

АЛГОРИТМ ОЦЕНКИ РИСКОВОГО ПОТЕНЦИАЛА РАЗВИТИЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА НА ЭНЕРГОБЛОКЕ АЭС НА ОСНОВЕ ТЕХНИКО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ

Сакрутина Е.А.

Институт проблем управления им. В.А. Трапезникова РАН
consoft@ipu.ru

Аннотация: Для значимых объектов критической информационной инфраструктуры, в том числе и для объектов атомной энергетики, все большую роль играют методы обнаружения аномалий, неисправностей и диагностики, а также системы информационной поддержки оператора с целью повышения безопасности и надежности эксплуатации. Одной из задач решаемой в рамках системы информационной поддержки является задача расчета технико-экономических показателей и ее связь с обеспечением режима нормальной эксплуатации АЭС. Техничко-экономические показатели характеризуют экономичность, безотказность и долговечность энергооборудования в процессе его эксплуатации. Условия оптимальной работы АЭС определяются в процессе анализа ее технико-экономических показателей. Поэтому анализ показателей является одной из важнейших задач АСУ ТП АЭС. Информационная задача расчета технико-экономических показателей в реальном масштабе времени на основе интеллектуального анализа данных и моделей прогноза рискового потенциала критической инфраструктуры объекта позволит оперативному персоналу заблаговременно принять меры для предотвращения выхода технологического процесса за допустимые эксплуатационные пределы.

Ключевые слова: рисковый потенциал, критическая информационная инфраструктура, значимый объект критической информационной инфраструктуры, атомная электростанция, система верхнего блочного уровня; информационная задача; технико-экономические показатели.

Введение

На сегодняшний день в мире приоритетной целью является обеспечение информационной безопасности объектов критической информационной инфраструктуры. Под критической информационной инфраструктурой (КИИ) понимаются объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Среди всех объектов КИИ можно выделить подмножество так называемых значимых объектов критической информационной инфраструктуры (ЗОКИИ). Значимыми объектами КИИ являются объекты КИИ, сбой в работе которых может отразиться на здоровье, безопасности и благосостоянии граждан [1-4]. К ЗОКИИ относятся крупные гидротехнические сооружения, объекты атомной энергетики, вредные химические производства, нефтеперерабатывающие заводы, газопроводы, транспортные системы и т.п. Воздействия компьютерных атак на информационно-технологическую инфраструктуру значимых объектов критической инфраструктуры, приводящие к выходу ее технологических параметров за установленные нормативные пределы, могут повлечь за собой реализацию нештатных ситуаций с тяжелыми и даже катастрофическими последствиями. Для успешной реализации мероприятий защиты значимых объектов критической информационной инфраструктуры необходимо решение ряда задач, из которых система мониторинга угроз безопасности является основной. В последние годы, системные причины многих инцидентов на ЗОКИИ привели к существенному повышению интереса к процедурам идентификации и управления рисками. Система мониторинга угроз безопасности позволит выявить слабые места системы и является лучшим способом предотвращения воздействия любых угроз на систему посредством выявления нештатности протекания технологических процессов на объекте.

Процесс развития автоматизации сложных технологических объектов, нарушения работоспособности которых приводят к большим экономическим, экологическим потерям, угрозам здоровью или жизни людей, характеризуется тенденцией разработки автоматизированных систем управления технологическими процессами (АСУ ТП), реализующих значительно более сложные алгоритмы управления и анализа данных с использованием сложных программно-технических комплексов [5].

При разработке систем для энергетики, где срок эксплуатации основного оборудования исчисляется десятками лет нужно использовать такие решения в АСУ ТП, которые бы позволяли эксплуатировать, ремонтировать и модернизировать поставленное оборудование без остановки

основного технологического процесса. Кроме этого требования, ключевыми требованиями являются обеспечение высокой надежности, живучести и безопасности [6].

Атомная энергетика все более заинтересована в использовании как методов обнаружения и диагностики неисправностей, так и кибератак для повышения безопасности и надежности атомных электростанций [7-9].

СВБУ АЭС, разработанная ИПУ РАН [5, 6], является одной из первых систем управления, в которой при проектировании закладывался глубокий уровень защиты от несанкционированного доступа. Поэтому архитектура системы и интегрированные средства защиты обеспечивают устойчивость системы к кибератакам, возможность обнаружения нарушений в защите, до того, как они приведут к отказу в реализуемых системой функциях. СВБУ предназначена для контроля и управления энергоблоком в режимах нормальной эксплуатации и режимах с нарушением нормальной эксплуатации, включая проектные аварийные режимы работы энергоблока АЭС, но без нарушения пределов и условий безопасной эксплуатации. На основе анализа технико-экономических показателей разрабатываются рекомендации по улучшению управления энергоблоком.

Информационная задача “Расчет технико-экономических показателей” (“IT-TEI”) является расчетной программой и входит в состав прикладного программного обеспечения СВБУ АСУ ТП АЭС. В настоящее время информационная задача “IT-TEI” модернизируется на основе интеллектуального анализа данных [10, 11] и модели прогноза рискованного потенциала критической инфраструктуры [12, 13] с целью предотвращения выхода технологического процесса на критические режимы. Задача “IT-TEI” функционирует в автоматическом режиме.

1 Объект управления

Разработанная система верхнего блочного уровня предназначена для управления энергоблоками АЭС с реакторами типа ВВЭ-1000, принципиальная тепловая схема которых приведена на рис. 1. Технологическая схема энергоблока АЭС с реактором типа ВВЭР-1000 имеет два контура. Первый контур – радиоактивный. Он включает в себя реактор типа ВВЭР-1000 и циркуляционные петли охлаждения. Второй контур – нерадиоактивный. Он включает в себя парогенераторы, паропроводы, паровые турбины, сепараторы-пароперегреватели, питательные насосы и трубопроводы, деаэраторы и регенеративные подогреватели. Парогенератор является общим оборудованием для первого и второго контуров. В нем тепловая энергия, выработанная в реакторе, от первого контура через теплообменные трубки передается второму контуру. Насыщенный пар, вырабатываемый в парогенераторе, по паропроводу поступает на турбину, которая приводит во вращение генератор, вырабатывающий электрический ток.

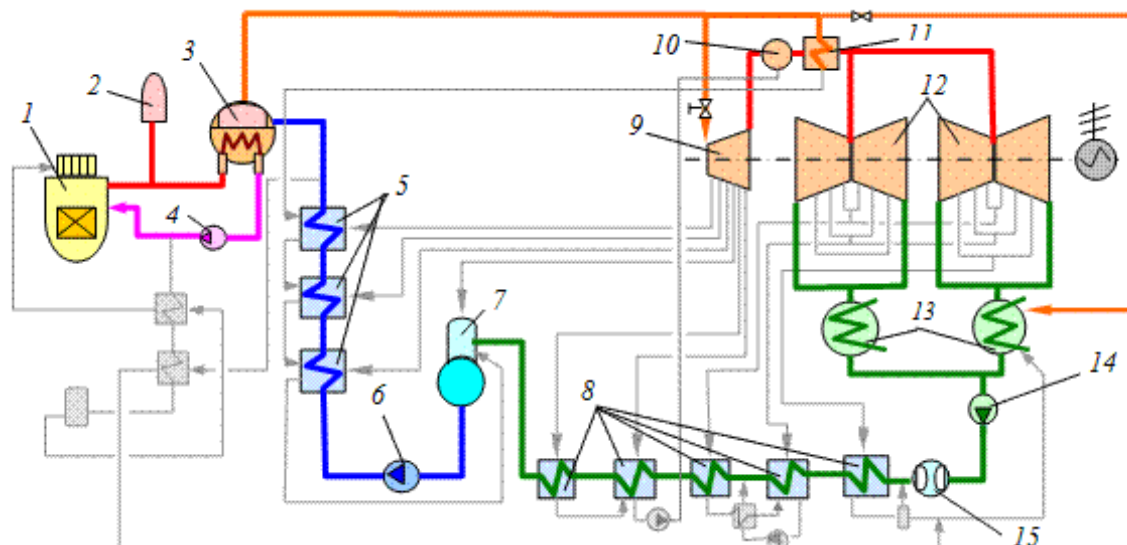


Рис. 1. Принципиальная тепловая схема энергоблока АЭС с реактором ВВЭР-1000: 1- реактор; 2- компенсатор объема; 3- парогенератор; 4- ГЦН; 5- подогреватель высокого давления; 6- питательный насос; 7- деаэратор; 8 – подогреватели низкого давления; 9 – ступени высокого давления турбины; 10 – сепаратор; 11- пароперегреватель; 12 – ступени низкого давления турбины; 13 – конденсаторы; 14- конденсатный насос; 15 - эжекторы.

Рассмотрение имеющихся показателей эффективности, которые могут быть полезны для оценки экономической составляющей не является новой идеей. Целью расчета ТЭП является предоставление информации для наиболее экономичного использования оборудования, прогнозирования его обслуживания и ремонта, для составления отчетности об экономичности энергоблока, а также для прогнозирования рискового потенциала, с целью предотвращения выхода технологического процесса за допустимые эксплуатационные пределы.

2 Проблема неполной оценки параметров

Задача расчета технико-экономических показателей является сильно связанной и отдельные входные сигналы (как дискретные, так и аналоговые) участвуют в вычислениях достаточно большого количества выходных параметров и их недостоверность (например, расход химобессоленной воды в конденсаторы турбины может привести к исключению из расчета до 30% выходных параметров задачи, связанных с этим недостоверным сигналом).

Проблему неполной оценки параметров информационной задачи можно решить на основе интеллектуального анализа данных [10, 11] с использованием корреляционного анализа. В Таблице 1 приведена корреляционная матрица для части параметров информационной задачи “IT-TEI”, где We – активная мощность турбогенератора (один из критических параметров технологического процесса), и V_i – входные параметры задачи. Для оценки We строится прогнозирующая модель на основе входных параметров, имеющих максимальные по абсолютной величине коэффициенты корреляции (V_1, V_2, V_3). Прогнозирующая модель позволяет оперативно оценивать все параметры работы энергоблока в части информационной задачи “IT-TEI” даже в случае отсутствия или недостоверности части измерений, а также на основе прогноза оценивать рисковый потенциал выхода технологического процесса за эксплуатационные пределы.

Таблица 1. Корреляционная матрица

| | We | V_1 | V_2 | V_3 | V_4 | V_5 | V_6 | V_7 | V_8 | V_9 | V_{10} | V_{11} |
|----------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|
| We | 1,00 | | | | | | | | | | | |
| V_1 | -0,48 | 1,00 | | | | | | | | | | |
| V_2 | -0,52 | 0,40 | 1,00 | | | | | | | | | |
| V_3 | -0,58 | 0,68 | 0,74 | 1,00 | | | | | | | | |
| V_4 | -0,31 | 0,60 | 0,60 | 0,84 | 1,00 | | | | | | | |
| V_5 | -0,41 | 0,73 | 0,20 | 0,32 | 0,24 | 1,00 | | | | | | |
| V_6 | -0,46 | 0,90 | 0,51 | 0,67 | 0,59 | 0,57 | 1,00 | | | | | |
| V_7 | -0,43 | 0,85 | 0,29 | 0,51 | 0,50 | 0,89 | 0,74 | 1,00 | | | | |
| V_8 | -0,33 | 0,52 | 0,63 | 0,62 | 0,55 | 0,43 | 0,71 | 0,53 | 1,00 | | | |
| V_9 | 0,47 | -0,61 | -0,29 | -0,52 | -0,38 | -0,54 | -0,48 | -0,56 | -0,27 | 1,00 | | |
| V_{10} | 0,38 | -0,20 | -0,10 | -0,22 | -0,14 | -0,02 | -0,09 | -0,02 | 0,16 | 0,05 | 1,00 | |
| V_{11} | 0,45 | -0,69 | -0,44 | -0,76 | -0,64 | -0,35 | -0,55 | -0,43 | -0,31 | 0,52 | 0,35 | 1,00 |

3 Алгоритм оценки рискового потенциала

Алгоритм оценки рискового потенциала заключается в определении положения значений текущих критических параметров по отношению к границам нормальной эксплуатации. Выход критических параметров технологического процесса за границы нормальной эксплуатации свидетельствуют о высоком рисковом потенциале, нахождение значений критических параметров на границах нормальной эксплуатации – о среднем рисковом потенциале, а нахождение критических параметров в рамках нормальной эксплуатации – о низком рисковом потенциале.

Чаще всего оценка рискового потенциала происходит в условиях неопределенности. В связи с этим необходим инструмент, позволяющий осуществлять оценку влияния различных рискообразующих факторов на прохождение технологического процесса, оценку интегрального рискового потенциала на основе всех критических параметров и разработку системы управления рисками. Стоит отметить, что в условиях неопределенности анализ рисков и рискового потенциала

проводить затруднительно, так как нелегко выявить их природу, источники и потенциальные последствия, поэтому в последнее время широкое распространение получили аналитические методы, основанные на интеллектуальных технологиях, которые применяются при решении задач прогнозирования [10], в том числе и прогнозирования рискованного потенциала [13]. На рис. 2 представлен обобщенный алгоритм оценки и контроля рискованного потенциала протекания технологического процесса.

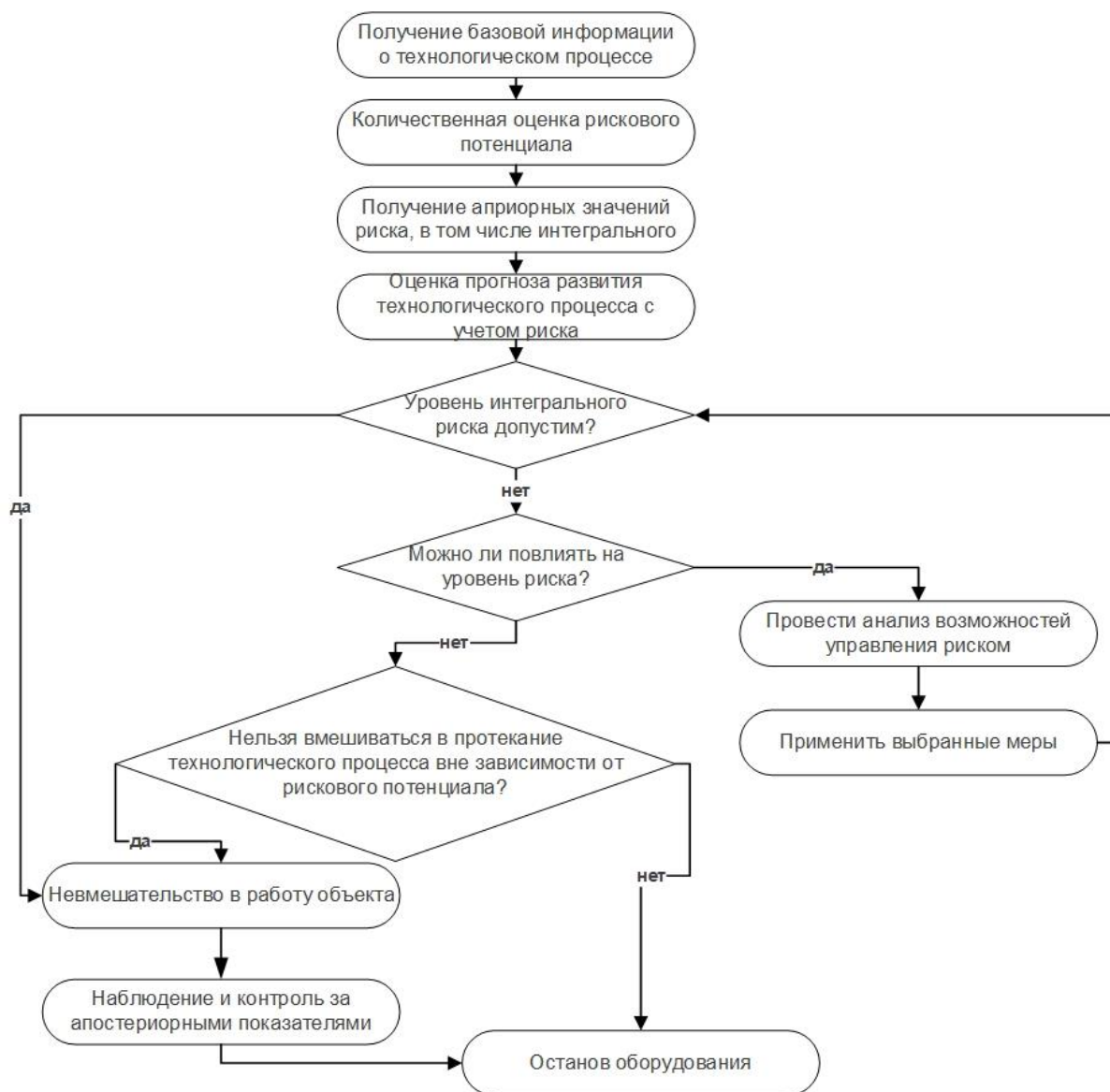


Рис. 2. Обобщенный алгоритм оценки и контроля рискованного потенциала протекания технологического процесса.

Заключение

Дополнение информационной задачи “Расчет технико-экономических показателей” (“IT-TEP”) интеллектуальным анализом данных [10, 11] и моделями прогноза рискованного потенциала позволит не только обеспечивать административный персонал АЭС оперативной информацией о работе энергоблока, но и осуществлять организационно-технические мероприятия по экономии энергоресурсов на основе рекомендаций по улучшению управления энергоблоком.

Литература

1. Critical Infrastructure: Cyber-attacks on the backbone of today’s economy. PandaSecurity, 2016.
2. PandaLabs Annual Report, PandaSecurity, 2018.
3. Tsegaye T., Flowerday S. Controls for Protecting Critical Information Infrastructure from Cyberattacks // Proceedings of the World Congress on Internet Security (WorldCIS-2014). 2014. – P.24-29.

4. *Hamida Y., Amine B., Mostafa B.* Toward resilience management in critical information infrastructure // Proceedings of the 5th World Congress on Information and Communication Technologies (WICT). 2015. – P.101-106.
5. *Бывайков М.Е., Жарко Е.Ф., Менгазетдинов Н.Э., Полетыкин А.Г., Прангшвили И.В.* Опыт проектирования и внедрения системы верхнего блочного уровня АСУ ТП АЭС // Автоматика и телемеханика. Т. 5. 2006. – С.65-79.
6. *Poletykin A., Jharko E., Mengazetdinov N., Promyslov V.* Some Issues of Creating the New Generation of Upper Level Control Systems of NPP APCS // Proceedings of the 5th International Conference on Control, Instrumentation, and Automation (ICCIA 2017, Shiraz, Iran). 2017. – P.78-83.
7. *Hashemian H.M.* Maintenance of Process Instrumentation in Nuclear Power Plant – Springer-Verlag, Berlin Heidelberg, 2006.
8. *Hashemian H.M., Feltus M.A.* On-Line Condition Monitoring Applications in Nuclear Power Plants // NPIC&HMIT, Albuquerque, NM, USA. 2006. – P.568-577.
9. *Ma J., Jiang J.* Applications of fault detection and diagnosis methods in nuclear power plants: A review // Progress in Nuclear Energy. Vol. 53. 2011, №3. – P.255-266.
10. *Bakhtadze N., Sakrutina E.* Applying the Multi-Scale Wavelet-Transform to the Identification of Non-linear Time-varying Plants // Applying the Multi-Scale Wavelet-Transform to the Identification of Non-linear Time-varying Plants. Vol. 49. 2016, №12. – P.1927-1932.
11. *Sakrutina E.* The process state identification methodology based on the associative search // Proceedings of the IEEE International Siberian Conference on Control and Communications (SIBCON-2017, Astana). 2017. – P.1-5.
12. *Калашиников А.О., Сакрутина Е.А.* Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа // Информация и безопасность. Т.20. 2017, №4. – С. 478-491.
13. *Калашиников 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, Москва). М.: ИПУ РАН. Т. 2. 2018. – С. 457-461.