классифицировать по степени серьезности последствий.

События классифицируют в соответствии с градацией влияния на безопасность и соответствуют типам особых ситуаций.

Для систематизации процесса идентификации опасностей и оценки степени риска события применяется матрица рисков, которая имеет категории особых ситуаций, определяемых в соответствии с частотой возникновения ситуаций данного вида, и классы особых ситуаций в соответствии с принятой категоризацией для каждого типа объекта энергетики. Степень риска – параметр, определяющий меры воздействия для предотвращения ситуации. Каждой степени риска должно соответствовать разработанное воздействие, направленное на снижение степени риска возникновения особых ситуаций данного вида. Таким образом, произошедшее событие можно оценить индексом риска, соответствующим категории, классу и степени риска. Смысл использования индекса риска состоит в том, что различные события могут быть одинаковыми по степени риска, но различаться по своей опасности и иметь разную вероятность появления.

Идентификация является первым и одним из основных этапов анализа рисков безопасности. Рисками о существовании или о свойствах, которых не известно, невозможно эффективно управлять. Поэтому задача обнаружения всех рисков является чрезвычайно важной [17].

По существу, идентификация рисков безопасности сводится к выявлению возможных проблем. В данном случае под «проблемой» можно понимать что-либо, что может встать между организацией, эксплуатирующей объект энергетики, и ее целями в области безопасности. То есть, сначала необходимо определить, что может пойти «не так», чтобы впоследствии решить, как устранить или обойти выявленную опасность.

Идентификация риска безопасности - процесс нахождения, составления перечня и описания элементов риска. Основными элементами риска являются:

- причины, которые приводят к наступлению опасного явления;
- причины, которые приводят к наступлению опасного явления;
- виды воздействия, которые могут привести к изменению уровня безопасности;
- последствия, представляющие собой потери из-за воздействия и их оценку со стороны субъекта;
- факторы риска, которые влияют на вероятность реализации риска и тяжесть последствий.

Организация процесса идентификации рисков безопасности требует решения целого ряда вопросов, к числу которых, в частности, относятся:

- какую информацию следует собирать;
- источники информации;
- систематизация/структуризация и хранение информации;
- анализ входной информации.

Процесс идентификации часто сводят к определению так называемых «risk exposure». Risk exposure [11] представляет собой «единицу» учета рисков, которая задается следующими параметрами:

- объект, которому может быть причинен вред;
- субъект, который понесет потери из-за причинения вреда данного объекта в результате наступления указанного события;
- потери субъекта, вызванные причинения вреда данному объекту в результате наступления указанного события.

Для полного описания экспозиции риска необходимо определить все параметры. Стоит отметить, что изменение хотя бы одного из параметров означает изменение экспозиции риска.

Результатом процесса идентификации рисков безопасности будет являться перечень рисков, содержащий:

- список потенциальных действий по корректирующим мерам;

- список потенциальных действий по корректирующим мерам;
- основные причины возникновения риска;
- уточнение категории риска.

Входная информация (данные об авариях/инцидентах) является ключевым элементом системы управления безопасностью. Действительно, на основе данных об авариях/инцидентах могут быть получены показатели безопасности и количественные оценки рисков. Однако качество данных об авариях/инцидентах, имеющихся в базах данных организации может повлиять на результаты (т.е. результат какого-либо анализа данных будет ограничен качеством имеющихся в распоряжении наборов данных). Эта проблема усугубляется при попытке агрегации баз данных разных организаций.

5. Заключение

Внедрение информационно-аналитических систем “Safety management system” в энергетике, обеспечит своевременную идентификации опасностей и уязвимостей, а также оценку рисков и, следовательно, упростит разработку управленческих решений для предотвращения возникновения событий, влияющих на безопасность. Системный подход к раннему обнаружению опасностей и уязвимостей является важной компонентой обеспечения безопасности энергетических объектов.

Список литературы

1. Wang F., Wang Juaqun, Wang Jin, Hu Y.Li, L., Wu Y. Risk monitor riskangel for risk-informed applications in nuclear power plants // Annals of Nuclear Energy. 2016. Vol. 91. P. 142-147.
2. Hashemian H.M., Feltus M.A. On-Line Condition Monitoring Applications in Nuclear Power Plants // NPIC&HMIT. Albuquerque, NM, USA, 2006. P. 568-577.
3. Jharko E. Towards the problem of creating information operator support systems for nuclear power plants // Proceedings of the 2nd IEEE International Conference on Control in Technical Systems (CTS). 2017. P. 356-359.
4. Jharko E. Design of Intelligent Information Support Systems for Human-Operators of Complex Plants // IFAC Proceedings Volumes. 2008. Vol. 41, No. 2. P. 2162-2167.
5. Gnonia M.G., Salehb J.H. Near-miss management systems and observability-in-depth: Handling safety incidents and accident precursors in light of safety principles // Safety Science. 2017. Vol. 91. P. 154-167.
6. Mononen P., Leviäkangas P. Transport safety agency's success indicators – How well does a performance management system perform? // Transport Policy. 2016. Vol. 45. P. 230-239.
7. Jharko E., Sakrutina E. Towards the Problem of Creating a Safety Management System in the Transportation Area // IFAC-PapersOnLine. 2017. Vol. 50, No. 1. P. 15610-15615.
8. Wahlström B. Systemic thinking in support of safety management in nuclear power plants // Safety Science. 2018. Vol. 109. P. 201-218.
9. Jharko E., Sakrutina E. On creating safety control systems for high operation risk plants // Proceedings of 2016 International Siberian Conference on Control and Communications (SIBCON). 2016. P. 1-6.
10. Li Y., Guldenmund F.W. Safety management systems: A broad overview of the literature // Safety Science. 2018. Vol. 103. P. 94-123.
11. Labaka L., Hernantes J., Sarriegi J.M. Resilience framework for critical infrastructures: An empirical study in a nuclear plant // Reliability Engineering & System Safety. 2015. Vol. 141. P. 92-105.
12. Калашников А.О., Сакрутина Е.А. Модель оценки рискового потенциала объектов критической инфраструктуры атомных электростанций // Труды 11-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD '2018). М.: ИПУ РАН, 2018. Т. 2. С. 457-461.
13. Liou J.H., Yen L., Tzeng G.H. Building an effective safety management system for airlines // Journal of Air Transport Management. 2008. Vol. 14, No. 1. P. 20-26.
14. Li C.-Y., Wang J.-H., Zhi Y.-R., Wang Z.-R., Gong J.-H. Simulation of the Chlorination Process Safety Management System Based on System Dynamics Approach // Procedia Engineering. 2018. Vol. 211. P. 332-342.

15. Hsu Y.-L. From reactive to proactive: using safety survey to assess effectiveness of airline SMS // Journal of Aeronautics, Astronautics and Aviation. Series A. 2008. Vol. 40, No. 1. P. 41-48.
16. Ding C.G., Lin H.-R., Wu Ch,-H., Jane T.-D. Using LGM analysis to identify hidden contributors to risk in the operation of a nuclear power plant // Safety Science. 2015. Vol. 75. P. 64-71.
17. A Guide to the Project Management Body of Knowledge: PMBOK(R) Guide. 5th Ed. Newtown Square, Pennsylvania: Project Management Institute, 2013.