ПАПКОВ Б.В.
ИЛЮШИН П.В.
КУЛИКОВ А.Л.

НАДЁЖНОСТЬ И ЭФФЕКТИВНОСТЬ СОВРЕМЕННОГО ЭЛЕКТРОСНАБЖЕНИЯ

МОНОГРАФИЯ

Папков Б.В.
Илюшин П.В.
Куликов А.Л.

НАДЁЖНОСТЬ И ЭФФЕКТИВНОСТЬ СОВРЕМЕННОГО ЭЛЕКТРОСНАБЖЕНИЯ

Монография

Нижний Новгород
2021

УДК 621.311+621.316
ББК 31.27
П 17

Р е ц е н з е н т ы :

Чукреев Ю.Я., д-р техн. наук, старший научный сотрудник, директор Института социально-экономических и энергетических проблем Севера Коми научного центра Уральского отделения Российской академии наук;

Шуин В.А., д-р техн. наук, профессор, профессор кафедры «Автоматическое управление электроэнергетическими системами» ФГБОУ ВО «Ивановский государственный энергетический университет им. В.И. Ленина».

П 17

Папков Б.В.

Надёжность и эффективность современного электроснабжения: монография / Б.В. Папков, П.В. Илюшин, А.Л. Куликов. – Нижний Новгород: Научно-издательский центр «XXI век», 2021. – 160 с.

ISBN 978-5-6045837-5-3

В монографии изложены основы системного подхода к анализу современных систем электроснабжения (СЭС). Приведены основные определения, необходимые для понимания и оценки сложности СЭС. Рассмотрен математический аппарат, используемый для решения задач создания, эксплуатации и развития СЭС. Отмечена необходимость учёта особенностей структурного построения схем технологических процессов потребителей и режимов их работы. Приведённые числовые примеры наглядно иллюстрируют теоретический материал, уделяя внимание содержательному описанию задач, методов их решения и толкованию полученных результатов.

В работе дано формализованное описание современных СЭС, отмечена необходимость расширения понятия «надёжность», рассмотрены вопросы кибербезопасности. Особое внимание уделено задачам оценки надёжности и эффективности структур СЭС с учётом развития систем распределённой генерации. Даны рекомендации по оценке вероятностей катастрофических ситуаций и вопросам, связанным с оценкой и управлением риском при обеспечении надёжности СЭС.

Издание предназначено для специалистов в области исследования, проектирования и эксплуатации СЭС, студентов, магистрантов и аспирантов всех форм обучения по направлению «Электроэнергетика».

УДК 621.311+621.316
ББК 31.27

ISBN 978-5-6045837-5-3

СОДЕРЖАНИЕ

АББРЕВИАТУРЫ

АЧР – автоматическая частотная разгрузка
АЭС – атомная электрическая станция
ВБР – вероятность безотказной работы
ВИЭ – возобновляемый источник энергии
ГПП – главная понизительная подстанция
ГЭС – гидроэлектростанция
ДФ – дестабилизирующий фактор
ЕНЭС – единая национальная (общероссийская) электрическая сеть
ЕЭС – единая энергетическая система
ЖКХ – жилищно-коммунальное хозяйство
ИКС – информационно-коммуникационные системы
ИЭС – интеллектуальная электрическая сеть
КВО – критически важный объект
КИУМ– коэффициент использования установленной мощности
ЛПР – лицо, принимающее решение
ЛЭП – линия электропередачи
НСД – несанкционированный доступ
НЭ – накопитель электроэнергии
ПА – противоаварийная автоматика
РГ – распределённая генерация
РЗ – релейная защита
РЗА – релейная защита и автоматика
РП – распределительная подстанция
СЗИ – система защиты информации
СТС – сложная техническая система
СЭС – система электроснабжения
СЭС – системообразующая электрическая сеть
ТП – трансформаторная подстанция
ТСО – территориальная сетевая организация
ТЭР – топливно-энергетические ресурсы
ЭСО – энергоснабжающая организация
ЭЭС – электроэнергетическая система
CPS – cyber-physical systems (киберфизическая система)

ВВЕДЕНИЕ

Одним из важных направлений системных исследований в энергетике является изучение проблемы надёжности и эффективности электроснабжения потребителей. Системы электроснабжения (СЭС) промышленных предприятий, предприятий агропромышленного комплекса, электрифицированного транспорта, магистральных нефте- и газопроводов, ЖКХ, крупных объектов торговли и социального назначения являются одной из подсистем электроэнергетической системы (ЭЭС) и основой её формирования. В состав ряда СЭС включены источники малой и распределённой генерации (РГ), в том числе возобновляемые источники энергии (ВИЭ). Всё более широкое применение интеллектуальных систем управления электрическими сетями, элементами электрооборудования и режимами потребления электроэнергии требуют исследования и анализа СЭС с позиций теории систем. Актуальность этих задач несомненна, поскольку свойства, режимы и параметры СЭС существенным образом определяют свойства и тенденции развития систем энергетики и энергетических комплексов, включая как традиционную ЭЭС, так и объекты РГ с традиционными и ВИЭ.

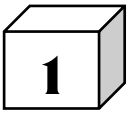
Современные СЭС представляют совокупность связанных между собой электроустановок и электрических устройств, предназначенных для обеспечения электроэнергией различных потребителей (приемников электрической энергии). Системный подход к разработке и исследованию режимов функционирования СЭС основан на результатах анализа связанных с СЭС технологических процессов производства продукции, технико-экономического анализа последствий управления режимами электропотребления, анализа возможных изменений экологических и социальных показателей. Системы потребления также, как и СЭС (ЭЭС) обладают временно́й, структурной, нагрузочной и информационной избыточностью, за счет которой можно ликвидировать или значительно уменьшить недовыпуск товарной продукции из-за нарушения нормального режима их работы и не допустить разрыва внешних производственных связей. Поэтому при решении комплексных задач создания, размещения и использования генерирующих мощностей (в том числе систем РГ) необходимо учесть возможность рационального использования имеющихся, включая все виды резервов потребителей.

Совместное использование избыточности ЭЭС, систем РГ, ВИЭ и потребителей основано на рациональном подборе объектов, управление режимами которых приводит к минимуму экономических потерь. Вместе с тем известно, что разработка методических принципов решения поставленных задач достаточно сложна. Это связано с трудностями прогноза спроса мощности и энергии потребителями, а ретроспективный анализ режимов электропотребления не может обеспечить получение достоверных оценок ожидаемых нагрузок. Аналогичная ситуация и с прогнозированием возможных ущербов. Поэтому сейчас очевидна необходимость исследований возможностей как ЭЭС, (РГ, ВИЭ) так и потребителей при управлении режимами электропотребления в нормальных и аварийных условиях, а также при прогнозировании развития СЭС и ЭЭС с учётом особенностей электроснабжения технологических систем потребителя. Анализ предельных параметров возможных состояний реальных производственных систем позволяет выработать требования к надёжности их внешнего энергоснабжения с учетом длительности введения режима регулирования, его периодичности, глубины ограничения. Это послужит основанием для согласованного изменения графика нагрузки с одновременной минимизацией экономических последствий изменения нормального режима электропотребления.

Системы электроснабжения стали такими, что в них постоянно что-то происходит: изменяется режим электропотребления, напряжение на шинах потребителя, возникают отказы отдельных элементов, сбои устройств РЗА и другие случайные события. Глубокое понимание физических основ поставленных задач требует системного подхода, основой которого является формализованное описание исследуемой СЭС с учётом технологических особенностей потребителя. Поэтому в монографии на примере СЭС рассматриваются проблемы больших технических систем и основы их формализованного описания; даны рекомендации по расширению надёжностных свойств СЭС при анализе кибербезопасности интеллектуальных электрических сетей; даны основы оценки вероятностей катастрофических ситуаций в СЭС; показаны возможности учёта особенностей структур систем РГ при оценке их надёжности и эффективности; рассмотрены возможности реализации задач риск менеджмента.

Материалы, представленные в монографии, неоднократно докладывались на постоянно действующем международном семинаре им. Ю.Н. Руденко «Методические вопросы исследования надёжности больших систем энергетики» при Институте систем энергетики им. Л.А. Мелентьева (ИСЭМ) СО РАН.

Монография рассчитана на широкий круг читателей, занимающихся теорией и практикой обеспечения надёжности систем энергетики, включая научных работников и специалистов, занятых в сфере электроэнергетики и электроснабжения, проектировщиков, студентов, магистрантов и аспирантов энергетических специальностей.



1 СИСТЕМА ЭЛЕКТРОСНАБЖЕНИЯ – БОЛЬШАЯ И СЛОЖНАЯ СИСТЕМА

1.1. Вводные замечания

Осложнение энергетической ситуации в мире связано с ростом энергопотребления, ограниченностью запасов традиционных ископаемых органических энергоресурсов, конкуренцией на рынках топливно-энергетических ресурсов (ТЭР), повышением экологических требований к технологиям и оборудованию. Современная электроэнергетика определяет условия жизнедеятельности и развития общества, а мировая потребность в электроэнергии продолжает расти. Ещё в большей степени растут требования к надёжности, безопасности и качеству электроснабжения, так как в условиях высокой конкуренции растёт количество отказов и связанная с ними стоимость простоя оборудования потребителей.

Исследование процессов функционирования систем электроэнергетики с учётом развития интеллектуальных электрических сетей (ИЭС), автоматизированного контроля параметров и управления режимами, необходимости обработки большого количества оперативной информации, внедрения распределённой генерации (РГ), ВИЭ и накопителей электроэнергии (НЭ) обусловило необходимость уточнения и развития понятия сложной системы, что привело к постановке проблем методического, математического и технологического плана.

Наиболее характерная структурная особенность сложной системы (сети, деревья, иерархические структуры) состоит во взаимосвязанности её элементов, которая обеспечивает ей возможность принимать большое число состояний, приспосабливаясь к изменению внешних условий и разрешая внутренние противоречия. Современный мир сложных (больших) технических, экономических и социальных систем отличается сильными взаимозависимостями между элементами, нелинейными реакциями на внешние и внутренние воздействия, зависит от редких (крайне редких) событий. Такие показатели, как:

- многообразие природы элементов (технологические агрегаты, системы автоматики, люди-операторы);
- количество элементов (объём оборудования), составляющих систему;
- структура связей между ними;

- квалификация персонала, осуществляющего создание системы, её монтаж, наладку, эксплуатацию;
- удобство эксплуатации и т. п.

уже дают интуитивное представление о сложности системы, которая является одной из основных её характеристик.

При разработке и в условиях эксплуатации в целевом пространстве системы S необходим выбор её поведения ξ, отвечающего совокупности поставленных условий (требований) α. Эта совокупность и определяет сложность, которая должна быть минимальна при оптимальном поведении ξ_*. Интуитивно сложная система – это система, статическая структура или динамическое поведение которой непредсказуемы, «запутаны», противоречат «здравому смыслу» и т. д. [26]. По [73] сложность системы в обобщённом виде представляется показателем, характеризующим техническое воплощение решений, обеспечивающих достижение основной цели её функционирования при заданном уровне качества управления. При этом качество управления – показатель, характеризующий степень (или полноту) выполняемой системой основной цели.

1.2. Основные определения

Понятие «система» – достаточно широко и размыто, поскольку оно относится к числу наиболее общих и универсальных. Дать определение, относящееся ко всем без исключения видам систем и, вместе с тем, четко выделяющее их из внесистемных объектов, на современном этапе развития общей теории систем практически невозможно.

Хотя фундаментальная наука предъявляет достаточно жесткие требования к формулировкам различных терминов и понятий, требуя их четкости и однозначности, выполнение их для определения понятия «система» пока не удается. Количество и содержание таких определений обусловлено большим разнообразием типов систем и разными задачами, возникающими при их исследовании, проектировании, монтаже и наладке, эксплуатации, ликвидации. Определения понятия «система» в течение многих лет изменялись не только по форме, но и по содержанию, которые происходили по мере развития теории систем и использования этого понятия на практике. В общем случае под системой S понимается непустое множество, класс или область T объектов, между которыми установлены некоторые отношения. Наиболее распространенные смысловые вариации этого понятия приведены в [54].

Система:

1) сущность, которая в результате взаимодействия её частей может поддерживать своё существование и функционировать как единое целое;

2) термин, используемый в случаях, когда исследуемый или проектируемый объект характеризуется как нечто целое (единое), сложное, о котором невозможно сразу дать представление, показав его, изобразив графически или описав математическим выражением (формулой, уравнением и т. п.);

3) любое, достаточно сложное образование, состоящее из множества взаимосвязанных элементов, которые как единое целое взаимодействуют с внешней средой;

4) совокупность элементов, объединенных конструкционно и (или) функционально для выполнения некоторых требуемых функций;

5) составной объект любого уровня сложности, который может включать персонал, процедуры, материалы, инструменты, оборудование, средства обслуживания, программное обеспечение;

6) объективное единство закономерно связанных друг с другом предметов, явлений, знаний о природе и обществе;

7) совокупность большого числа элементов с заданными между ними законами взаимодействия;

8) организованное множество элементов, находящихся в отношениях и связях между собой, образующих некоторое целостное единство;

9) объект, представляющий собой множество элементов, находящихся в рациональных (целесообразных, устойчивых, упорядоченных, предсказуемых) отношениях и связях между собой и образующих целостность (единство), границы которого задаются пределами управления;

10) множество взаимосвязанных элементов (подсистем), отношения которых между собой порождают системное качество интегративности и которые в совокупности обладают свойствами, не сводящимися к свойствам отдельных элементов (или подсистем);

11) совокупность элементов со связями и целью функционирования, отличной от целей функционирования отдельных элементов;

12) конечное множество функциональных элементов и отношений между ними, выделенное из среды в соответствии с определенной целью, в рамках определенного временного интервала;

13) отграниченное, взаимосвязанное множество, отражающее объективное существование конкретных отдельных взаимосвязанных совокупностей и не содержащее специфических ограничений, присущих этим частным совокупностям.

Относительно систем электроэнергетики и электроснабжения отметим, что определения их более конкретны. Так, например:

- система энергетики – открытая (большая, сложная) человеко-машинная производственная система, предназначенная для добычи (про-

изводства, получения), переработки (преобразования), передачи, хранения и распределения соответствующего энергоресурса и снабжения им потребителей;

- энергетическая система – 1) совокупность энергетических ресурсов всех видов, методов их получения, преобразования, распределения и использования, а также технических средств и организационных комплексов, обеспечивающих потребителей всеми видами энергии; 2) совокупность электростанций, электрических и тепловых сетей (независимо от форм и принадлежности собственности), энергопотребляющих установок потребителей, соединенных между собой и связанных общностью режима в процессе производства, преобразования, распределения и потребления электрической энергии и тепла при общем управлении этим режимом;
- электроэнергетическая система (ЭЭС) – 1) система энергетики, представляющая собой совокупность электрических станций, электрических и тепловых сетей, узлов потребления электрической энергии и тепла, объединенных процессом их производства, преобразования, передачи, распределения и предназначенная для снабжения потребителей электрической энергией и теплом; 2) совокупность электрических станций, электрических сетей и энергопринимающих устройств потребителей электрической энергии, связанных общностью режима в непрерывном процессе производства, передачи, распределения и потребления электрической энергии в условиях централизованного оперативно-диспетчерского управления в электроэнергетике; 3) группа из одного или более генерирующих источников, подстанций и объединяющих передающих и распределительных линий, находящихся под единым управлением и руководством, для снабжения потребителей; 4) электрическая часть энергосистемы и питающиеся от нее приемники электроэнергии, объединенные общностью процесса производства, передачи, распределения и потребления электроэнергии;
- электрическая система – условно выделенная часть энергосистемы, в которой генерируется, преобразуется, передается и потребляется электрическая энергия;
- система электроснабжения – 1) совокупность взаимосвязанных объектов электроэнергетики (электроустановок), предназначенных для обеспечения потребителей электроэнергией; 2) система, объединенная общим процессом генерирования и (или) преобразования, передачи и распределения электрической энергии и состоящая из источников и (или) преобразователей электрической энергии, электрических сетей, распределительных устройств, а также устройств, обеспечивающих поддержание её параметров в заданных пределах.

Такое количество приведённых определений не отнимает права на существование каждого из них. Анализируя различные определения системы, не выделяя ни одно из них в качестве основного, отметим, что,

во-первых, практически все их можно с уверенностью отнести к ЭЭС;

во-вторых, на разных этапах представления объекта в виде системы, в различных конкретных ситуациях (проектирование, монтаж, наладка, эксплуатация, утилизация), можно и нужно пользоваться разными определениями;

в-третьих, по мере уточнения представлений о системе или при её развитии, переходе на другой уровень её исследования определение системы не только может, но и должно уточняться.

В общем случае под системой S понимается непустое множество, класс или область T объектов, между которыми установлены некоторые отношения.

Выше отмечалось, что система состоит из большого количества взаимосвязанных элементов. Понятие элемента системы и расчленение её на элементы на практике весьма условно. Рассматривая ЭЭС как сложную систему, её элементами можно считать территориальные, региональные и районные системы. Если, например, региональная ЭЭС рассматривается как сложная, то элементами её могут быть системы электроснабжения (СЭС) потребителей. Для СЭС элементами являются линии электропередачи (ЛЭП), трансформаторы, коммутационная аппаратура и т. д. При формальном подходе элемент – объект, не подлежащий дальнейшему расчленению при данном рассмотрении исследуемой системы [6, 7]. При этом внутренняя структура элемента не является предметом изучения. Существенны только такие его свойства, которые определяют его взаимодействие с другими элементами или влияют на свойства системы в целом.

Общая схема формального описания элементов большой системы может быть представлена в виде агрегата. Особое значение выделение агрегатов приобретает при решении задач оценки технико-экономических последствий (ущерба) от внезапных нарушений электроснабжения технологических установок производств и плановых изменений режимов их электропотребления [50]. При этом считается, что в каждый момент времени $t \in (0, T)$ выделенный агрегат находится в одном из возможных состояний, характеризующихся набором показателей $\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n$. Поскольку время работы t изменяется в интервале $(0, T)$, показатели α_i, также изменяются в функции времени $\alpha_i(t)$ и являются фазовыми траекториями движения системы.

Очевидно, что рациональное выделение элементов, агрегатов и подсистем способствует упрощению расчётов при исследовании и более наглядному представлению его результатов.

Приведенные рассуждения позволяют сформулировать общий принцип образования систем: совокупность материальных или идеальных объектов, имеющих общие признаки, объединяется в систему, которая сама по себе являясь объектом, обладает свойствами, отличными от свойств объектов её составляющих. Другими словами, система – это полный, целостный набор элементов (компонентов), взаимосвязанных и взаимодействующих между собой так, чтобы могла реализоваться функция системы. В зависимости от постановки задачи детальность деления системы на подсистемы (компоненты) может быть разной, в результате чего складывается иерархия (многоступенчатость, упорядоченность) систем.

Итак, сущность такого широкого и ёмкого понятия, как «система» невозможно раскрыть и соответственно сформулировать в виде сколь угодно сложного, но однозначного определения. На практике это понятие признается открытым, непрерывно развивающимся понятийным объектом, не определяемым исчерпывающим образом в рамках каких бы то ни было логических или формальных построений.

1.3. Основы классификации

При классификации обычно выделяют простые, большие и сложные системы. Однако эта классификация довольно условна и зависит от требуемой цели и постановки задачи, в зависимости от чего ту или иную систему можно отнести к разряду сложных больших или простых.

Идеальная простая система состоит из относительно небольшого числа элементов, не имеет разветвленной структуры, ориентирована на достижение одной цели, её функционирование не зависит от внешних условий и не изменяется с течением времени. В качестве терминологического определения элемента системы обычно используются следующие:

- элемент – 1) простейшая, неделимая при конкретной постановке задачи исследования часть системы; 2) предел членения системы с точки зрения решения конкретной задачи, поставленной цели; 3) материальный, энергетический, информационный объект, рассматриваемый при проведении анализа как единое целое, не подлежащее дальнейшему разукрупнению;
- элемент системы электроэнергетики – 1) объект электроэнергетики, представляющий собой законченное устройство, способное самостоятельно выполнять некоторые локальные функции при производстве, преобразовании, передаче, распределении и потреблении электроэнергии и являющийся частью системы энергетики (отдельные агрегаты электрических станций, электростанции в целом, группы электростанций, ЛЭП, трансфор-

маторы, подстанции, электродвигатели и другие элементы ЭЭС и СЭС); 2) часть (подсистема) системы энергетики, выделяемая с точки зрения либо оперативно-диспетчерского управления, либо выполняемых функций, либо решаемых задач.

В случаях, когда система не может быть сразу разделена на составляющие, являющиеся пределом ее членения, термин «элемент» используется в более широком смысле. Если части системы полностью или частично не обладают свойствами подсистемы, их принято называть компонентами системы. Понятие «компонент» определяется как любая часть системы, вступающая в определенные отношения с другими частями (подсистемами, элементами).

Формально любая совокупность элементов данной системы вместе со связями между ними может рассматриваться как ее подсистема. Однако использование этого понятия наиболее плодотворно в тех случаях, когда в качестве подсистем фигурируют некоторые более или менее самостоятельные части системы. Систему можно расчленять на элементы различными способами в зависимости от формулировки задачи, цели и ее уточнения в процессе проведения системного исследования. При необходимости можно изменять принцип расчленения, выделять другие элементы и получать с помощью нового расчленения более адекватное представление об анализируемом объекте или проблемной ситуации. Выделение подсистем является важным этапом формального описания системы. Оно позволяет упростить исследования, путем уменьшения количества связей и упрощения вычислительных процедур.

В качестве примера рассмотрим систему из $n = 20$ элементов, которую характеризуют

$$N = n(n-1) = 380$$

связей.

Предположим, что она расчленяется на $m = 4$ подсистемы по $k = 5$ элементов в каждой. Количество возможных связей между элементами подсистем

$$P = [k(k-1)]m = 5 \cdot 4 \cdot 4 = 80.$$

Число связей между подсистемами определится как

$$R = m(m-1) = 4 \cdot 3 = 12.$$

Если связи между элементами выделенных подсистем по условиям поставленной задачи можно не учитывать, то общее число связей вместо $N = 380$, составит только

$$C = P + R = 80 + 12 = 92,$$

то есть, более чем в 4 раза меньше, чем в начальной стадии исследования.

1.4. Особенности «простых» систем

Простая система может находиться только в двух состояниях: работоспособном (исправном) и в состоянии отказа. Её отличительная особенность – отсутствие разветвлённой структуры, детерминированность номенклатуры режимов, числа элементов и связей как внутри системы, так и с внешней средой. Естественно, что подобные системы служат моделями простейших процессов. К таким системам прежде всего относятся невосстанавливаемые элементы систем электроснабжения (электрические лампы, плавкие вставки предохранителей, выключатели низкого напряжения, различные реле и другие слаботочные коммутационные аппараты и измерительные приборы). Признаком простой системы считают также сравнительно небольшой объем информации, требуемый для её успешного управления.

Так как реальные простые системы достаточно далеки от идеальных, в них обычно не выделяются иерархические уровни. Однако они могут представлять хорошо организованные и управляемые взаимосвязанные элементы, обеспечивающие выполнение заданных функций с каким-то одним определённым качеством функционирования. Хотя динамические характеристики простых систем в большей своей части линейны, реакция их на внешние воздействия может быть неоднозначной, но в среднем вполне предсказуемой. Это в терминах причины и следствия позволяет отслеживать, оценивать, прогнозировать их будущее функционирование и восстанавливать прошлые состояния. При этом реакция реальных простых систем на внешние воздействия может быть и неоднозначной, но в среднем вполне предсказуемой.

Особо отметим, что при отказе любого элемента отдельные простые системы могут продолжить в полном объеме выполнение своей функции, если отказавший элемент имеет постоянно включённый 100 % общий резерв. Кроме того, простая система может быть восстанавливаемой, если процесс восстановления моделируется экспоненциальным распределением времени обслуживания и пуассоновским потоком отказов.

Поскольку реальных простых систем практически не существует, простая система – частный случай (подсистема, элемент), в котором достижим идеал исчерпывающего описания реальной системы. Поэтому возникла необходимость введения понятия класса, так называемых, больших систем.

1.5. Особенности «больших» систем

В реально существующих больших системах число подсистем достаточно велико, а состав их чрезвычайно разнороден. При этом физические

размеры объекта, количество элементов и связей не являются критерием отнесения его к классу больших систем. В зависимости от цели исследования и имеющихся ресурсов, его можно отнести или нет к классу больших систем. Так, рассмотренные выше простые системы с резервированием и возможностью восстановления вполне соответствуют большим. Поэтому один и тот же объект электроэнергетики с точки зрения наблюдателя (исследователя, разработчика, менеджера, экономиста, эколога) может быть представлен как большая система, если она в каком-то аспекте, важном для достижения цели, превосходит его возможности.

Большие системы одновременно ненаблюдаемы и (или) неуправляемы с позиции одного наблюдателя во времени и (или) в пространстве. Потому исследование (моделирование) их поведения затруднено из-за большой размерности (множество функций, состояний, режимов, параметров). Сведение большой системы к системе меньшей размерности возможно при использовании более мощных вычислительных средств (ресурсов) либо разбиением (если возможно) её на ряд подсистем меньшей размерности. При этом большая система может быть описана как бы на одном языке, с помощью единого метода моделирования, хотя и по частям, подсистемам. Но об этой возможности можно судить только для конкретной системы (проблемы), конкретной цели её исследования и конкретных ресурсов.

Известно, что профилактике должно уделяться большое внимание, но и результаты её должны быть правильно истолкованы.

Представим, что анализируются СЭС двух предприятий: 1) «большого», с количеством установленных трансформаторов 10/0,4 кВ мощностью 1000 кВ·А $n_{\text{Б}} = 100$ штук; 2) «маленького», с количеством установленных на нём трансформаторов 10/0,4 кВ мощностью 1000 кВ·А – $n_{\text{М}} = 10$ штук.

Предположим, что все трансформаторы 10/0,4 кВ идентичны: одинаковый срок службы, работа в одинаковых режимах при одинаковых условиях эксплуатации. В результате технической диагностики $m = 5$ (пяти) случайно отобранных трансформаторов одного из предприятий установлено, что $k = 2$ (два) трансформатора нуждаются в ремонте.

На каком предприятии это скорее всего могло бы произойти?

Первая мысль, что этот результат может быть отнесён как к «большому», так и к «малому» предприятию.

Вторая, что этот результат относится к «большому» предприятию, так как ремонт двух трансформаторов при большом их числе кажется более вероятным. Это заключение основано на предположении, что вероятность отказа любого трансформатора в заданных (стационарных) условиях эксплуатации постоянна.

На самом деле, количество вариантов случайной выборки для диагностирования 5 трансформаторов из 100 равно

$$C_{100}^{5} = \frac{100!}{(100-5)! \cdot 5!} = 75287520,$$

а количество случайной выборки 5 трансформаторов из 10:

$$C_{10}^{5} = \frac{10!}{(10-5)! \cdot 5!} = 252.$$

Количество вариантов того, что из 5 трансформаторов 2 нуждаются в ремонте

$$C_{5}^{2} = \frac{5!}{(5-2)! \cdot 2!} = 10.$$

Соответственно, оценка вероятности того, что трансформаторы, нуждающиеся в ремонте, находятся на «большом» предприятии

$$P_{\text{Б}}^{*} = \frac{10}{75287520} \approx 0{,}13 \cdot 10^{-6},$$

а на «малом» –

$$P_{\text{М}}^{*} = \frac{10}{252} = 0{,}04.$$

В ряде простейших случаев большую систему можно представить как совокупность множества однородных элементов, объединенных связями одного типа. Например, известно, что при проектировании ЭЭС и СЭС широко используется критерий *n*–1, определяющий схемно-технические решения, при которых вывод из работы одного любого (в том числе наиболее нагруженного) элемента не приводит к ограничению электроснабжения потребителей. Но для оценки показателей надежности функционирования ЭЭС (СЭС) необходим перечень сценариев, приводящих к возможным множественным отключениям в сети и ограничениям электроснабжения потребителей. Для этого в принципе возможно использование критерия *n*–*k*, где *k* – количество одновременно отключаемых элементов.

Прямое решение этой задачи предполагает проведение расчетов, количество которых определяется множеством сценариев функционирования (сочетаний из *n* по *k*):

$$\mathrm{C}_{N}^{k} = \frac{N!}{(N-k)! \cdot k!}$$

Так, для относительно небольшой схемы, содержащей $n = 100$ элементов (суммарное количество узлов и ветвей), в случае применения критерия *n*–2 число сценариев будет – 4950, а при критерии *n*–3 – уже 161700.

С другой стороны, если речь идет о системе, состоящей из n элементов, необходимо рассматривать

$$N = n(n-1)$$

возможных связей между её элементами, учитывая, что в общем случае связь элемента a с элементом b не эквивалентна связи между элементами b и a.

Если характеризовать состояние каждой связи наличием – 1 или отсутствием – 0 в данный момент определенного воздействия (что на практике часто недостаточно), то число состояний определится как

$$S = 2^N = 2^{n(n-1)}.$$

Кроме того, каждый объект n_i такой системы может находиться в нескольких d режимах (работоспособный, частично работоспособный, резерв, ремонт и т. п.). Тогда число расчетных режимов (состояний) составит

$$K = (d!)^n.$$

При этом общее число состояний M будет определяться произведением числа состояний S на число режимов K:

$$M = SK.$$

Легко видеть, что для большой системы это число может оказаться громадным даже при относительно небольших значениях d и n.

Так, если решается задача оценки возможного ущерба при нарушениях нормального режима электроснабжения, и СЭС предприятия обеспечивает питание всего $n = 3$ технологических установок, то число возможных технологических связей между ними – $N = 6$ и, соответственно, количество состояний этих связей – $S = 2^6 = 64$. Если каждая установка может работать в $d = 3$ режимах (работоспособна, неработоспособна, частично работоспособна) получим еще $K = (3!)^3 = 216$ состояний. При этом общее число состояний технологической схемы будет: $M = 64 \cdot 216 = 13\,824$.

Развитие современных СЭС привело к тому, что они должны рассматриваться как системы, состоящие из большого числа разнородных и взаимосвязанных элементов со сложной структурой и алгоритмами функционирования. Это требует разработки специальных методов обеспечения, повышения и поддержания их надёжности, включая разработку новых математических методов, опирающихся не только на аппарат классической теории вероятностей, но и на дискретный анализ.

1.6. Особенности «сложных» систем

Поскольку для сложных систем не существует общепринятого понятия «отказ», изменения в их структуре из-за отказов отдельных элементов при-

водят, как правило, лишь к некоторому ухудшению качества функционирования, а не к полному нарушению работоспособности. Это связано с наличием полного или частичного резервирования отказавших элементов, перекрытием зон функционирования отдельных подсистем, наличием обратных связей и средств коррекции некоторых структурных, параметрических и режимных параметров.

Объективная характеристика сложности зависит от качественных и количественных различий компонентов и связей системы (её разнообразия). В реальных задачах отличие сложных систем от простых определяется следующими основными характеристиками:

- множество неоднородных элементов (компонентов);
- активность (целенаправленность) компонентов;
- множество различных, параллельно проявляющихся взаимосвязей между компонентами;
- слабая формализуемость природы взаимосвязей;
- возможность кооперативного поведения компонентов;
- открытость;
- распределённость;
- динамичность, адаптируемость, потенциал эволюционного развития;
- неопределенность параметров среды.

Сложные системы реагируют на внешние воздействия, сообразуясь с внутренней целью, которую «надсистема» или наблюдатель (исследователь) не могут достоверно определить ни при каких обстоятельствах. Сложные системы в одном случае могут на два одинаковых воздействия сформировать разные реакции, а в другом – на два разных воздействия отреагировать одинаково. Например, при одной и той длительности внезапного нарушения электроснабжения какого-либо определенного технологического процесса время восстановления его параметров может резко различаться в зависимости от стадии технологического процесса. В то же время отключение подстанций промышленного предприятия с разной нагрузкой (мощностью трансформаторов) может привести к абсолютно одинаковым технико-экономическим последствиям (ущербу).

Известно, что ЭЭС функционирует в условиях воздействия большого количества случайных факторов, источниками которых являются: переменная (часто непрогнозируемая) нагрузка потребителей, внешняя среда, ошибки, шумы, помехи, критические и закритические отклонения параметров элементов системы и параметров её режима.

Таким образом, система сложная, если в реальной действительности существенно проявляются её следующие признаки [6, 7]:

- структурная сложность – определяемая по числу элементов системы, числу и разнообразию типов связей между ними, количеству иерархических уровней и общему числу подсистем;
- возможность разбиения системы на подсистемы, цели функционирования которых подчинены общей цели системы;
- сложность функционирования (поведения) – определяемая характеристиками множества состояний (режимов), правилами перехода из состояния в состояние, воздействием системы на среду и среды на систему, степенью неопределенности перечисленных характеристик и правил;
- сложность развития – определяемая характеристиками эволюционных или скачкообразных (аварийных, катастрофических) процессов;
- наличие разветвленной информационной сети;
- наличие часто иерархической структуры управления и интенсивных потоков информации;
- сложность выбора поведения в многоальтернативных ситуациях, когда этот выбор определяется целью системы, гибкостью реакций на заранее неизвестные воздействия среды;
- наличие взаимодействия с внешней средой и функционирования в условиях случайных факторов.

В этой связи возникает ещё один аспект, связанный с понятием сложности. Поскольку СЭС должна достигать заданной цели в условиях отказов её элементов по внутренним (сбои, ошибки, старение) или внешним (несанкционированные воздействия, помехи) причинам, средством обеспечения надёжности служит наличие не единственного, а нескольких режимов работы, в которых цель функционирования может быть достигнута, но с различным качеством. Поэтому говорить об описании сложной системы с помощью единственной математической модели неправомерно. В действительности существует ряд моделей, каждая из которых способна дать ответ только на вполне определённый круг конкретных вопросов о поведении СЭС в том или ином режиме. Для максимально полного представления о сложной системе необходимо создание множества моделей, являющихся проекциями, представляющими разные аспекты её функционирования. Очевидно, что одновременный анализ таких проекций (моделей) может сопровождаться появлением противоречий. При этом на основе теории сложности может быть предложен алгоритм нечёткой реализации возможных режимов с целью обеспечения непрерывности функционирования, то есть – живучести и других важных эксплуатационных характеристик.

При всё возрастающем усложнении условий работы современных СЭС, увеличения их стоимости сооружения и эксплуатации, а также воз-

можных последствий всякого рода нарушений нормального режима работы требование живучести становится одним из определяющих.

Система *S* обладает живучестью, если она содержит хотя бы одну собственную подсистему, имеющую общесистемную цель и способна выполнить её при невыполнении (отключении, отказе, сбое, несанкционированном внешнем воздействии и т. п.) ЭЭС (СЭС) общесистемной цели. Отсюда следует, что система обладает живучестью, если она имеет достаточный резерв и несколько путей достижения цели функционирования.

В СЭС с наиболее распространённым иерархическим построением схемы живучесть определяется как наличие подсистем *i*-го иерархического уровня, имеющих цели подсистем *j*-го уровня ($j<i$) и способных выполнять их при невыполнении своих целей подсистемами *i*-го уровня.

Отказ отдельных элементов и даже подсистем сложной системы, как правило, не приводит к потере работоспособности, а только снижает характеристики её эффективности. Это свойство обусловлено функциональной, временной и информационной избыточностью.

Необходимым условием обеспечения заданного уровня эффективности СЭС является высокая надёжность её элементов (агрегатов, установок). Так как понятие «надёжность» для большой (сложной) системы не определено, то необходимо исследование влияния надёжности отдельных элементов на эффективность её функционирования [48]. Если в качестве признака неисправного состояния СЭС принимается установленный заранее процент потери эффективности, то под надёжностью СЭС понимается её свойство сохранять эффективность в течение заданного времени на уровне не ниже критического, определяемого условиями совместной работы с питающимися от неё потребителями и ЭЭС.

Под обобщённой эффективностью понимается показатель, содержащий ряд независимых (или неявно зависимых) факторов, определяющих выполнение системой заданной цели [73]. Эффективность $Э$ системы *S* является мерой её целесообразности, выгодности, работоспособности. Поэтому понятие эффективности связано с получением некоторого полезного результата – выигрыша *G* [30], который обеспечивается энергетическими, экономическими, информационными и другими платами *C* (затратами)

$$Э = G - C,$$

если *G* и *C* выражены в одинаковых единицах измерения и в виде отношения

$$Э = \frac{G}{C}$$

или в виде показательной функции, если в разных.

Эффективность может определяться в виде показательной функции

$$Э = \alpha e^{-\beta C},$$

где α и β – масштабные коэффициенты, или как выигрыш G при предельно ограниченной плате C^*

$$Э = G|_{C \le C^*}.$$

Ряд задач СЭС, решение которых осуществляется на основе выбора функций (функционалов) эффективности, включает:

1. Обеспечение условий, необходимых при создании СЭС

$$Э \ge Э_* \text{ при } C \le C_*,$$

где $Э_*$ – пороговое значение эффективности; C_* – допустимые затраты на создание СЭС.

2. Сравнение вариантов СЭС для выбора наилучшего

$$Э_1 > Э_2 \text{ или } Э_1 < Э_2 \text{ при } C \approx C_*.$$

3. Оптимизация выбранного i-го варианта по техническим параметрам x, применительно к наиболее тяжёлым режимам y работы СЭС

$$\max_x \min_y Э_i .$$

Показатель эффективности – мера, количественно оценивающая качество выполняемых системой РГ функций, то есть, мера полезности функционирования системы РГ в определённой ситуации при обеспечении электроснабжения потребителей в конкретных режимах работы ГУ.

Система электроснабжения является сложной динамической системой, развивающейся во времени и в пространстве и обладающая свойствами, отсутствующими у элементов и связей, их образующих. Поведение динамической системы непрерывно меняется. При этом переход в новое состояние совершается не мгновенно, а с некоторой, зависящей от конкретных условий, постоянной инерции. Однако многие СЭС (в частности системы распределённой генерации (РГ)) могут работать в состоянии постоянной адаптации к изменяющимся условиям. Для объективного описания состояний, режимов, законов функционирования, оценки управляющих параметров СЭС часто не хватает ресурсов (главным образом, информационных). Это приводит к неопределённости зависимости причины и следствия возникающих в СЭС изменений структуры и параметров.

Сложные системы не описываются средними, случайными величинами показателей надежности, живучести, безопасности, помехозащищенности, качества управления, вероятность отказа, эффективности, устойчивости функционирования и др. Реальная сложность проблемы не позволяет замкнуться и в вероятностных схемах. Даже там, где имеются системы с высокой степенью организации, весьма малые структурные изменения могут

вызвать значительные перемены, далеко не всегда, сопровождающиеся положительными последствиями.

Сложная система обеспечивает решение многоцелевой, многоаспектной задачи и отражает объект с разных сторон в нескольких структурных моделях (технологической, функциональной, коммуникационной, административной и т. д.). Каждая из моделей имеет свой язык, а для согласования их возникает необходимость разработки метаязыка.

Структура СЭС – совокупность внутренних, связей между элементами, определяющими её основные свойства. В упрощенной структурной классификации сложных систем различают:

- открытые системы, внутренние процессы в которых существенно зависят от условий среды и сами оказывают на её элементы значительное влияние;
- замкнутые (закрытые), внутренние процессы в которых слабо связаны с внешней средой, а функционирование определяется внутренней информацией;
- вероятностные (стохастические) системы, связи между элементами и событиями в которых носят вероятностный характер и существуют в виде вероятностных закономерностей;
- детерминированные, представляющие частный случай вероятностных систем, связи между элементами и событиями в которых носят однозначный, предопределенный характер;
- централизованные системы, некоторый элемент (подсистема) в которых играет доминирующую роль;
- децентрализованные – доминирующая подсистема в них отсутствует.

Существует ряд подходов к делению систем по сложности, и, к сожалению, нет единого определения этому понятию, поскольку нет и четких критериев, определяющих границы такого деления. В зависимости от числа элементов, входящих в систему, принято, что при числе элементов от 10 до 10^3 – системы малые; от 10^4 до 10^6 – сложные; от 10^7 до 10^{30} – ультрасложные и от 10^{30} и более – суперсистемы. Однако в этой классификации не учитывается возможная разнотипность элементов, количество и вид связей, другие, отмеченные выше свойства больших и сложных систем, что существенно при их исследовании и функционировании.

Таким образом, понятие сложности системы не является универсальным и может меняться динамически, от состояния к состоянию. При этом и слабые связи, и взаимоотношения подсистем могут повышать результирующую сложность системы. Из всего сказанного очевидно, что действительно сложной системой следует считать систему, цели и поведение которой могут быть противоречивы и с трудом поддаются формализации. Объекты

энергетики при этом являются наиболее сложными, из числа искусственно созданных человеком к настоящему времени. Это:

- предприятия по добыче, транспорту и переработке первичных ТЭР;
- материальные (здания и сооружения);
- генерирующие, преобразующие и потребляющие электрическую и тепловую энергию агрегаты;
- распределительные сети;
- системы контроля и управления;
- системы и устройства РЗА;
- информационные системы (сбор и обработка информации, принятие решений по параметрам режима и структуры системы, передача управляющих воздействий, прогнозирование, обеспечение защиты от кибератак).

1.7. Дальнейшие перспективы

Рост сложности структур СЭС и задач управления ими обуславливает применение принципиально новых методов и средств управления. Развитие СЭС на основе технологий интеллектуальных ЭЭС радикально изменяет структуру и свойства будущих сложных систем электроэнергетики, порождая новые проблемы их функционирования.

Речь идёт о киберфизических системах (cyber-physical systems (CPS)) – сложных распределённых системах, состоящих из различных природных объектов, искусственных подсистем (СЭС, ЭЭС), управляемых и (или) контролируемых компьютерными алгоритмами и интегрированных в Интернет, что позволяет представить такие образования как единое целое.

Предпосылками появления CPS являются:

- рост сложности структур СЭС и задач управления ими;
- развитие систем РГ, ВИЭ, НЭ;
- необходимость применения принципиально новых методов, средств и систем управления;
- рост числа устройств со встроенными процессорами и средствами хранения данных;
- интеграция, позволяющая достигнуть наибольшего эффекта путем объединения отдельных компонентов в сложные (большие) системы;
- ограничение когнитивных способностей человека, эволюционирующих медленнее, чем системы контроля, управления и защиты.

Обычно выделяются следующие элементы типовой CPS:

- управляющие программно-аппаратные компоненты (микроконтроллеры с заданными цифровыми и аналоговыми интерфейсами);

- датчики, отвечающие за измерения, связанные с конкретными физическими процессами, позволяющие получить числовую (бинарную) характеристику физических факторов, необходимых для осуществления мониторинга процессов электроснабжения;
- устройства, регулирующие потребление активной и реактивной мощности, уровни напряжения и др.;
- проводные и беспроводные каналы связи для передачи технологической, служебной и бизнес-информации;
- системы автоматизированного наблюдения и контроля за нормальными режимами и процессами в СЭС;
- компоненты мониторинга системы, включающие анализатор инцидентов, сбоев, отказов и аварий в СЭС;
- компоненты сбора и хранения данных;
- системы видеонаблюдения, контроля и управления доступом, пожарной и охранной сигнализации и др.;
- интерфейс взаимодействия с человеком.

В CPS используются принципиально новые методы и алгоритмы адаптации, самообучения, распознавания, прогнозирования и мониторинга, учитывающие изменения внутренних и внешних физических процессов протекающих в элементах СЭС. При этом цикл «управление – получение данных – обработка данных – управление» при налаженной работе CPS каждый раз должен давать позитивные результаты и создавать новую ценность.

Таким образом, CPS представляют собой распределенные системы с «умными узлами» с возможностью реконфигурации потоков электроэнергии и информации в зависимости от условий.

Поскольку в CPS физические и программные компоненты тесно взаимосвязаны, и каждая компонента работает в разных пространственных и временных масштабах, появляется множество различных поведенческих ситуаций и взаимодействущих друг с другом множества способов их реализации, которые меняются в зависимости от контекста реального состояния (режима) СЭС.

При этом необходимо уточнить, что для практической реализации CPS требуется проведение серьёзных научных исследований с целью поиска новых методов и алгоритмов построения имитационных моделей, распознавания сигналов, прогнозирования аномальных и критических ситуаций, что может существенно затруднить их массовую реализацию.

2 СТРУКТУРНЫЕ МОДЕЛИ НАДЁЖНОСТИ СИСТЕМ ЭЛЕКТРОСНАБЖЕНИЯ

2.1. Вводные замечания

В современной электроэнергетике различают внешнюю и внутреннюю сложность. Внутренняя сложность определяется сложностью множества внутренних состояний, режимов, структур, и управления ими. Внешняя – сложностью взаимоотношений с окружающей средой, сложностью управления системой потенциально оцениваемых по обратным связям системы и среды.

Так, электрическая система представляется двумя составляющими: энергетической и информационной. Энергетическая определяет внутреннюю сложность, представляемую взаимосвязанной системой генерации, преобразования, передачи, распределении, потребления. Информационная определяется состоянием рынка, диспетчером (оператором) ЭЭС, сервис-провайдером (поставщиком услуг). Обобщённая структура такой системы приведена на рис. 2.1.

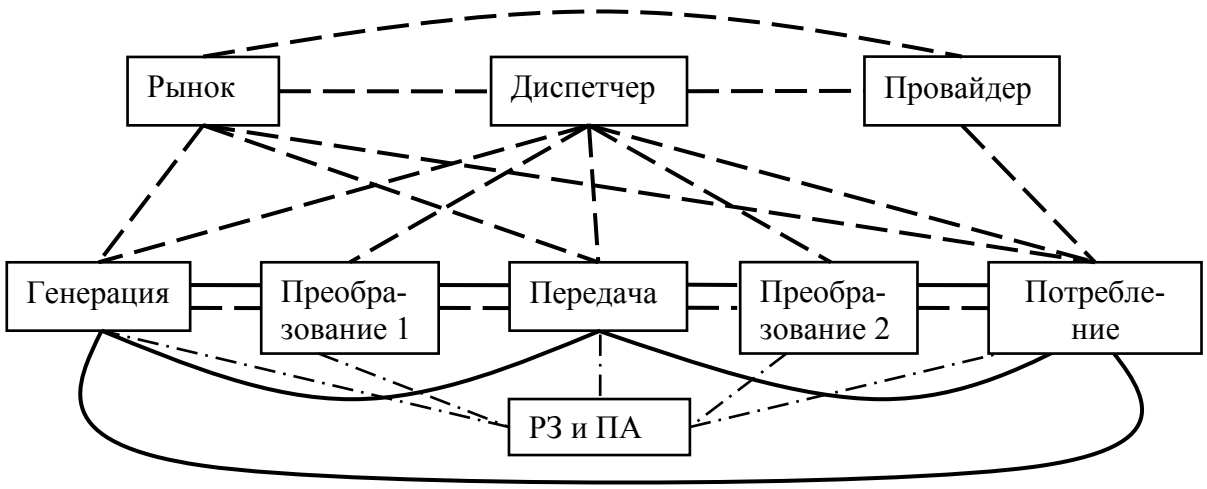


Рис. 2.1. Обобщённая структура ЭЭС. *Условные обозначения*:
сплошная линия – энергетические связи; пунктир – информационные;
штрих-пунктир – связи системы релейной защиты
и противоаварийной автоматики (РЗ и ПА)

Важным фактором здесь являются связи энергетики с экономикой промышленности, транспорта, ЖКХ, сельского хозяйства, объектами культурного назначения. Следовательно, сложные системы характеризуются и

тем, что они одновременно интегрируют в себе природные и социальные составляющие, естественное и искусственное.

2.2. Структурные модели больших систем

На основании приведённых результатов расчёта можно утверждать, что изучение больших систем путем непосредственного анализа всех их состояний практически невозможно. Для этого рядом авторов [6, 7, 74–76, 40] предлагаются структурные модели надёжности отражающие связи между показателем надёжности и структурой с учётом конструктивно-технических, производственно-технологических и эксплуатационно-технических факторов.

В простейшем случае структурная модель надёжности СЭС представляется состоящей из n элементов и связей между ними с некоторым возможным уровнем работоспособности (выдача мощности, нагрузка, электропотребление) $N_{\text{в}}$, который представляется как [40]

$$N_{\text{в}} = \frac{1}{n}\sum_{i=1}^{n} N_{\text{в}i} \ , \tag{2.1}$$

где $N_{\text{в}i}$ – уровень работоспособности i-го элемента СЭС ($0 \le N_{\text{в}i} \le 1$); n – число элементов, функционирующих в определённом режиме работы СЭС.

На основании (2.1) вычисляется среднее (математическое ожидание) суммы случайных величин

$$M_{\nu\text{в}} = \frac{1}{n}\sum_{i=1}^{n} m_{\nu\text{в}i} \ , \tag{2.2}$$

где – $m_{\nu\text{в}i}$ – уровень работоспособности i-го элемента в ν-м режиме СЭС.

Допустим, что каждый элемент может находиться только в двух состояниях: работоспособном и неработоспособном. Тогда

$$m_{\nu\text{в}i} = P_{\nu\text{в}i} \ , \tag{2.3}$$

где $P_{\nu\text{в}i}$ – вероятность того, что i-й элемент СЭС при работе её в ν-м режиме находится в работоспособном состоянии ($\nu_{\text{в}i} = 1$).

Подставив (2.3) в (2.2) получим обобщённую структурную модель, представляющую показатель надёжности СЭС P, как среднее арифметическое из показателей уровня работоспособности (надёжности) её элементов

$$P = \frac{1}{n}\sum_{i=1}^{n} P_{\nu\text{в}i} \ . \tag{2.4}$$

Естественно, что использование (2.4) приводит к значительному упрощению расчётов. Однако для применение этой модели в реальных СЭС необходимо обоснование справедливости тех допущений, которые были приняты при её построении.

Дальнейшее развитие общей и специальной теории систем и системного анализа показало, что понятие большой системы не удовлетворяет целому ряду задач исследования, проектирования и эксплуатации конкретных объектов современной инфраструктуры общества (энергетика, транспорт, связь, технологии и т. п.). Поэтому было введено понятие сложной системы, хотя часто термины «большая система» и «сложная система» используются как синонимы. В то же время существует точка зрения, что большие и сложные системы – это разные классы систем.

Понятие «большая» связывается с величиной системы, количеством элементов (часто относительно однородных), а понятие «сложная» – со сложностью взаимосвязей, отношений, алгоритмов функционирования и развития, сложностью поведения. Но сложная система – это не только система с разветвленной структурой и значительным количеством взаимосвязанных и взаимодействующих элементов (подсистем). Поэтому большие системы – подкласс сложных систем, и в общем случае система может быть и большой, и сложной.

2.3. Примеры простейших структур сложных СЭС

Как было показано в разделе 1 одной из особенностей ЭЭС (СЭС) является сложность структуры и взаимосвязей между элементами. Однако оценка показателей надёжности даже в простейших (последовательных и параллельных) структурных схемах СЭС требует тщательного анализа их возможного изменения, что и определяет сложность даже, казалось бы, «простых» систем.

Если при последовательном соединении n элементов ЭЭС (СЭС) (рис. 2.2) требуется определить ВБР системы $P(A)$ при выполнении ей поставленной задачи (событие A), то при условии независимости отказов ВБР определяется как

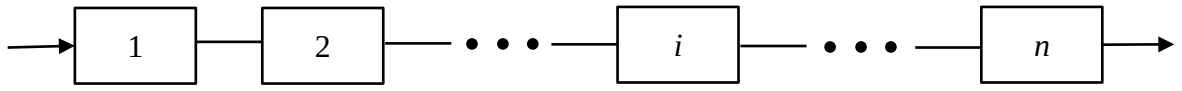


Рис. 2.2. Последовательная структурная схема СЭС

$$P_{\text{н}}(A) = \prod_{i=1}^{n} P(A_i), \qquad (2.5)$$

Пример 1. Допустим, что электроснабжение непрерывного производственного процесса, состоящего из четырёх последовательно соединённых агрегатов (установок) (рис. 2.3) осуществляется по четырём ЛЭП от четырёх ТП. На вход этой системы подаётся сырьё С, а на выходе получается товарная продукция Т.

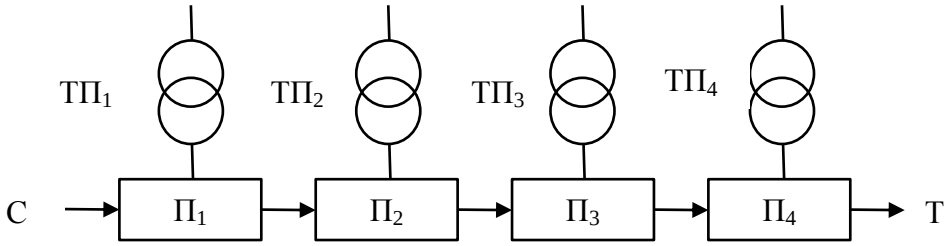


Рис. 2.3. Технологическая схема производства

Для того, чтобы работало всё производство, должны работать все ТП и все агрегаты. Условные показатели ВБР элементов $\{П_i,ТП_i\}$ этой системы:

$$p_1 = 0{,}9966;\ \ p_2 = 0{,}9885;\ \ p_3 = 0{,}9991;\ \ \ p_4 = 0{,}9750.$$

ВБР системы определится как

$$P_c = \prod_{i=1}^{4} p_i = 0{,}9966 \cdot 0{,}9885 \cdot 0{,}9991 \cdot 0{,}9750 = 0{,}9596.$$

Предположим, что СЭС и технологический процесс элемента $\{П_4,ТП_4\}$ можно модернизировать, доведя его ВБР до уровня ВБР элемента $\{П_2,ТП_2\}$. В этом случае ВБР системы составит

$$P_{\text{см}} = \prod_{i=1}^{4} p_i = 0{,}9966 \cdot 0{,}9885 \cdot 0{,}9991 \cdot 0{,}9885 = 0{,}9729.$$

Достигнутое увеличение ВБР системы составит

$$\Delta P_c = P_{\text{см}} - P_c = 0{,}9729 - 0{,}9596 = 0{,}0133.$$

При непрерывном технологическом процессе производства это будет соответствовать увеличению числа рабочих часов в году на величину

$$\Delta T_{\text{г}} = \Delta P_c \cdot T_{\text{г}} = 0{,}0133 \cdot 8760 \approx 117 \text{ ч/год}.$$

В действительности отказы последовательно соединённых элементов не являются независимыми, так как отказ одного из них уже исключает возможность отказа любого другого элемента этой схемы. Кроме того,

находясь в определённой функциональной связи, элементы этой схемы подвергаются воздействию общих возмущающих факторов (колебания напряжения, температуры, влажности), что также приводит к зависимости отказов. В этом случае, по теореме умножения вероятностей для зависимых событий имеем:

$$\begin{gathered} P(A) = P(A_1 A_2 \dots A_n) = \\ = P(A_1) \cdot P(A_2|A_1) \cdot P(A_3|A_1 A_2) \cdot \dots \cdot P(A_n|A_1 A_2 \dots A_{n-1}) = \\ = P(A_1) \prod_{i=2}^{n} P(A_i|A_1 \dots A_{i-1}), \end{gathered} \tag{2.6}$$

где $P(A_1)$ – ВБР первого элемента при работе СЭС в конкретном (заданном) режиме (выполнении поставленной задачи); $P(A_i|A_1 \dots A_{i-1})$ – условная вероятность безотказного функционирования i-го элемента при выполнении СЭС поставленной задачи.

Пример 2. Когда между отдельными участками производственного процесса имеются промежуточные накопители *V* продукции (рис. 2.4) задача существенно усложняется.

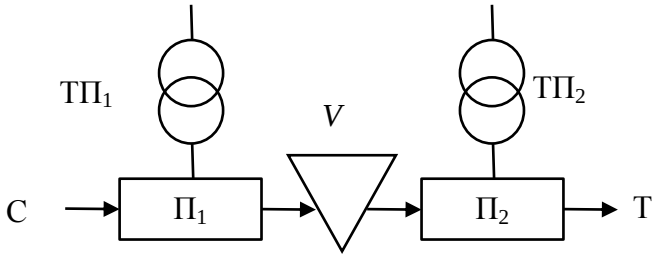


Рис. 2.4. Технологическая схема производства
с промежуточным накопителем

Характеристики системы с промежуточным накопителем зависят от объёма этого накопителя; производительности элементов {П$_1$, ТП$_1$} и {П$_2$, ТП$_2$} и пределов её изменения; режима эксплуатации; уровня заполнения накопителя на момент изменения режима работы системы (останова {П$_1$}, при отказе его СЭС {ТП$_1$} или {П$_2$} при отказе его СЭС, {ТП$_2$}).

Допустим, что ВБР элемента {П$_1$,ТП$_1$} равна $p_1 = 0{,}9$, а элемента {П$_2$, ТП$_2$} – $p_2 = 0{,}8$. При отсутствии промежуточного накопителя надёжность анализируемой системы $P_{с\text{без/н}}$ определится по (2.5):

$$P_{с\text{без/н}} = p_1 p_2 = 0{,}9 \cdot 0{,}8 = 0{,}72.$$

Далее рассмотрим несколько возможных режимов функционирования анализируемой системы при отказах её элементов {П$_1$, ТП$_1$} или {П$_2$, ТП$_2$} в зависимости от объёма промежуточного накопителя.

1) Если объём промежуточного накопителя относительно «мал» $V_{\min\to 0}$ и отказывает элемент {П$_1$, ТП$_1$}, это не окажет существенного влияния на ВБР системы, которая будет близка к $P_{c\text{без}/\text{н}} = 0{,}72$.

2) При достаточно «большой» ёмкости накопителя $V_{\min\to\infty}$ его можно рассматривать как элемент, разделяющий анализируемую систему на две подсистемы. При этом:

а) отказ элемента {П$_1$, ТП$_1$} практически не отразится на работе {П$_2$, ТП$_2$} и можно считать, что $P_{c\infty/\text{н}} = p_2 = 0{,}8$. Фактически ВБР такой системы оценивается в интервале $P_{c\text{без}/\text{н}} \le P_{c\infty/\text{н}} = 0{,}72 \le 0{,}8$;

б) отказ элемента {П$_2$, ТП$_2$} сопровождается остановом участка производства П$_2$ и ущербом от недовыпуска товарной продукции Т за время его простоя. Элемент {П$_1$, ТП$_1$} продолжает при этом работу в нормальном режиме с ВБР равной исходному значению $p_1 = 0{,}9$.

В реальных условиях заполнение объёма промежуточного накопителя полуфабрикатом – случайная величина, закон распределения которой зависит от условий анализируемого технологического процесса производства и режимов его работы. Однако в общем случае (для упрощения расчётов) можно предположить равномерный закон распределения с соответствующими числовыми характеристиками математическим ожиданием и дисперсией.

3) Пусть V_{var} – заполнение объёма промежуточного накопителя на момент отказа элемента {П$_1$, ТП$_1$}, выраженное в часах работы элемента {П$_2$, ТП$_2$} с номинальной производительностью. Если считать, что отказы элемента {П$_1$, ТП$_1$} происходят в соответствии с экспоненциальным законом распределения и достаточно редко (с относительно большими интервалами времени), то влияние на {П$_2$, ТП$_2$} оказывается только тогда, когда длительность простоя $t_{\text{пр}\{\text{П1,ТП1}\}}$ превышает время полного срабатывания объёма накопителя V_{var}. Так, если $t_{\text{пр}\{\text{П1,ТП1}\}} = 5$ ч, и $V_{max} = t_{max} = 8$ ч, то при условии равномерного закона распределения уровня заполнения промежуточного накопителя, среднее время его использования при отказе {П$_1$, ТП$_1$} будет $\overline{t_V} = 4$ ч. То есть, вероятность останова элемента {П$_2$, ТП$_2$} по причине отсутствия продукта для переработки составит

$$p_V = \frac{\overline{t_V}}{t_{\text{пр}\{\text{П1,ТП1}\}}} = \frac{4}{5} = 0{,}8.$$

ВБР анализируемой системы определится как

$$P_{c|\overline{t_V}} = 1 - (1 - p_1)p_V p_2 = 1 - (0{,}1 \cdot 0{,}8 \cdot 0{,}8) = 0{,}936.$$

4) Влияние отказа {П$_2$, ТП$_2$} на работу всей системы происходит в случае, когда время заполнения объёма промежуточного накопителя от V_{var} до V_{max}, выраженное в часах работы элемента {П$_1$, ТП$_1$} с номинальной произ-

водительностью меньше длительности простоя {$П_2$, $ТП_2$}. Расчёты, аналогичные проведённым в п. 3, дают результат

$$P_{c|\overline{t_V}} = 1 - (1 - p_2)p_V p_1 = 1 - (0{,}2 \cdot 0{,}8 \cdot 0{,}9) = 0{,}856.$$

ВБР системы без промежуточного накопителя была $P_{c\text{без/н}} = 0{,}72$. Его учёт при заданных условиях повышает ВБР системы при отказе {$П_1$, $ТП_1$} на

$$\Delta P_{c|\overline{t_V}} - P_{c\text{без/н}} = 0{,}936 - 0{,}72 \approx 0{,}22,$$

что соответствует увеличению (при непрерывном производстве) числа рабочих часов в году на величину

$$\Delta T_\text{г} = \Delta P_{c|\overline{t_V}} \cdot T_\text{г} = 0{,}22 \cdot 8760 \approx 1890 \text{ ч/год}.$$

При отказе элемента {$П_2$, $ТП_2$} ВБР системы с учётом промежуточного накопителя увеличивается на

$$\Delta P_{c|\overline{t_V}} - P_{c\text{без/н}} = 0{,}856 - 0{,}72 = 0{,}136,$$

что соответствует увеличению числа рабочих часов в году на величину

$$\Delta T_\text{г} = \Delta P_{c|\overline{t_V}} \cdot T_\text{г} = 0{,}136 \cdot 8760 \approx 1190 \text{ ч/год}.$$

Пример 3. Промышленное предприятие имеет технологическую схему производства продукции и условную схему электроснабжения, приведенные на рис. 2.5. Между участками имеются промежуточные накопители полуфабрикатов продукции (бункеры) *V*, объем которых позволяет при нарушении электроснабжения отдельных участков, последующим нормально работать до полного использования полуфабриката, находящегося в бункере, а предыдущим – до полного заполнения бункера. Каждый участок производства $П_i$ получает питание от своей подстанции – $ТП_i$.

Требуется найти вероятность того, что при нарушении электроснабжения *i*-го участка производства остановится *m* последующих участков и *l* предыдущих.

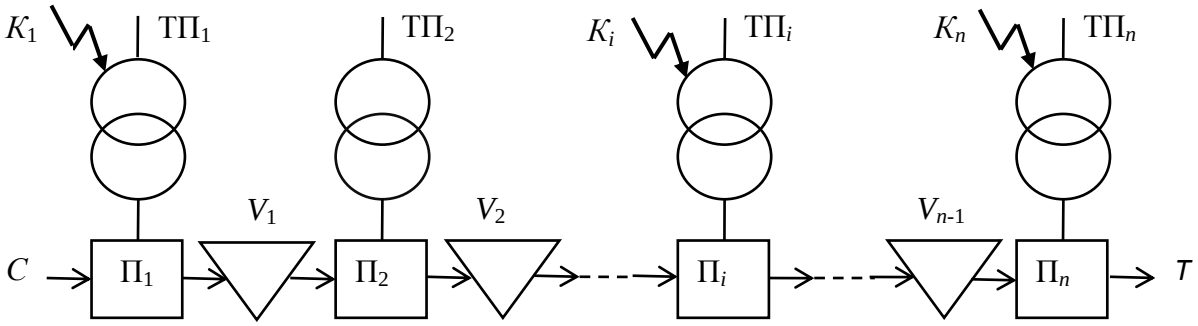


Рис. 2.5. Технологическая схема предприятия

При нарушении электроснабжения участка {$П_1$, $ТП_1$} ($К_1$) последующие продолжают нормально работать до полного использования резерва,

находящегося в бункере V_1. Вероятность того, что встанет участок {$П_2$, $ТП_2$}, равна вероятности того, что объема полуфабриката в бункере V_1 будет недостаточно, чтобы продолжалась его нормальная работа в течение времени, равного длительности простоя участка {$П_1$, $ТП_1$} (сумма длительностей нарушения электроснабжения, возможных ремонтных работ, восстановления параметров технологического процесса и наращивания производительности) $P(П_2, ТП_2) = P(V_1)$.

Вероятность останова участка {$П_3$, $ТП_3$} при нарушении электроснабжения {$П_1$,$ТП_1$} равна вероятности того, что объема V_2 будет недостаточно, при условии, что объем V_1 израсходован полностью: $P(П_3, ТП_3) = P(V_1)P(V_2|V_1)$.

Вероятность останова n-го участка {$П_n$, $ТП_n$} при нарушении электроснабжения на участке {$П_1$,$ТП_1$} по формуле умножения вероятностей (2.6) равна вероятности того, что объема бункера V_{n-1} будет недостаточно, при условии, что объемы бункеров V_1, V_2,…, V_{n-2} израсходованы полностью:

$$P(П_n) = P(V_1)P(V_2 \mid V_1) \cdot \ldots \cdot P(V_{n-1} \mid V_1 V_2 \ldots V_{n-2}).$$

При нарушении электроснабжения участка {$П_n$, $ТП_n$} (K_n) предыдущие продолжают нормально работать до полного заполнения пустой части бункера.

Вероятность того, что прекратит работу участок {$П_1$, $ТП_1$}, равна вероятности того, что бункер V_1 заполнен полностью, при условии, что V_{n-1}, V_{n-2}, … V_2 тоже уже полностью заполнены:

$$P(П_n) = P(V_{n-1})P(V_{n-2} \mid V_{n-1}) \cdot \ldots \cdot P(V_1 \mid V_{n-1} V_{n-2} \ldots V_2).$$

Тогда вероятности того, что при нарушении электроснабжения (K_i) i-го участка производства {$П_n$, $ТП_n$} остановятся k последующих P_k и l предыдущих P_l участков определятся как:

$$P_k = P(V_i)P(V_{i+1} \mid V_i) \cdot P(V_{i+2} \mid V_i V_{i+1}) \cdot \ldots \cdot P(V_{k-1}) \mid V_i V_{i+1} \ldots V_{k-2});$$

$$P_l = P(V_{i-1})P(V_{i-2} \mid V_{i-1}) \cdot P(V_{i+2} \mid V_i V_{i+1}) \cdot \ldots \cdot P(V_{k-1}) \mid V_i V_{i+1} \ldots V_{k-2}).$$

Полное и подробное решение этой задачи с учётом методики учёта промежуточных накопителей рассмотренной в примере 2, и разветвлённой схемы технологического процесса приведено в [50, 54].

Если все элементы последовательной цепи подвергаются воздействию только общих возмущающих факторов (перегрузка), то вероятность отказа СЭС – $P_з(A)$ зависит от ВБР наименее надёжного (слабого звена) $P(A_{i\,min})$ в конкретном режиме работы СЭС:

$$P_з(A) = P(A_{i\,min}). \qquad (2.7)$$

Очевидно, что реальная надёжность всегда ниже этой величины. Если считать наиболее ненадёжным элемент, который отказывает первым, то система, которая отказывает в тот же момент, так же ненадёжна, как и её самый ненадёжный элемент. Однако не обязательно, что первый отказавший элемент наименее надёжен. Он может иметь, например, меньший средний срок службы. Предполагая, что заранее неизвестно, какой из элементов откажет первым, необходимо считаться с вероятностью отказа любого элемента, а не только наименее надёжного. Поэтому интервал возможных значений ВБР исследуемой СЭС определяется неравенством

$$P_{\text{н}}(A) \leq P(A) \leq P_{\text{з}}(A). \qquad (2.8)$$

Для получения более точной информации о $P(A)$ необходимо знать закон её изменения в интервале (2.8) в виде функции от степени зависимости отказов элементов, которая характеризуется коэффициентом $0 \leq r \leq 1$. Поскольку в реальных условиях эксплуатации СЭС достоверную оценку r получить практически невозможно из-за малого объёма и неопределённости исходной статистической информации, предполагается линейная зависимость, как наиболее простая и не противоречащая здравому смыслу. Тогда по [40] получаем:

$$P(A) = P_{\text{н}}(A) + r[P_{\text{з}}(A) - P_{\text{н}}(A)]. \qquad (2.9)$$

Если все значения r на интервале $[0,1]$ равновероятны, то $r = 0{,}5$ и (2.9) принимает вид

$$P(A) = 0{,}5[P_{\text{н}}(A) + P_{\text{з}}(A)]. \qquad (2.10)$$

Анализ выражений (2.5 – 2.10) позволяет получить представление о том, какую роль играет информация о зависимости отказов последовательно соединённых элементов в СЭС.

При параллельном соединении элементов (рис. 2.6) СЭС выполняет поставленную задачу (или какую-то её часть), если безотказно функционирует хотя бы один из *n* элементов.

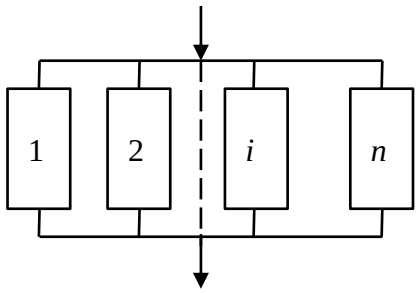


Рис. 2.6. Параллельная структурная схема СЭС

Если отказы элементов независимы, то ВБР системы

$$P(A) = 1 - \prod_{i=1}^{n}[1 - P(A_i)]. \qquad (2.11)$$

Надёжность схем, состоящих из последовательных и параллельных ветвей вычисляется обычно методом последовательного преобразования. Однако если элементы повторяются, необходимо принимать во внимание их взаимозависимость. В качестве примера рассмотрим схему рис. 2.7 [84].

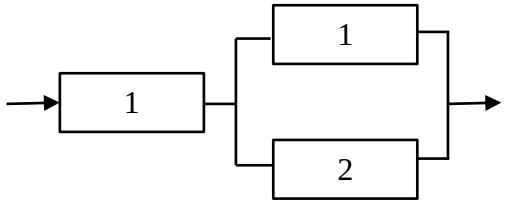


Рис. 2.7. Последовательно-параллельная схема

Предположим, что ВБР элементов этой схеме $P_1 = 0{,}9$; $P_2 = 0{,}8$.

В соответствии с классикой преобразования объединив параллельные ветви 1 и 2 в блок *A*, получим

$$P_A = 1 - [(1 - P_1) \cdot (1 - P_2)] = 1 - [(1 - 0{,}9) \cdot (1 - 0{,}8)] = 0{,}98\ .$$

Далее вычисляем ВБР системы – $P_{\text{С}}$

$$P_{\text{С}} = P_1 \cdot P_A = 0{,}9 \cdot 0{,}98 = 0{,}882.$$

Ошибка в этих вычислениях связана с тем, что элемент 1 и блок *A* не являются независимыми. В этом случае необходимо использовать уравнение (2.6), представив его в виде

$$P_A = P_1 \cdot P_A|P_1 = 0{,}9 \cdot 1 = 0{,}9\ ,$$

где $P_A|P_1 = 1$, так как элементы 1 и 2 соединены параллельно и блок *A* заведомо работает при условии, что элемент 1 находится в работоспособном состоянии.

Пример 4. В рассмотренном выше примере 1 начальная ВБР элемента {П$_4$, ТП$_4$} была $p_4 = 0{,}9750$. При наличии возможности, вместо его модернизации можно установить аналогичный резервный элемент П5 (рис. 2.8).

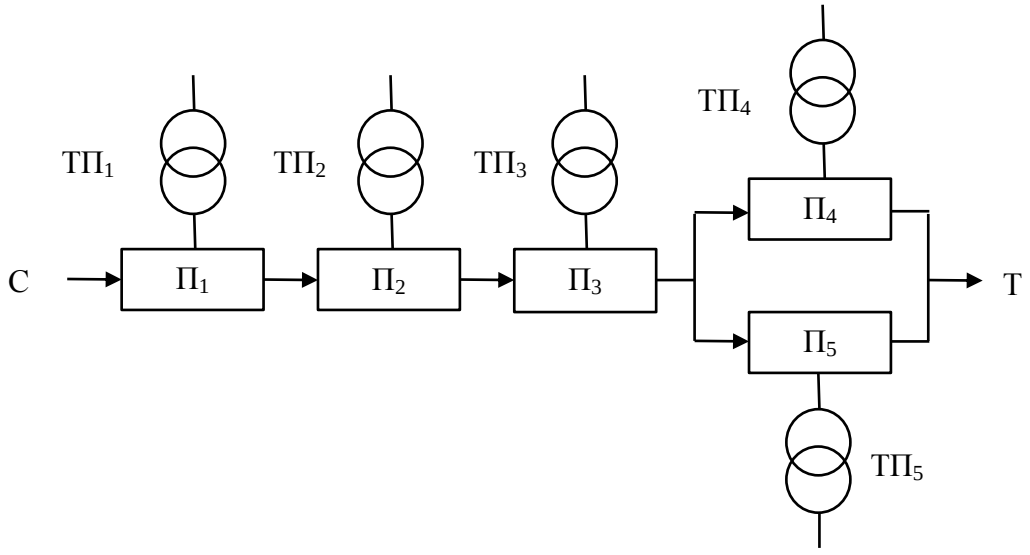


Рис. 2.8. Технологическая схема производства

ВБР параллельно подключённых элементов {П$_4$, ТП$_4$} и {П$_5$, ТП$_5$} определится по (2.11) и составит

$$P_{4,5} = 1 - \prod_{i=1}^{2}[1 - P(A_i)] = 1 - (1 - 0{,}9750)^2 = 0{,}9994. \qquad (2.12)$$

Тогда

$$\mathrm{P}_{\mathrm{с(м4,5)}} = \left(\prod_{\mathrm{i=1}}^{3} p_i\right) P_{4,5} = 0{,}9966 \cdot 0{,}9885 \cdot 0{,}9991 \cdot 0{,}9994 = 0{,}9837.$$

Увеличение ВБР системы при этом составит

$$\Delta P_{с(\mathrm{м4,5})} = P_{с\mathrm{м}} - P_с = 0{,}9837 - 0{,}9596 = 0{,}0241.$$

Число рабочих часов в году увеличится на

$$\Delta T_{\mathrm{г(м4,5)}} = \Delta P_{с(\mathrm{м4,5})} \cdot T_{\mathrm{г}} = 0{,}0241 \cdot 8760 = 211 \text{ ч/год}.$$

Полученный результат можно рассматривать как наилучший, который может быть достигнут в результате изменений в СЭС и структуре технологического процесса. При этом следует учесть, что в расчётах примеров 1 и 2 не учитывались затраты на модернизацию элемента {П$_4$, ТП$_4$} (пример 1) и введение резервного элемента {П$_5$, ТП$_5$} (пример 2). Не учитывалось и время, необходимое для модернизации элемента {П$_4$, ТП$_4$} (пример 1) и сооружения (монтажа, пуска) резервного элемента {П$_5$, ТП$_5$} (пример 2).

Пример 5. Резервируемые элементы не всегда рассчитаны на работу с полной производительностью (мощностью, нагрузкой). Примем, что в условиях примера 4 при отказе одного из элементов {П$_4$, ТП$_4$} или {П$_5$, ТП$_5$} производительность (мощность, нагрузка) всей системы снижается.

Полная производительность N (мощность, нагрузка) анализируемой системы принимается за 1,0. (N=1). Допустим, что (производительность, мощность, нагрузка) каждого элемента {П$_4$, ТП$_4$} и {П$_5$, ТП$_5$} составляет 0,7N номинальной производительности (что обычно соответствует расчётной нагрузке трансформаторов двухтрансформаторной подстанции) при ВБР $p_4 = p_5 = 0{,}9750$. При этом возможны следующие ситуации:

- оба элемента {П$_4$, ТП$_4$} и {П$_5$,ТП$_5$} отказали

$$Q_{4,5} = (1 - p_4)^2 = (1 - 0{,}9750)^2 = 0{,}0006;$$

- отказал элемент {П$_4$, ТП$_4$} при работающем {П$_5$, ТП$_5$}

$$Q_{4,\overline{5}} = (1 - p_4)p_5 = 0{,}025 \cdot 0{,}9750 = 0{,}024;$$

- отказал {П$_5$, ТП$_5$} при работающем {П$_4$, ТП$_4$}

$$Q_{5,\overline{4}} = (1 - p_5)p_4 = 0{,}9750 \cdot 0{,}025 = 0{,}024;$$

• если оба элемента {П$_4$, ТП$_4$} и {П$_5$, ТП$_5$} находятся в работоспособном состоянии, то

$$Q_{\overline{4},\overline{5}} = p_4 \cdot p_5 = 0{,}9750^2 = 0{,}951.$$

Ожидаемая средняя производительность параллельно работающих элементов {П$_4$, ТП$_4$} и {П$_5$,ТП$_5$}

$$\overline{N} = Q_{4,5} \cdot 0N + Q_{4,\overline{5}} \cdot 0{,}7N + Q_{5,\overline{4}} \cdot 0{,}7N + Q_{\overline{4},\overline{5}} \cdot 1N =$$

$$= 2 \cdot 0{,}024 \cdot 0{,}7 + 0{,}951 = 0{,}9846.$$

При сохранении надёжности элементов {П$_1$, ТП$_1$}, {П$_2$, ТП$_2$} и {П$_3$, ТП$_3$} последовательной цепи (рис. 2.8)

$$P_{1-3} = p_1 \cdot p_2 \cdot p_3 = 0{,}9966 \cdot 0{,}9885 \cdot 0{,}9991 = 0{,}9843,$$

общая производительность анализируемой системы определится как

$$N = P_{1-3} \cdot \overline{N} = 0{,}9843 \cdot 0{,}9846 = 0{,}97.$$

2.4. Модель участка производства для анализа последствий нарушений электроснабжения

Поскольку надежность электроснабжения потребителей должна стать товаром с соответствующей ценой и предметом договорных отношений, необходима объективная оценка технико-экономических последствий возможных нарушений электроснабжения для разработки требований и мер ответственности субъектов рынка на границах балансовой принадлежности. Решение задач учета экономических требований потребителей к надежности СЭС необходимо рассматривать как одну из важнейших проблем современной энергетики.

Несколько приведённых ниже примеров показывают, что при разработке и эксплуатация современных СЭС возникает необходимость анализа взаимосвязей схемы электроснабжения с технологической схемой производства с целью оценки технико-экономических последствий изменения режимов электроснабжения или отказов элементов СЭС. Отдельные объекты производственных систем представляются при этом в виде четырех основных сочетаний взаимодействия технологических агрегатов (механизмов), каждый из которых получает питание от «своей» ТП, кабельной или воздушной линии (рис. 2.9) [54].

На рис. 2.9 представлены:

• последовательная (многофазная) система, состоящая из *n* производственных механизмов (производство пластмасс, поточно-транспортные системы, автоматические станочные линии и др.) – *а*);

• параллельная (многоканальная), состоящая из m механизмов (термические цехи насосные, компрессорные, вентиляционные установки и др.) – *б*);

• последовательно-параллельная – n последовательных и m параллельных (целлюлозно-бумажное, металлургическое, химическое производства) – *в*);

• последовательно-параллельная с изменяющимся числом производственных механизмов в параллельных звеньях (предприятия нефтепереработки, химии, производство искусственных кормов) – *г*).

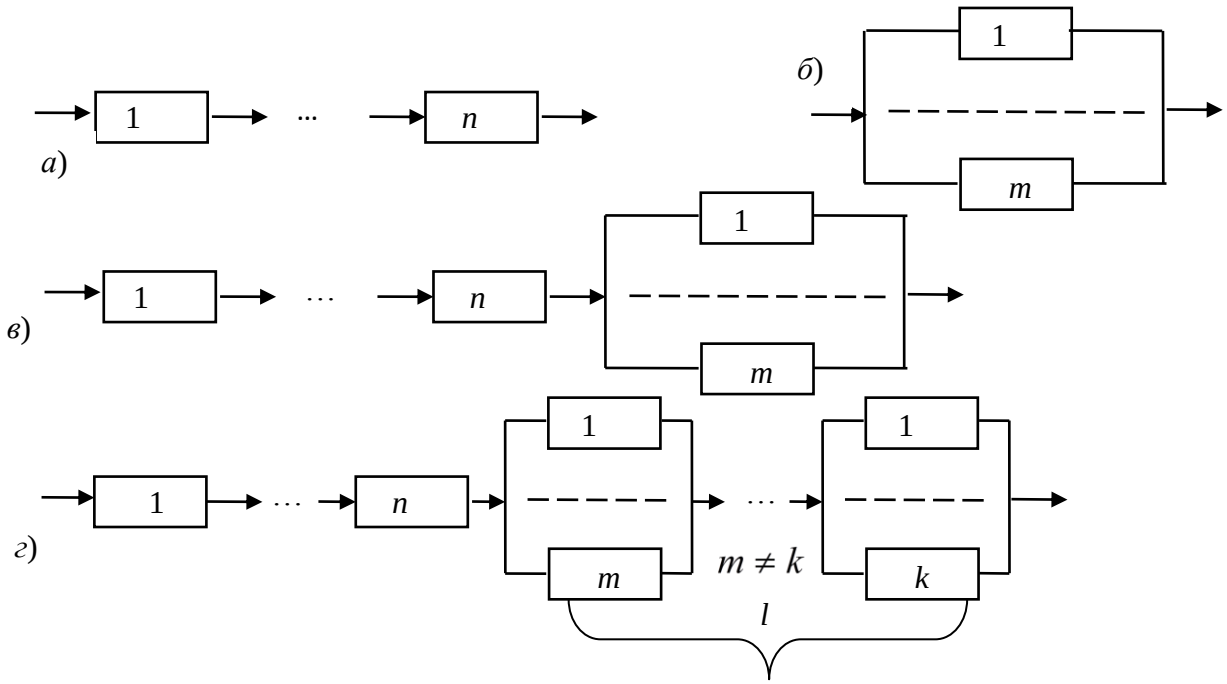


Рис. 2.9. Формализованное представление структурных функциональных схем производственных систем

Возможны модификации схем *в*) и *г*). Это параллельно-последовательные схемы; схемы, когда параллельное звено включено в рассечку последовательной цепи или последовательное звено включено в рассечку параллельных.

Построение структурной схемы связей производственных механизмов осуществляется в соответствии с надёжностной схемой оценки последствий нарушений их электроснабжения. При этом могут наблюдаться отклонения от реальной технологической схемы производственной системы. Так, в машиностроении на станочном участке производится обработка деталей на множестве станков разного функционального назначения. Однако структурная схема будет здесь параллельной, так как отключение любого станка (или их группы) сопровождается практически одинаковыми последствиями.

При последовательной структурной схеме (рис. 2.9, *а*)) нарушение электроснабжения даже одного производственного механизма приводит к безусловному останову всего выделенного участка. Фактически отключенная мощность N_0 равна в этом случае мощности N, потребляемой всем объектом. При этом возможны лишь два состояния: рабочее и нерабочее. Последствия отключения оцениваются линейной (кусочно-линейной) моделью и определяются ущербом

$$У = at + b, \qquad (2.13)$$

где a –ущерб от отключения выделенного подмножества производственных механизмов, руб./ч; b – ущерб, определяемый фактором внезапности, руб./откл.

Оценка ущерба, производимая по (2.13) в случае отключения лишь части производственных механизмов $N_0 < N$, может быть несколько завышенной из-за того, что фактор внезапности b учитывается здесь для всей выделенной совокупности. Для отдельных производств (химия, нефтепереработка) это завышение несущественно и может не учитываться. Для производств машиностроения, в зависимости от соотношения N_0 и N, возможно некоторое уточнение расчетного значения ущерба за счет коррекции величины b коэффициентом α, которое при $N_0 < N$ достигает 10–15 %. Тогда

$$У = at + \alpha b, \qquad \alpha = \frac{N_0}{N}. \qquad (2.13, а)$$

При параллельной структурной схеме (рис. 2.9, *б*)) нарушение электроснабжения одного из механизмов не приводит к нарушению всего производственного процесса. Поскольку фактор внезапности появляется только на отключенных производственных механизмах выделенной совокупности, ущерб определяется как

$$У = \alpha(at + b), \qquad (2.14)$$

Наличие параллельной схемы позволяет расширить возможности управления нагрузкой, построив схему электроснабжения так, чтобы имелась возможность индивидуального отключения производственных механизмов и их групп.

При последовательно-параллельной схеме (рис. 2.9, *в*)) имеются два потребляющих электроэнергию множества производственных механизмов: N_1 – в последовательной цепи и N_2 в параллельной $N_1 \cup N_2 = N$.

Обозначим: N_{01} и N_{02} – множества отключаемых механизмов, причём $N_{01} \subset N_1,\ N_{02} \subset N_2,\ N_{01} \cup N_{02} = N_0$. Если нарушение электроснабжения

рассматривается для элементов $N_{01} \subset N_1$, то расчет последствий выполняется также, как и при последовательной схеме по формулам (2.13), (2.13, *а*). По этим же формулам производится расчет, если совместно выполняются условия $N_{01} \subset N_1$ и $N_{02} \subset N_2$ или $N_0 \subset (N_1 \cap N_2)$, соответствующие одновременному отключению производственных механизмов в последовательной и параллельной ветвях структурной схемы. И только в случае $N_{02} \subset N_2$, что соответствует проведению отключений только в параллельной ветви схемы, расчет последствий выполняется по выражению

$$У = \alpha at + \beta b, \qquad \beta = \frac{N_{02}}{N_2}. \tag{2.15}$$

При $N_{02} \subset N_2$ следует учитывать возможное снижение производительности механизмов множества N_1, которое необходимо для обеспечения синхронной работы всего объекта производства. Но если анализируется последовательно-параллельная схема в производствах машиностроения, то снижения производительности, как правило, не происходит ввиду изыскания возможности временного складирования продукции и расчет последствий выполняется по (2.15).

При анализе параллельно-последовательных схем в условиях невозможности временного складирования (металлургия, химическая и целлюлозно-бумажная промышленность) снижение производительности механизмов из множества N_2 уже отражается на работе последовательной цепи (множество N_1), которое тем больше, чем больше N_{02}.

Вследствие особенностей непрерывных, технологических процессов в указанных и ряде других отраслей производительность отдельных механизмов может быть снижена лишь до 50 % от номинальной. Тогда при $N_{02} \geq 0{,}5N_2$ последствия определяются также по (2.15). В остальных случаях можно считать, что снижение производительности косвенно учитывается за счет коррекции величины *а*, характеризующей все выделенное подмножество механизмов коэффициентом α.

Оценка последствий нарушения электроснабжения производственных механизмов, работающих по схеме (рис. 2.9, *г*) носит более сложный характер, но в итоге сводится к уже рассмотренным случаям. Если $N_{01} \subset N_1$,то для расчетов используется (2.14) или (2.13), соответствующие полному погашению объекта. Когда происходит отключение производственных механизмов в последовательном и одном или нескольких параллельных звеньях одновременно: $N_0 \subset (N_1 \cap N_2 \cap ... \cap N_l)$, анализируемое производство тоже полностью останавливается и расчет также ведется по (2.13) или (2.14). Отключения, производимые в любом из па-

раллельных звеньев $N_0 \subset N_l$, сопровождаются ущербом, определяемым по (2.15), с учетом того, что величина β определяется в соответствии со структурной схемой как $\beta = \frac{N_0}{N_l}$.

Наиболее общим является случай, когда производственные механизмы одновременно отключаются в разных звеньях последовательно-параллельной схемы. Ущерб от их отключения при этом составит:

$$У = \alpha a + \gamma b; \quad \gamma = \frac{\sum_n N_{0n} + \sum_l N_{0l}}{N}.$$

Таким образом, оценка последствий нарушений электроснабжения выделенных по рассмотренному принципу производственных механизмов осуществляется введением весовых коэффициентов α, β, γ, зависящих от соотношения величин отключенной и потребляемой мощностей.

Производственная система, отдельные объекты которой представляются набором указанных типов структурных схем, позволяет повысить эффективность управления нагрузкой и при возникновении длительных ограничений. При этом появляется возможность проводить переключения с сохранением заданной величины снижения нагрузки, также обеспечивая минимум потерь.

Вариантное решение собственно задач надежности ЭЭС обычно заканчивается определением: состава узлов нагрузки, которые отключаются при нарушениях электроснабжения или на уровне которых должна быть уменьшена нагрузка; частоты нарушений электроснабжения; глубины снижения нагрузки и длительности восстановления электроснабжения.

Определить среднегодовой ущерб у потребителя по таким сведениям и справочной информации об ущербе можно после проведения некоторых дополнительных исследований. Если задача надежности рассматривается на уровне узлов нагрузки распределительной сети промышленного предприятия, к которым непосредственно подключены электроприёмники производства, то необходимо определить состав производственного оборудования, прекращающего работу при отключении этих электроприемников. При проектировании распределительной сети промышленного объекта необходимо учитывать, что значение среднегодового ущерба от нарушения электроснабжения в этой сети будет зависеть не только от достигнутого уровня надежности электроснабжения, но и от группировки электроприемников в узлы нагрузки. Распределить электроприёмники по узлам нагрузки из условия минимизации ущерба, возникающего при погашении этих узлов, можно только при использовании модели предприятия, составленной по правилам, обеспечивающим возможность системного анализа ущерба.

При нарушениях электроснабжения на более высоких иерархических уровнях ЭЭС между требуемым снижением нагрузки и составом отключаемого оборудования уже нет однозначного соответствия. Появляется возможность выбора отключаемого оборудования, обеспечивающего минимизацию возникающего в таких режимах ущерба. Решение этой задачи при проектировании объектов ЭЭС не обязательно совмещать с решением оптимизационных задач надежности. Её результат – построение функции $У_{\min} = \varphi(N, t_э)$ – минимального ущерба, обеспечиваемого за счет выбора состава отключаемых объектов производства, что позволит принимать решения о режимах электропотребления на высших иерархических уровнях с учетом объективной информации об ущербах потребителей.

2.5. Сложность системы энергетики с объектами распределённой генерации

Традиционной является задача оптимизации наилучшего «выхода» системы при условии управления несколькими сигналами «входа». Предположим, что система РГ состоит из двух ГУ с разными «входными» сигналами T_1 и T_2 (разные типы и установленная мощность ГУ). Электроснабжение условного потребителя П осуществляется по схеме рис. 2.10, *а*).

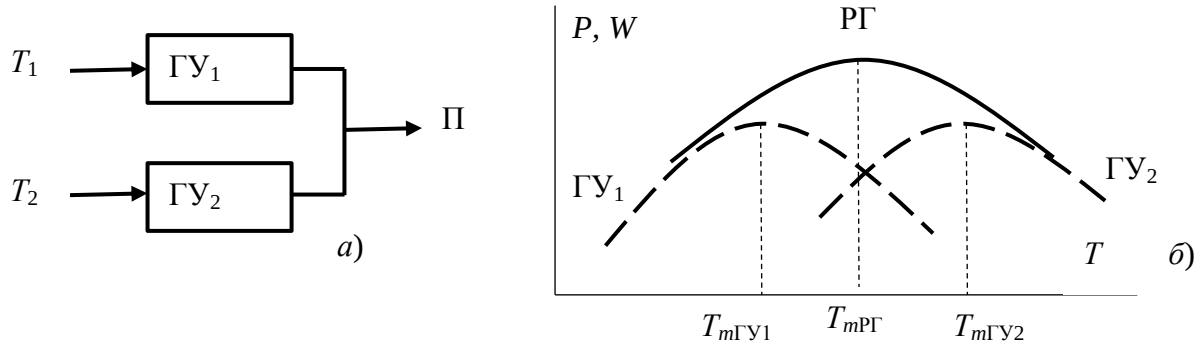


Рис. 2.10. Структурная схема – *а*);
характеристики ГУ и системы РГ – *б*)

Результирующий «выход» определяется суммированием «выходов» двух параллельно работающих ГУ: суммой генерируемых мощностей $P_1 + P_2 = P_\Sigma$ или суммой потребляемой П электроэнергии $W_1 + W_2 = W_\Sigma$. Несмотря на то, что «выходы» ГУ достигают максимума при соответственно разных величинах $T_{m\text{ГУ1}}$ и $T_{m\text{ГУ2}}$ «входных» сигналов, «выход» всей системы РГ максимален при «входе» $T_{m\text{РГ}}$, существенно отличающемся и от $T_{m\text{ГУ1}}$ и от $T_{m\text{ГУ2}}$ (рис. 2.10, *б*). Естественно, что одного знания оптимумов

составляющих подсистем РГ для определения оптимального режима всей системы недостаточно.

Для систем РГ задача экономичного распределения нагрузки и регулирования частоты соответствует её классической постановке: регулирование мощности отдельных ГУ в целях поддержания частоты не должно противоречить экономичному распределению нагрузки между ГУ. Естественно, что требования надёжности электроснабжения потребителей и устойчивости параллельной работы ГУ нарушаться не должны. Даже при незначительных отклонениях частоты в энергообъединении могут происходить существенные изменения обменной мощности между частями системы.

В качестве примера [4] рассмотрим систему РГ, относительная суммарная мощность которой $P_{\Sigma} = 1$, и $P_{\text{ГУ}_1} = P_{\text{ГУ}_2} = 0{,}5$. Пропускная способность ЛЭП не превышает 10 % мощности каждой ГУ: $P_W = 0{,}05$. На рис. 2.11, *а*) показано соотношение генерации, потребления и переток мощности в исходном режиме. Коэффициент статизма по частоте принят равным

$$s = \frac{\Delta f}{\Delta P_{\text{н}}} = 0{,}1.$$

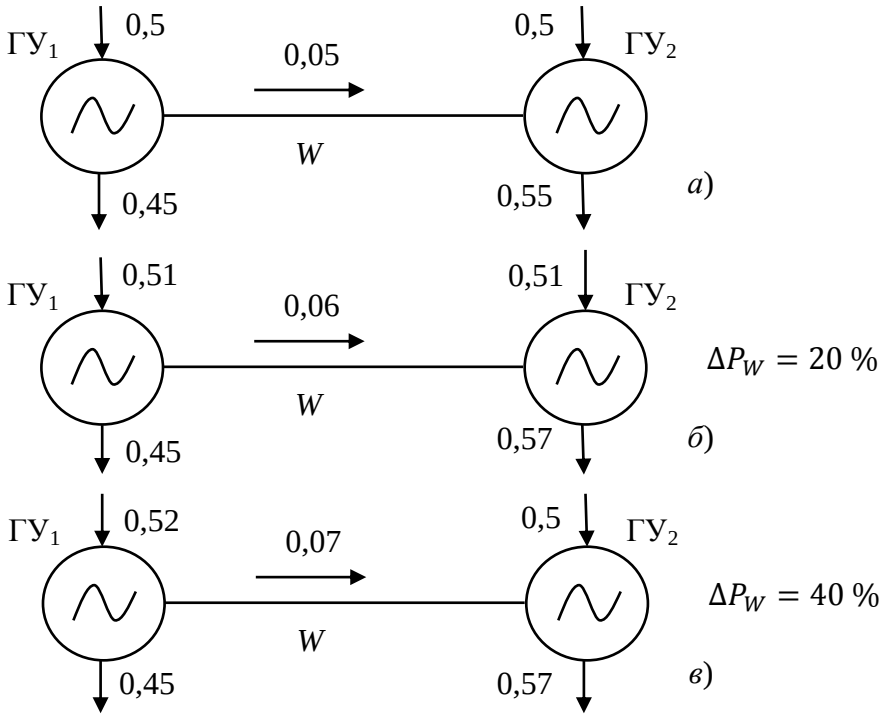


Рис. 2.11. Изменения обменной мощности в системе РГ между ГУ_1 и ГУ_2

Если нагрузка $ГУ_2$ увеличивается, вызывая суммарное снижение частоты на 0,1 Гц, что в относительных единицах составляет 0,002, то прирост нагрузки

$$\Delta P = \frac{\Delta f}{s} = \frac{0{,}002}{0{,}1} = 0{,}02.$$

Для сохранения баланса (без учёта регулирующего эффекта нагрузки) суммарная мощность системы должна возрасти на $\Delta P_{\Sigma} = 0{,}02$.

Если $ГУ_1$ и $ГУ_2$ равномерно воспримут наброс мощности, обменная мощность составит $P_W = 0{,}06$, увеличившись на 20 % по сравнению с исходным режимом (рис. 2.11, *б*)).

Если регулирование частоты осуществляется только $ГУ_1$, то обменная мощность в ЛЭП составит $P_W = 0{,}07$, то есть, возрастёт уже на 40 % по сравнению с исходным режимом (рис. 2.11, *в*)).

Если исходный режим соответствовал 20 % запасу статической устойчивости, то режим, соответствующий рис. 2.11, *б*) будет критическим, а режим рис. 2.11, *в*) – недопустимым.

Отметим, что ещё в [16] были рассмотрены основные понятия и теория метода относительных приростов для распределения нагрузки между станциями. Метод позволял оценить наибольшую экономичность работы системы в целом с учётом расхода топлива на кВт·ч выработанной электроэнергии, характеристик и параметров станционного оборудования. Поэтому для решения поставленной задачи оптимизации наилучшего «выхода» современных систем РГ можно (хотя бы частично) воспользоваться результатами системных исследований 1949 г.

Более строгий математический аппарат решения подобной задачи основан на использовании метода множителей Лагранжа и предложен в [49], для решения задач оптимального резервирования многоэлементных систем с учётом стоимости, а также в [41] при оптимизации режимов электропотребления по минимуму расхода энергоресурсов и ограничениях потребления мощности и энергии в СЭС промышленных предприятий.

По аналогии с [26] рассмотрим, пример системы, включающей два предприятия – П1 и П2, для нормальной работы которых требуется тепло и электроэнергия. Причём для П1 требуется в основном тепло, а для П2 – электроэнергия. Оба предприятия имеют фиксированную нагрузку и, соответственно, электро- и теплопотребление, равное производству тепла коммерческой котельной, принадлежащей предприятию П1; электроэнергии, вырабатываемой на местной, также коммерческой, электростанции, принадлежащей П2 и муниципальной ТЭЦ, производящей как тепловую, так и электрическую энергию.

Котельная и местная электростанция производят объёмы тепла и электроэнергии в соответствии с требованиями предприятий П1 и П2. ТЭЦ обеспечивает баланс потребностей П1 и П2 в тепле и электроэнергии. Допустим, что работа ТЭЦ определяется какой-то одной условной единицей.

Поскольку муниципальное правительство субсидирует предприятия П1 и П2, они полностью потребляют всё тепло и электроэнергию, производимые на ТЭЦ. Данная ситуация представлена на рис. 2.12 и описывается следующими уравнениями:

$$Q = D_q + G^q;\ W = D_w + G^w;\ P = D_q + D_w + G\ ,$$

где Q – количество потребляемого тепла, необходимого для технологического процесса предприятия П1; W – количество электроэнергии, потребляемой предприятием П2; D_q – спрос на тепло предприятием П1; D_w – спрос на электроэнергию предприятием П2; G – производительность ТЭЦ по теплу G^q и электроэнергии G^w: $G = G^q + G^w$; P – полные производственные мощности всех генерирующих источников.

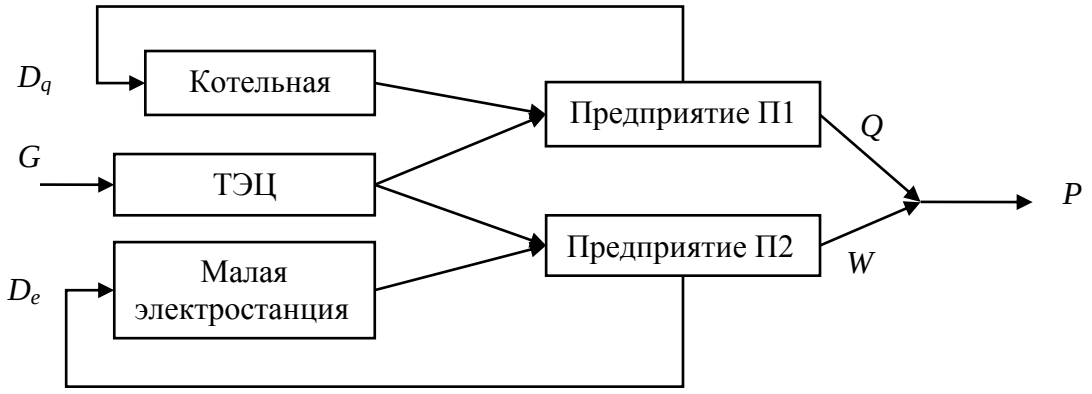


Рис. 2.12. Блок-схема системы

В общем случае существует возможность управления спросом на тепло D_q, на электроэнергию D_w и полными производственными мощностями всех генерирующих источников P. Управляющие органы – предприятия П1, П2 и муниципальное правительство. Правительство управляет переменной P, изменяя G, предприятие П1 управляет Q через D_q, предприятие П2 контролирует W, варьируя D_w.

При обеспечении полной потребности в тепловой и электрической энергии предприятий П1 и П2 правительство, не владея достаточно достоверной информацией о прогнозируемом спросе, всё же принимает решение увеличить G на одну условную единицу. Тем самым, в соответствии с принятыми условиями, в два раза увеличивается производительность по теплу и электроэнергии. Тогда предприятия П1 и П2, на которых

никаких изменений технологии не предусмотрено, вынуждены тоже на одну единицу (наполовину) уменьшить D_q и, соответственно D_w для сохранения баланса тепло- и электропотребления. Следовательно, изменение D_q и D_w приводит к уменьшению P на две единицы. Окончательно: увеличение на единицу G приводит к уменьшению полных генерирующих мощностей P на единицу.

Парадокс исчезает, если регулируется все три величины: D_m, D_e и G. Однако основная проблема возникает из-за других управляющих воздействий на взаимосвязь между управляемыми M, P, E и управляющими D_m, D_e, G переменными. В отличие от обычных представлений такое парадоксальное поведение вызвано не наличием нелинейности, стохастичности, неопределённости, а порождается исключительно структурой схемы, имеющимися связями и ограничениями, присущими элементам системы.

Данный пример иллюстрирует чрезвычайно важный момент, присущий понятию сложности системы – различие между сложностью неуправляемой и сложностью управляемой системы. Сложность неуправляемой системы определяется совокупностью статической и динамической сложности в отсутствии управления. Процесс управления здесь может привести к неустойчивым конфигурациям (режимам, структурам, параметрам и т. п.), появление которых возможно из-за разрыва между вычислительными потребностями системы в целом и вычислительными возможностями подсистем. Под сложностью управляемой системы понимается уровень сложности, сопряжённый с вычислениями, необходимыми для полного управления системой. Однако неустойчивые конфигурации могут появиться и здесь, если быстродействие некоторых подсистем не так велико, чтобы вовремя реагировать на изменения входных управляющих воздействий. Допущение возможности выбора внешних управляющих воздействий на модель системы означает переход исследователя с позиций пассивного наблюдения к активному вмешательству.

Сложность объектов электроэнергетики определяется ещё и тем, что в подавляющем большинстве случаев их можно отнести к классу критически важных (ТЭС и ГЭС (мощность свыше 600 МВт), крупные районные подстанции (класс напряжения 330 кВ и выше), центры управления работой ЕЭС), нарушение или прекращение функционирования которых может привести к потере управления экономикой административно-территориальной единицы страны, её субъекта или страны в целом, необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения. К объектам систем энергетики в полной степени можно отнести и понятие потенциально опасных, поскольку уни-

чтожение или прекращение действия их может представлять угрозу для национальной (информационной, экономической, военной, внешнеполитической, экологической) безопасности страны.

Очевидно, что даже в относительно «простых» системах могут возникнуть явления, если сложность взаимосвязей не изучена должным образом. Поэтому отнесение той или другой реальной системы к классу «сложных» или «простых» в значительной мере является условным и связано в основном с тем, насколько существенную роль играют комплексные, общесистемные вопросы.

3 ОСНОВЫ ФОРМАЛИЗОВАННОГО ОПИСАНИЯ СЛОЖНЫХ СИСТЕМ ЭЛЕКТРОСНАБЖЕНИЯ

3.1. Вводные замечания

Сложность любой ЭЭС и СЭС – относительное понятие, зависящее от

- иерархического уровня её исследования (анализа);
- характеристик (параметров режима), нелинейно зависящих от множества составляющих её элементов (подсистем), качественных различий между ними, количества, вида и формы связей;
- свойств, обусловленных внутренними закономерностями, определяющими ряд наиболее существенных её параметров, включая пространственную структуру и свойства протекающих в этой структуре процессов;
- динамического поведения.

Сложность системы определяет и нелинейность её переменных параметров (напряжение, ток, мощность, частота и т. д.), структуры схемы (последовательная, параллельная, радиальная, кольцевая и т. д.), связей (статические, динамические, информационные и т. д.). Нелинейность приводит к тому, что многие переменные зависят не только от времени, но и являются функциями других переменных, влияют друг на друга. В процессе познания любой системы, в том числе СЭС, необходима постановка вопросов, являющиеся критериальными парами, взаимосвязи которых представляет полный граф (рис. 3.1).

Взаимосвязи могут влиять на систему больше, чем отдельные её элементы и их группы. Ключевое свойство сложных систем в том, что их функционирование и развитие (поведение) сопровождаться появлением редких, неординарных событий, приводящих к неуправляемым цепным (каскадным) реакциями, достоверное прогнозирование которых практически невозможно. Одно из таких событий может осуществиться после тысяч ординарных, не приводящих к каким-либо серьёзным последствиям.

Система, состоящая из относительно небольшого количества элементов способна обладать достаточно большой динамической сложностью. Появление даже одного нового элемента может привести к созданию множества дополнительных связей. Причём добавление каждого последующего элемента увеличивает количество связей в большей степени, чем при добавлении предыдущего.

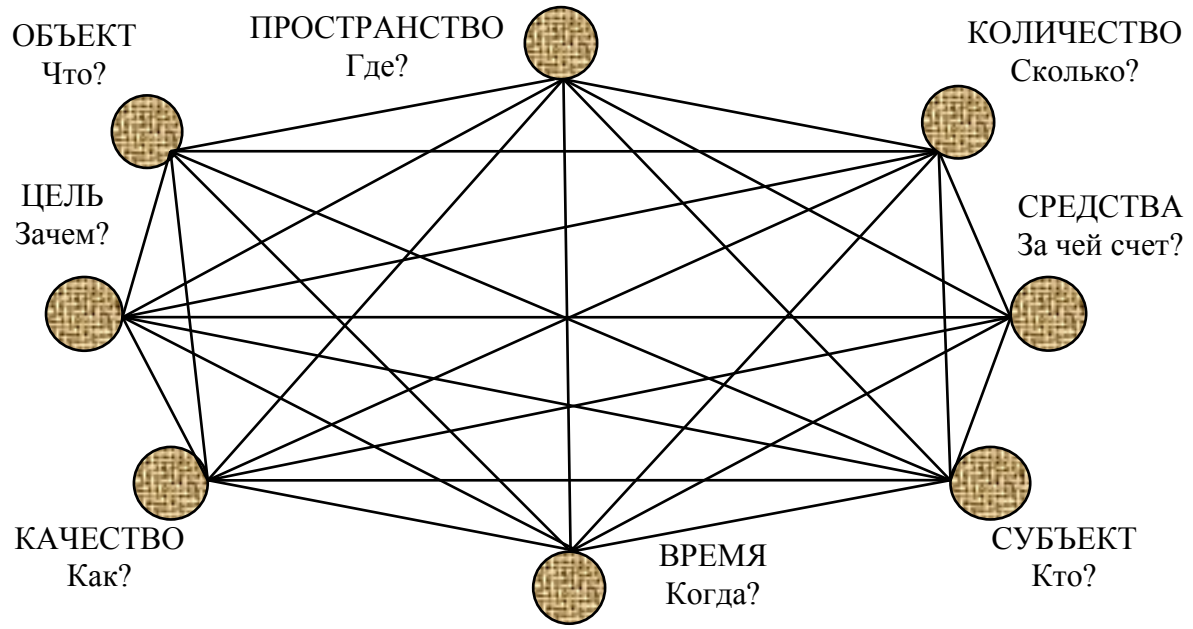


Рис. 3.1. Критериальные пары взаимосвязей вопросов исследования сложной системы

При двух элементах *A* и *B* возможны только две связи и два направления (рис. 3.2, *а*). Добавление элемента *C* увеличивает число возможных связей до 6 (рис. 3.2, *б*). Если элементы *A* и *B* вступают в коалицию (энергообъединение), и она начинает влиять на *C*, то число связей увеличивается до 8 (рис. 3.2, *в*). Если таких коалиций 3 (*AB*, *AC*, *BC*), то число связей достигнет 12 (рис. 3.2, *г*).

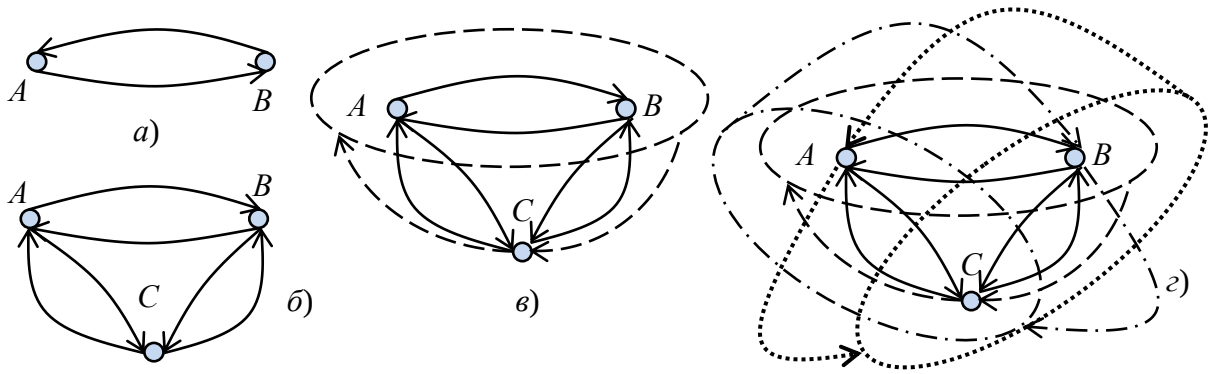


Рис. 3.2. Рост сложности системы с увеличением числа элементов и числа связей

Представление о сложности системы обычно складывается на основании представлений [7]

- об объёме оборудования (число элементов, номенклатура, габариты и т. п.), входящего в систему;

- разветвлённости связей между элементами и степенью их взаимодействия, что определяет безопасность, живучесть, надёжность, наблюдаемость, управляемость, устойчивость и др.;
- квалификации персонала, осуществляющего изготовление, монтаж, наладку и эксплуатацию элементов и системы в целом;
- стоимости строительства и удобства эксплуатации системы и др.

3.2. Формальное понятие сложности

Но на современном уровне развития ЭЭС (СЭС) подобного представления о сложности системы явно недостаточно. Нельзя точно определить, что такое сложная система, несмотря на то, что распознавание её доступно. Для исключения субъективных оценок необходимо введение формального понятия сложности, которое можно представить в нескольких вариантах.

1. В зависимости от учитываемых факторов и степени абстрактности описание СЭС можно представить в следующей символьной форме [54].

Система *S* есть нечто целое *A*. Двоичное суждение $A(1,0)$ отображает наличие или отсутствие этого качества: $S = A(1,0)$.

Система *S* есть организованное множество *M*, в котором *O* – оператор организации: $S = (O, M)$.

Система *S* есть множество *m* элементов, *n* свойств и *r* отношений: $S = (\{m\},\{n\},\{r\})$.

Система *S* есть множество *m* элементов, образующих *st* структуру и обеспечивающих определенное *be* поведение в условиях *SR* окружающей среды: $S = (\{m\}, st, be, SR)$.

Система *S* есть множество *x* входов, *y* выходов и *k* состояний, характеризуемых операторами *H* переходов и *G* выходов с учетом временной *T* динамики: $S = (\{x\},\{y\},\{k\}, H, G, T)$.

Функционирование системы *S* должно учитывать:

- условия существования – *kd*;
- обменные явления с внешней средой – *mb*;
- развитие – *ev*;
- функционирование – *fc*;
- репродукцию (воспроизведение) – *rp*;
- самообучение – *fl*,
- самоорганизацию – *fo*.

Тогда система представляется в виде: $S = (\{kd\},\{mb\}, ev, fc, rp, fl, fo)$.

В организационных системах, обеспечивающих, в частности, функционирование технологических (производственных) систем учитывают:

- цели – *z*;
- ресурсы внешние – out и внутренние – *in*;
- исполнителей – *ex*;
- помехи – *dt*;
- контроль – *sv*;
- управление – *rd*;
- эффект – *ef*.

При этом: $S = (\{z\}, \{out\}, \{in\}, \{ex\}, \{dt\}, \{sv\}, \{rd\}, \{tf\})$.

2. Обобщенное формальное описание понятия «система» представляется следующим образом.

Система – множество $\{A\}$, на котором заранее реализуются данное, интересующее нас, множество отношений $\{R\}$ с множеством фиксированных свойств $\{H\}$ [13].

Используя теоретико-множественные представления, определение системы *S* записывается в виде:

$$S \equiv \{A, R\} \quad \text{или} \quad S \equiv \{\{a_i\}, \{r_i\}\}, \tag{3.1}$$

где $A = \{a_i\}$ – множество элементов системы *S*, $R = \{r_i\}$ – множество отношений между ними; или – $a_i \in A, r_i \in R$.

Формализацией системы в записи

$$S \equiv \{\{a_i\} \& (r_j)\}, \quad a_i \in A, r_j \in R \tag{3.2, \textit{a}}$$

учитывается тот факт, что система – это не простая совокупность элементов и связей того или иного вида, а включающая только те элементы и связи, которые находятся в области & (логический символ «И», пересечения (конъюнкции)).

Для более четкого определения (формализации) элементов и связей системы учитывают их свойства *H*:

$$S \equiv \{A, R, H\}. \tag{3.3}$$

Таким образом, система представляется с учетом характеристик элементов $H(a_i)$ и связей $H(r_j)$:

$$S \equiv \{[a_i : H(a_i)] \& [r_j; H(r_j)]\}. \tag{3.4, \textit{a}}$$

Если по определению элементы системы неоднородны (генераторы, ЛЭП, трансформаторы, электроприёмники и т. д.), то выделяются их одно-

родные подмножества, обладающие свойством (атрибутом) H (воздушные ЛЭП одинакового напряжения на металлических опорах и т. п.):

$$S \equiv \{A, B, R\},\ A = \{a_i : H(a_i)\},\ B = \{b_k : H(b_k)\}. \qquad (3.5)$$

Если какой-то вид отношений r_1 применяется только к элементам разных A и B подмножеств исходной системы S и не используется внутри них самих, можно говорить о создании новой системы S_1 с элементами $a_i \in A,\ b_k \in B$, образованными из элементов исходных множеств

$$S_1 \equiv \{a_i r_1 b_k\}. \qquad (3.5, a)$$

Учет целенаправленности системы происходит при введении множества целей Z её функционирования (выдача определённой мощности по диспетчерскому графику, обеспечение показателей качества электроэнергии, экономических и экологических показателей производства, передачи и потребления электроэнергии):

$$S \equiv \{A, R, H, Z\}. \qquad (3.6)$$

Наряду с элементами и их свойствами, связями, целями, при решении конкретных задач требуется учет среды SR (грозовые и ветровые нагрузки, климатические условия района и др.), которая влияет на систему (или из которой она выделилась); наблюдателя N – лица, представляющего объект или процесс и формального языка LN этого наблюдателя

$$S \equiv \{A, R, H, Z, SR, N, LN\}. \qquad (3.7)$$

Дифференциация конкретных условий разработки, функционирования и прогнозирования системы (долгосрочное, краткосрочное, оперативное) может привести к еще большему количеству составляющих на интервале времени Δt.

3. Ещё более общее определение системы возможно, если она не расчленяется на подсистемы (элементы), а представляется как единое целое

$$S \equiv \{Z, STR, TECH, COND\},$$

где $Z=\{z_i\}$ – совокупность или структура целей; $STR=\{str_j\}$ – совокупность структур, реализующих цели z_i; $TECH=\{tech_k\}$ – совокупность, системных технологий (методы, средства, алгоритмы); $COND = \{COND_l\} = \{\varphi_{in}, \varphi_{ex}\}$ – условия существования системы (внешние φ_{ex} и внутренние φ_{in} факторы, влияющие на её создание и функционирование).

4. Сложность системы может быть оценена степенью целостности (связности, взаимозависимости элементов, устойчивости, управляемости, степени централизации управления) α и коэффициентом использования

компонентов системы (самостоятельность, автономность) β, которые интерпретируются как оценки устойчивости или централизации управления [54, 65, 66]

$$C_{\text{с}} = C_0 + C_{\text{в}}, \tag{3.8}$$

где $C_{\text{с}}$ – системная сложность, представляющая систему, как целое (сложность разработки, сооружения, монтажа, эксплуатации); C_0 – собственная сложность, представляющая суммарную сложность элементов вне связи их между собой, влияющая на достижение системой поставленной цели; $C_{\text{в}}$ – взаимная сложность, характеризующая степень взаимосвязи элементов системы (сложность устройства, схемы, структуры).

Разделив члены выражения (3.8) на C_0 получаем две сопряженные оценки: α – степень целостности и β – коэффициент использования компонентов системы

$$\alpha = -\frac{C_{\text{в}}}{C_0}; \qquad \beta = \frac{C_{\text{с}}}{C_0}; \qquad \beta = 1 - \alpha. \tag{3.9}$$

Знак минус введен для того, чтобы характеристика целостности α была положительной, поскольку $C_{\text{в}}$ в устойчивых системах, для которых характерно $C_0 > C_{\text{с}}$, формально имеет отрицательный знак [65, 66]. Это объясняется тем, что $C_{\text{в}}$ характеризует работу системы «на себя», а не на выполнение стоящих перед ней целей. Увеличение β трактуется как увеличение децентрализации управления, а увеличение α – централизации. Отсюда следует, что сумма «свободы» и «связности» элементов есть величина постоянная. Это свойство особенно актуально для ЭЭС с объектами РГ, ВИЭ и накопителями электроэнергии.

Важными характеристиками сложности структуры являются степень централизации α и норма управляемости μ.

Степень централизации α – мера разделения полномочий между иерархическими уровнями системы. Для каждой пары смежных уровней $(i-1,\ i),\ i = \overline{2, N}$ степень централизации измеряется отношением объёма задач μ_i, решаемых на i-м уровне, к объёму задач μ_{i-1}, решаемых на (i–1)-м уровне

$$\alpha_i = \frac{\mu_i}{\mu_{i-1}}.$$

Объём решаемых задач μ_i оценивается через количество перерабатываемой информации на i-м уровне. Тогда степень централизации системы в целом определяется как

$$\alpha = \sum_{i=1}^{N} \beta_i \alpha_i , \qquad \sum_{i=1}^{N} \beta_i = 1 ,$$

где β_i – весовой коэффициент соответствующего уровня системы.

Смещение основной массы решений в сторону высшего уровня (повышение степени централизации) обычно отождествляется с повышением управляемости подсистем и улучшением качества решений с одновременным увеличением объёма перерабатываемой информации на верхних уровнях. Смещение решений в сторону нижних уровней (повышение степени децентрализации) соответствует увеличению самостоятельности подсистем (системы РГ, ВИЭ), уменьшению объёма информации, перерабатываемой верхними уровнями.

Понятие степени централизации тесно связано с другой характеристикой сложности системы – нормой управляемости. Норма управляемости характеризует объём задач, решением которых может эффективно управлять лицо, принимающее решение (ЛПР). Ограничение на объём перерабатываемой информации в подсистемах существенно влияет на выбор структуры.

Степень централизации и норма управляемости, как правило, изменяются с переходом от одного иерархического уровня к другому (крупная районная подстанция – главная понизительная подстанция (ГПП) предприятия – распределительная подстанция (РП) – цеховая трансформаторная подстанция (ТП)). Кроме того, на характеристики управляемости большое влияние оказывает автоматизация управления коммутационными аппаратами. Определение количественных показателей степени централизации и нормы управляемости – одна из важных и вместе с тем наиболее трудных проблем синтеза структур.

Например, в задачах электроэнергетики размещение устройств автоматической частотной разгрузки (АЧР) можно произвести на разных уровнях напряжения схемы электроснабжения потребителя. Снижение уровня иерархии приводит к повышению эффективности работы системы при наличии конкретной и достоверной информации низших уровней иерархии СЭС. Достигаемый при этом эффект характеризуется снижением экономических потерь за счёт увеличения числа и рационального выбора отключаемых присоединений [50]. С другой стороны, увеличивается структурная сложность системы АЧР (увеличивается количество элементов, вероятность их отказа и ложного срабатывания, вычислительная сложность, сложность монтажа и обслуживания).

5. Предположим, что в СЭС имеется *n* типов элементов (трансформаторов, генерирующих установок или др.) и *k* – число элементов каждого типа (мощность, класс напряжения и др.). Для каждого типа элементов мето-

дом экспертных оценок или интуитивно (с учетом накопленного опыта) устанавливается сложность элемента, измеряемая некоторым числом s_{ij}. Сложность s системы, состоящей из элементов со сложностью s_i (i = 1, 2, … , n) определится как

$$s = \sum_{i=1}^{n} \sum_{j=1}^{m} s_{ij} k_j ,$$

где k_j $(j = 1, 2, ..., m)$ – число элементов i-го типа, входящих в систему.

При наличии $nk = L$ элементов в системе максимальное число связей между элементами – $N = L(L-1)$. Но при достаточно большом L число фактических связей N^*, как правило, $N^* < N$, а относительное число реализованных связей

$$\alpha = \frac{N^*}{N}.$$

Относительная сложность связей определяется коэффициентом v. Тогда сложность всей системы определится выражением

$$S = (1 + v\alpha)s ,$$

где v – коэффициент, учитывающий сложность связей по сравнению со сложностью элементов системы.

Возможности системы определяются её потенциалом – основой эффективности ее деятельности. Поэтому повышение потенциала системы представляет задачу первостепенной важности [54, 65, 66].

Под потенциалом подразумевается существующие у системы жизненно важные ресурсы (материальные, энергетические, людские, информационные, экономические, временны́е, социальные, духовные и т. п.), которые включают как количественные, так и качественные составляющие и могут быть приведены в действие, для достижения определенной цели. Потенциал любой системы определяют ресурсы, которые используются при решении задач, то есть, являются актуализированными. Если ресурсы пока не используются, но могут быть использованными, то они являются неактуализированными.

Проблема управления системой упрощается, если она располагает количественно большим потенциалом и возможностью его использования по мере необходимости. Неактуализированная часть потенциала вводится в действие для повышения надёжности выполнения поставленной цели. В «хорошо» организованной системе A её потенциал P превышает сумму потенциалов всех составляющих элементов (подсистем)

$$P(A) > [P(a_1) + P(a_2) + ... + P(a_n)].$$

В «нейтральных» системах, или псевдосистемах, где степень организованности не обеспечивает эффективного и согласованного взаимодействия элементов, потенциал системы равен сумме потенциалов элементов

$$P(A) = [P(a_1) + P(a_2) + ... + P(a_n)].$$

В «плохо» организованных, или неорганизованных системах, где взаимодействие элементов носит неуправляемый или случайный характер, потенциал всей системы равен потенциалу её отдельного усредненного элемента

$$P(A) = \frac{P(a_1) + P(a_2) + ... + P(a_n)}{n}.$$

В «плохо» организованной системе, когда взаимодействие элементов носит антагонистический характер и каждый элемент противодействует всем остальным («война каждого со всеми»), потенциал системы меньше потенциала самого слабого элемента

$$P(A) < \min[P(a_1), P(a_2), ..., P(a_n)].$$

В этом случае потенциал всей системы оценивается как разность потенциалов элементов в произвольном парном порядке пока от системы не останется один элемент. При этом чем менее дифференцированы значения потенциалов элементов, тем меньше их результирующий системный потенциал $P(A)$, который в пределе, при $n \to \infty$, приближается к нулю $P(A) \to 0$.

Таким образом, у «плохих» систем, или псевдосистем, потенциал системы может быть меньше суммы потенциалов элементов и даже одного элемента.

В строго научном понимании «плохо» организованные системы не удовлетворяют системным требованиям, в первую очередь по интегративным качествам.

6. Сложность системы S в аспекте системности представляется суммой сложности состава $S_с$ и организации $S_о$:

$$S = S_с + S_о ,$$

где: $S_с = S_{суб} + S_п + S_д + S_г$; $S_{суб}$ – субстратная, $S_п$ – параметрическая, $S_д$ – динамическая и $S_г$ – генетической сложности.

Под субстратом понимают простейшие структуры (элементы), которые остаются устойчивыми, неизменными при любых преобразованиях системы и обусловливают её конкретные свойства. Субстратная сложность складывается из сложности компонентов, подсистем и уровней анализируемой системы.

Параметрическая сложность включает субстратные свойства, сложность связей и отношений.

Динамическая сложность определяется сложностью состояний, стадий, фаз и переходных процессов.

Генетическая или эволюционная сложность включает развитие (возможность изменений) числа состояний, стадий, уровней системных параметров, режимов и т. п.

Сложность организации системы $S_{\text{о}}$ представляется суммой:

$$S_{\text{о}} = \{R\} + \{L\},$$

где: $\{R\}$ – множество связей и отношений, объединяющих иерархические уровни управления, подсистемы внутри уровней, компоненты; $\{L\}$ – множество законов, инструкций правил, обеспечивающих функционирование и развитие системы.

Таким образом, система не может быть универсально сложной. Сложность ЭЭС и СЭС может представляться рядом интегральных показателей, каждый из которых в каждом конкретном случае нуждается в детальном анализе.

Число элементов, сила межэлементных связей, их локализация, могут неконтролируемо меняться, что делает поведение сложных систем (особенно в экстремальных условиях функционирования) неопределённым и, соответственно, плохо предсказуемым. Поэтому расчёту или теоретическому анализу, связанному с исследованием сложной системы, предшествует накопление статистического материала, характеризующего поведение отдельных элементов, их групп и системы в целом в реальных условиях эксплуатации.

3.3. Особенности учёта возможных колебаний системных параметров

Влияние изменения жизненно важных параметров на систему неодинаково и зависит от множества факторов внешнего (состояние среды, связи с другими системами) и внутреннего характера (диапазон изменений параметров). Последовательная смена состояний системы, связанная с изменением параметров режима и (или) параметров системы во времени определяет ее поведение.

Область допустимого изменения общесистемного параметра *X(t)* в пределах границ $\{\alpha,\beta\}$ представлена на рис. 3.3.

Пока значение $X(t)$ не выходит за пределы $\alpha < X < \beta$, система сохраняет интегративное качество, включающее свойства: целостности (единство, достигаемое посредством взаимосвязей и взаимодействий элементов и проявляющиеся в возникновении новых свойств) и эмерджентности (степень

несводимости свойств системы к свойствам элементов, обусловливающее появление новых свойств и качеств, не присущих элементам, входящих в состав системы). При выходе X за пределы $\alpha < X < \beta$ (пунктир на рис. 3.3) система утрачивает свое интегративное качество, и по определению при $t > t_5$ перестает существовать. Однако критические значения частных компонент общесистемного параметра X могут принимать значения $\{\gamma > \alpha, \delta < \beta\}$.

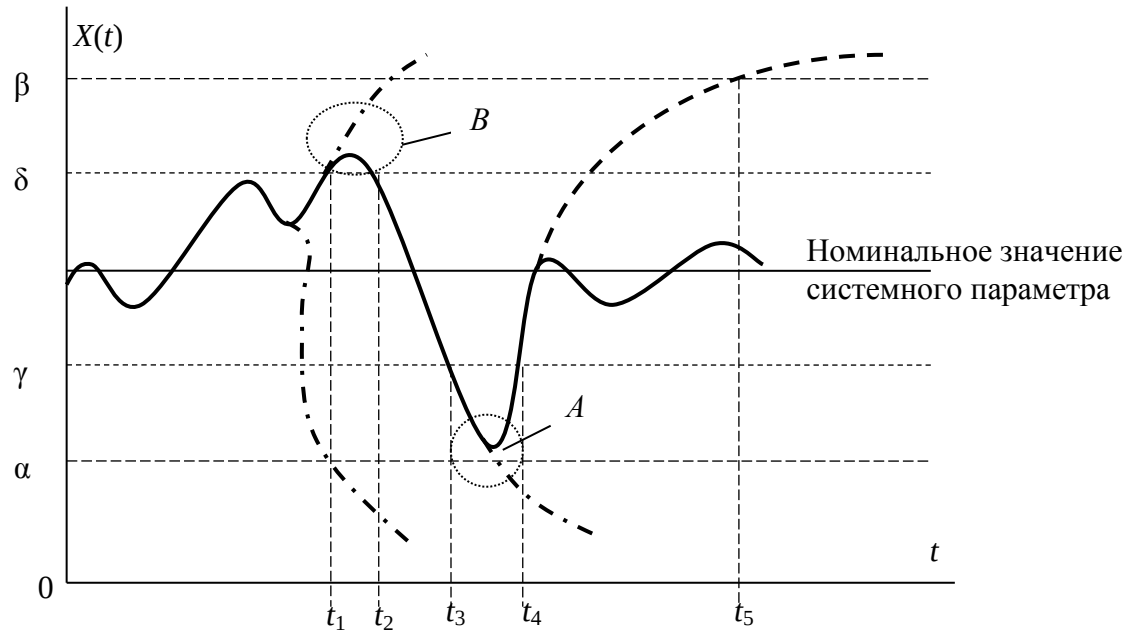


Рис. 3.3. Возможные колебания
общесистемного параметра

При $\gamma < X < \alpha$ или $\delta < X < \beta$ система переходит в новое качественное состояние, но не прекращает существовать как целое. Это происходит в диапазонах времён $\{t_1, t_2\}$ и $\{t_3, t_4\}$. Приближение системных параметров к предельно допустимым значениям (области *A* и *B* на рис. 3.3) может порождать ситуацию системного кризиса – стадии жизни системы, когда её длительное дальнейшее функционирование оказывается под вопросом.

Системный кризис может привести к распаду, разрушению и даже прекращению существования системы, если вовремя не принять соответствующие меры. Здесь система вступает в зону бифуркации и будущее её состояние становится непредсказуемым. В связи с развитием систем распределённой генерации, электроснабжения потребителей от ВИЭ и ростом IOT системный кризис может привести к распаду, разрушению и даже прекращению существования СЭС, если вовремя не принять соответствующие меры. Здесь система вступает в зону бифуркации и будущее её состояние становится непредсказуемым.

Под влиянием малейших флуктуаций даже какого-либо одного фактора, внутреннего или внешнего, она может начать процесс случайного движения в нескольких альтернативных направлениях, крайние из которых – возврат в нормальное состояние или прекращение существования. На рис. 3.4 приведены примеры траекторий движения системы с точками возможной бифуркации [54]. Под действием ряда факторов в некоторой точке p_i происходит разветвление траектории движения системы. В этой точке система сама принимает решение и случайным образом выбирает новое направление своего дальнейшего движения до следующей точки бифуркации p_{i+1}. Там снова происходит выбор и процесс повторяется. Точно предсказать моменты бифуркаций и результаты выбора направления движения невозможно ни при каком сколь угодно глубоком и полном знании системы, ни при каком сколь угодно длительном наблюдении за её поведением.

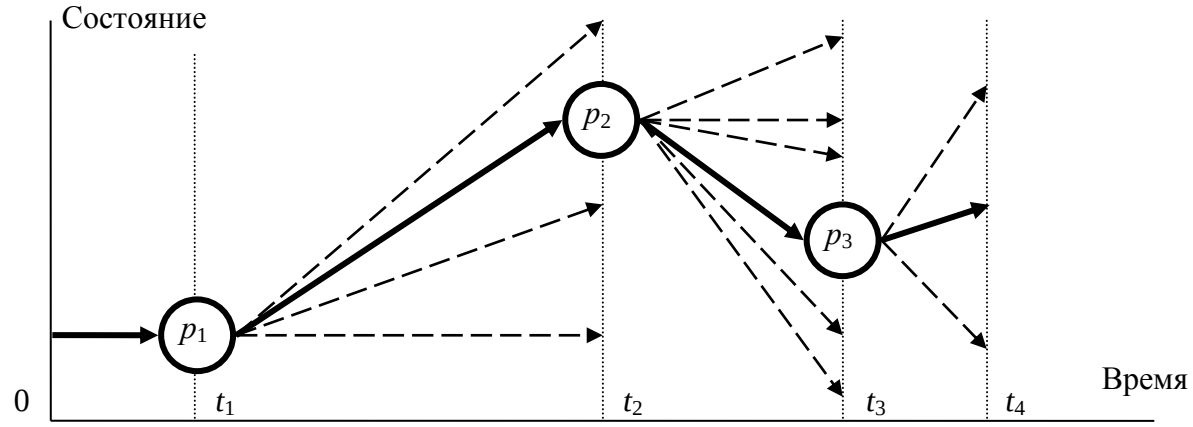


Рис. 3.4. Последовательные бифуркации

Особый вид кризисов представляют собой внезапные, резкие, лавинообразные изменения параметров систем из-за дезорганизующих внешний воздействий или внутренних противоречий. Сущность любого скачкообразного преобразования заключается в таких резких изменениях отдельных структурных элементов системы (или системы в целом), которые приводят к внезапному изменению путей ее дальнейшего развития. Некоторые формы таких скачков рассматриваются как катастрофы (штрих-пунктир на рис. 3.3).

Развитие лавинообразного процесса (рис. 3.5) обусловлено накоплением факторов (энергии) деградации ещё до возникновения «взрыва». Постоянно накапливаемая энергия деградации образует негативный фон $Э_{нф}$. После превышения энергией деградации значения $Э_{нфл}$ при $t_л$ происходит интенсивное, лавинообразное развитие процесса, которое в момент $t_в$ достижения величины $Э_{нфв}$ приводит к катастрофе («взрыву»).

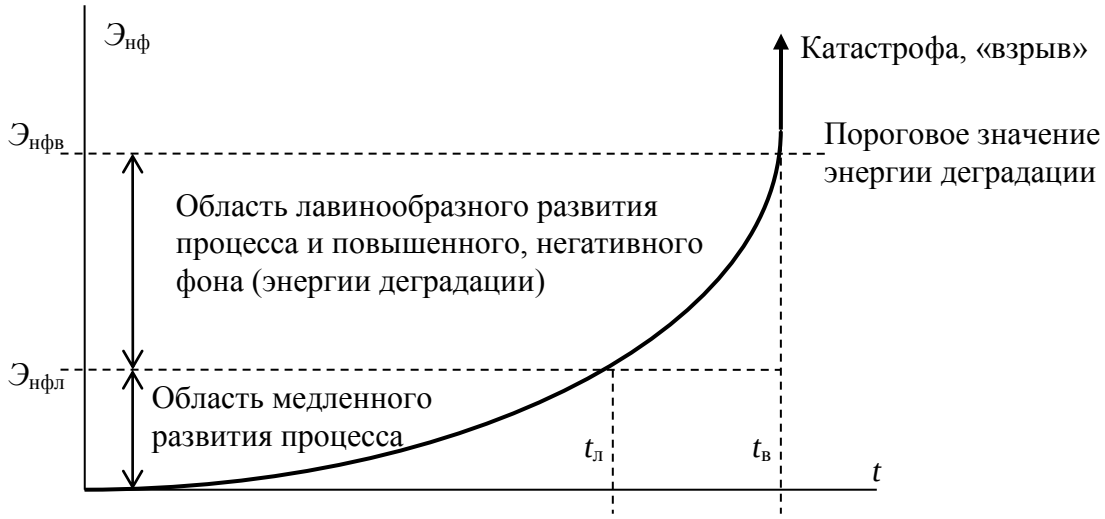


Рис. 3.5. Развитие лавинообразного процесса

Частным случаем развитием лавинообразного процесса является экспоненциальный рост, который обладает характерным свойством, называемым «время удвоения». Время удвоения – интервал, за который происходит удвоение значения соответствующей переменной величины системы.

Экспоненциальный рост нагляден при сравнении его с некоторым пределом. Предположим, что один из системных параметров, начиная со значения $П = 0{,}1$, удваивается за каждую единицу времени (таблица 3.1).

Таблица 3.1

Пример экспоненциального роста параметра П

t	0	1	2	3	4	5	6	7
$П$	0,1	0,2	0,4	0,8	1,6	3,2	6,4	12,8

Критический уровень этого системного параметра примем $П_{кр} = 10{,}0$, когда конфликтные взаимодействия между его ростом и принятым ограничением становятся существенными. Здесь очевидно, что рост определяющего параметра, который происходит на интервале от $6t$ до $7t$ на величину 3,2 единицы, происходит всего за $0{,}25t$, что уже достаточно близко к $П_{кр} = 10{,}0$.

При построении зависимости $П(t)$ масштаб следует выбирать так, чтобы кризисный уровень находился примерно на середине вертикальной оси, поскольку при этом видна крутизна кривой и «взрывной» характер процесса.

Если внутри системы наблюдается напряжённое состояние, то достаточно появления спускового (триггерного) механизма, способного перевести систему в критическое состояние (интервал между $t_л$ и $t_в$ на рис 3.5). Примерами развития аварийных лавинообразных процессов в элек-

троэнергетике, приводящими к нарушению устойчивости, являются «лавина напряжения» и «лавина частоты».

Естественно, что и внешние, и внутренние случайные воздействия оказывают влияние на режимы работы элементов системы и могут существенно менять режимы её функционирования. Пусть ξ – случайная величина, характеризующая некоторое внешнее воздействие на исследуемую СЭС или на один из внутренних её параметров (элементов) с законом распределения $f_\xi(x)$. В общем случае результат U функционирования СЭС зависит от ξ: $U = \varphi(\xi)$ и также является случайной величиной, закон распределения которой определяется функциями φ и $f_\xi(x)$. Очевидно, что каждому возможному значению ξ соответствует некоторое возможное значение случайной величины U. При этом рассеивание (разброс) значений воздействий внешней среды приводит и к рассеиванию результатов её функционирования.

Для прогнозирования результатов функционирования как ЭЭС, так и СЭС желательно оценить поведение системы в среднем под воздействием случайных факторов, то есть, выяснить, будет ли справедливо отношение

$$\varphi[M(\xi)] = M(U)\,, \qquad (3.10)$$

где $M(\xi)$ – математическое ожидание ξ; $M(U)$ – математическое ожидание U.

Другими словами, если ξ примет значение $M(\xi)$, то будет ли соответствующее значение U равно $M(U)$. Иначе, будет ли рассеивание внешних воздействий или значений параметров системы вызывать только рассеивание результатов её функционирования или, с учётом действия случайных факторов, может изменяться её поведение в среднем [6, 7].

Например, из-за непостоянства нагрузки P электропотребление W – случайная величина с соответствующим рассеиванием, но его средняя величина в большинстве случаев соответствует номинальным значениям (рис. 3.3). Можно ли при этом считать, что W будет средним, если P равна номинальному значению, так как под воздействием случайных факторов (даже когда средние их значения равны номинальным), результаты функционирования системы U (в нашем примере W) не только подвергаются рассеянию, но и получают смещение средних значений, что вызывает сомнение в справедливости формулы (3.10).

В качестве примера рассмотрим линейную функцию [6, 7]:

$$U = a\xi + b. \qquad (3.11)$$

Математическое ожидание линейной функции определяется как [10]

$$M(U) = aM(\xi) + b. \qquad (3.12)$$

Сопоставляя (3.11) и (3.12), очевидно, что при линейной зависимости между случайными факторами и результатами функционирования системы смещение средних значений отсутствует.

Во многих практических задачах требуется (желателен) учёт нелинейности функций факторов, воздействующих на систему. В [22] отмечается, что за исключением некоторых специальных случаев, невозможно вывести точные формулы плотности вероятности этих нелинейных функций, и, следовательно, необходимо описывать эти плотности вероятностей с помощью моментов распределения.

Если $\varphi(\xi)$ функция нелинейная, например, квадратичная, что характерно для ряда процессов в СЭС

$$\varphi(\xi) = \xi^2, \tag{3.13}$$

то

$$M(U) = M(\xi^2). \tag{3.14}$$

При этом математическое ожидание квадрата случайной величины равно второму её моменту [6–8]

$$M(U) = M(\xi^2) = [M(\xi)]^2 + \sigma_\xi^2 , \tag{3.15}$$

где σ_ξ^2 – дисперсия случайной величины ξ.

Сопоставляя выражения (3.15) и (3.13) очевидно, что разница между ними равна дисперсии σ_ξ^2 случайной величины ξ. Таким образом при нелинейности функций факторов, воздействующих на систему возникает смещение математического ожидания (среднего значения) $M(U)$ – результата функционирования системы. Естественно, что это обстоятельство требует дополнительной информации и особого внимания к учёту случайных факторов при исследовании сложных систем.

Важной задачей системного анализа является определение границы между системами, а также между системой и средой, поскольку не всегда ясно, как выделить анализируемую систему. В рассматриваемых условиях функционирования ЭЭС и СЭС одной из таких границ может быть граница балансовой принадлежности.

Граница системы – это совокупность объектов, одновременно принадлежащих (например, технологически) и не принадлежащих (например, при экономических расчётах) данной системе. При этом границы системы почти всегда неопределенны, расплывчаты. Для формализации этого понятия вводится мощность межэлементных связей:

$$\omega = \omega(m, \gamma),$$

где m – элементы системы; γ – межэлементные связи.

Тогда граница системы определяется как

$$F(m, \gamma, \omega_0) = 0,$$

где ω_0 – заданная для данной системы минимальная мощность межэлементных связей.

Внутри анализируемой системы будут находиться элементы m_1, с межэлементными связями γ_1 мощностью $\omega(m_1, \gamma_1) > \omega_0$.

Вне системы остаются элементы m_2, у которых межэлементные связи γ_2 имеют мощность $\omega(m_2, \gamma_2) < \omega_0$. Могут быть и пограничные элементы m_3, у которых есть хотя бы одна связь γ_3 мощностью $\omega(m_3, \gamma_3) \le \omega_0$, а остальные связи – $\omega(m_3, \gamma_3') > \omega_0$.

4 РАСШИРЕНИЕ НАДЁЖНОСТНЫХ СВОЙСТВ ЭЛЕКТРИЧЕСКИХ СИСТЕМ

4.1. Вводные замечания

Проблемам оценки, обеспечения повышения и оптимизации показателей надёжности элементов и систем электроэнергетики посвящено большое количество исследований, проведённых коллективами и отдельными исследователями середины XX [18, 27, 36, 44, 46, 69, 70, и др.], и начала XXI века [14, 15, 47, 71 и др.]. Большинство этих разработок применимо в основном к элементам (электроприёмникам, установкам, объектам) систем энергетики, включая ограниченную совокупность технических свойств их функционирования и развития.

Поскольку процесс функционирования сложной системы представляется совокупностью действий её элементов, подчинённых единой цели, особое место в исследовании ЭЭС, СЭС и их подсистем занимает вопрос оценки эффективности работы, осуществляемой на основе соответствующих показателей. Они могут использоваться для выбора оптимальных параметров и режимов функционирования и управляющих алгоритмов в системах электроэнергетики, сравнительной оценки вариантов при проектировании и развитии СЭС (ЭЭС).

Под показателем эффективности понимается числовая характеристика системы, оценивающая степень приспособленности её к выполнению поставленных задач [6, 74 – 76]. Выбранный показатель эффективности должен максимально полно учитывать структурные особенности системы, значения её параметров, режимы, свойства отдельных элементов, условия её функционирования, воздействие внутренних и внешних случайных факторов.

Следовательно, можно представить множество возможных процессов функционирования системы, элементы которого отличаются различными режимами и условиями работы. Каждому элементу этого множества ставится в соответствие элемент другого множества – множества значений показателей эффективности, являющихся действительными числами. В этом случае можно говорить об отображении множества процессов функционирования системы на множество действительных чисел в некотором заданном интервале.

Таким образом, показатель эффективности – функционал от процесса функционирования системы. Функционал здесь – функция, заданная на

множестве процессов функционирования системы, принимающая значения из области действительных чисел. Элементам множества процессов функционирования ставится в соответствие множество случайных событий, каждому из которых соответствует функционал, принимающий значения 1 (событие произошло) и 0 (события не было). Вероятность события определяется средним значением соответствующего функционала.

В [6, 48] в качестве показателей эффективности рекомендуется использовать вероятности случайных событий (вероятность аварийной ситуации, перегрузки оборудования, вероятность восстановления в течение определённого времени, вероятность выполнения производственного задания в условиях ограничений и т. п.). Если A – событие, состоящее в том, что задача решена, то показатель эффективности $Э$ есть вероятность события A

$$Э = P(A).$$

Так как ЭЭС и СЭС работают в условиях действия случайных факторов, значения функционалов оказываются также случайными величинами, что затрудняет их оценку и применение. Поэтому целесообразен переход к их средним значениям. При решении множества однотипных задач интерес представляет средний размер успеха (ущерба) Тогда относительно каждой задачи достаточно знать математическое ожидание получаемого в результате её решения успеха(ущерба):

$$Э = M(Y),$$

где Y – достигнутый успех или ущерб.

Любая система имеет практически неограниченное число свойств. Но если каждая подсистема (элемент) будут работать с максимальной эффективностью, система в целом может и не обеспечить также максимальной эффективности, поскольку эффективность системы зависит не только от работы её элементов, а и от их взаимодействий.

Отдельные показатели эффективности сложных систем оцениваются при помощи числовых характеристик, определяющих степень приспособленности системы к выполнению поставленных перед ней задач. Каждая из них должна удовлетворять следующим требованиям:

- представлять показатель (параметр), зависящий от особенностей функционирования системы;
- давать наглядное представление об одном из свойств системы;
- допускать приближенную оценку числовых характеристик параметров по экспериментальным данным.

Поскольку условия функционирования ЭЭС отличаются от стационарных, необходимо указывать период или условия, к которым относится рассматриваемое значение показателя эффективности, так как в зависимости от

выбора характеристик системы соответствующим образом интерпретируются её свойства и результаты исследования.

Так, если в качестве показателя эффективности работы электростанции принять коэффициент использования установленной мощности (КИУМ), то при проведении мероприятий по его увеличению наибольшее внимание и будет уделяться факторам, способствующим его увеличению. При этом неизбежно будут упущены из вида другие стороны работы именно этой станции, не связанные непосредственно с увеличением КИУМ (изменение параметров режима присоединённой сети, износ оборудования, дополнительный расход первичных энергоносителей, увеличение себестоимости производства электроэнергии, изменение количества выбросов и др.).

Если в качестве показателя эффективности этой же станции выбрать себестоимость производимой электроэнергии, то факторы, связанные с дополнительным расходом первичных энергоносителей, фондом зарплаты, изменением количества выбросов будут иметь больший вес.

Таким образом, характер показателя эффективности определяет основные направления в поиске свойств, обеспечивающих оптимальность режимов функционирования системы. Для согласования разнородных тенденций в характере работы системы возможно использовать показатели эффективности, содержащие ограничительные условия. В рассмотренном выше примере с электростанцией такими показателями могут быть:

а) КИУМ, при условии обеспечения средней себестоимости производства электроэнергии;

б) средняя себестоимость производства электроэнергии, при условии обеспечения заданного КИУМ.

Однако отметим, что использование показателей эффективности с ограничительными условиями может оказаться тормозом повышения эффективности функционирования системы в целом. Так, жёсткое ограничение себестоимости может тормозить увеличение затрат в связи с введением новых технологий. Но если допустить возможность относительно небольшого её увеличения, в дальнейшем возможно значительное увеличение производительности и соответственно прибыли.

На основании изложенного очевидно, что при использовании показателей эффективности с ограничениями необходимо дополнительно учитывать возможные последствия введенных ограничений. Поэтому вполне естественно желание исследователей, разработчиков и эксплуатационного персонала употреблять такие показатели эффективности, которые позволяют согласовать разнородные тенденции в задачах и целях функционирования сложной системы.

Поскольку любой показатель эффективности системы R зависит от ряда параметров, выделяются параметры системы α_1, α_2, …, α_n и параметры, характеризующие воздействия внешней среды β_1, β_2, …, β_m:

$$R = R(\alpha_1, \alpha_2, \dots \alpha_n;\ \beta_1, \beta_2, \dots \beta_m. \qquad (4.1)$$

Помимо параметров системы и внешней среды, явно присутствующих в строгом математическом описании (4.1), обобщенный или комплексный показатель эффективности зависит от структуры системы, характера связей между элементами, вида управляющих алгоритмов, особенностей и закономерностей функционирования, не поддающихся формализации. Поэтому на практике, особенно при проведении предварительных расчетов, предлагается пользоваться приближенными методами.

В процессе жизненного цикла системы количество показателей эффективности и их числовые значения могут существенно изменяться. Поэтому остановимся лишь на основных показателях, в число которых входят: надежность, безопасность, живучесть, управляемость, помехозащищенность, устойчивость, экономичность.

4.2. Основные единичные и комплексные показатели надёжности СЭС

Надежность – свойство, которое должно учитываться при исследовании, создании, функционировании и прогнозировании перспективного развития. Однако в отличие от элементной надежности пути обеспечения надёжности сложных систем не очевидны и в каждом отдельном случае обусловлены особенностями исследуемой системы. По мере усложнения систем становится более сложной и оценка их надёжности. Классические показатели надёжности элементов «простых» систем такие, как «среднее время безотказной работы», «вероятность безотказной работы в течение заданного промежутка времени» и целый ряд других, применительно ко многим «сложным» системам, лишены практического смысла [6, 74].

Для сложной системы задача оценки надёжности формулируется в предположении известных, полученных статистическими методами характеристик интенсивности отказов её элементов и восстановлений в течение определённого времени: математического ожидания и дисперсии, закона распределения времени между отказами и др. В самом общем виде под отказом сложной системы понимается событие, когда выходной объём информации снижается до уровня, меньше допустимого [48]. Однако известно, что многие сложные системы могут выполнять практически все

свои функции при условии, что некоторая часть их элементов и связей между ними находится в нерабочем (или отличающемся в пределах допустимых норм от рабочего) состоянии.

Например, отказ отдельных элементов в системах энергетики может вообще не отразиться на работе потребителей. Но в этих случаях речь идет не об отказе системы, а лишь о возможном снижении показателей эффективности её работы.

Сосредоточивая внимание на самом факте отказа, классические единичные показатели надёжности [44] часто не позволяют установить последствия отказа и влияние его на конечный эффект функционирования системы. Поэтому для выработки обоснованных рекомендаций по обеспечению требуемого уровня надёжности сложных систем необходимы научные исследования, соизмеримые по своим масштабам разработке основной идее построения системы. Относительно недавно появились предложения по прогнозированию уровня надёжности оказываемых услуг при управлении единой национальной (общероссийской) электрической сетью (ЕНЭС) и территориальными сетевыми организациями (ТСО) [37] на основе комплексных показателей, применяемых зарубежными энергокомпаниями [5, 43], где в качестве индикаторов системной надежности используются:

SAIFI (System Average Interruption Frequency Index) – среднее число перерывов электроснабжения в расчёте на одного конечного потребителя (клиента), которые он испытывает в течение года

$$\text{SAIFI} = \frac{N_i}{N}, \tag{4.2}$$

где N_i – число потребителей, для которых наблюдались перерывы (отказы) электроснабжения; N – обще число потребителей энергокомпании.

SAIDI (System Average Interruption Duration Index) – индекс средней длительности перерывов (отключений) электроснабжения конечных потребителей в течение года

$$\text{SAIDI} = \frac{T}{N}, \tag{4.3}$$

где T – среднегодовое время простоя потребителей энергокомпании.

CAIDI (Customer Average Interruption Duration Index) – средняя продолжительность отключений в системе. В отдельных случаях – среднее время восстановления или среднее время простоя в течение года

$$\text{CAIDI} = \frac{\text{SAIDI}}{\text{SAIFI}}. \tag{4.4}$$

RNRE (Relative Network Reconstruction Efficiency) – относительная эффективность реконструкции сети, характеризующая, насколько улучшится SAIFI после реконструкции по сравнению с ситуацией до реконструкции

$$\text{RNRE} = \frac{1-\text{SAIFI}}{\text{SAIFI}(0)}, \tag{4.5}$$

где SAIFI(0) – среднее количество установившихся повреждений в год на одного потребителя до и после реконструкции соответственно.

ARAE (Average Recloser Fpplicftion Efficiency) – средняя эффективность применения реклоузеров, характеризующая среднюю эффективность применения реклоузеров, то есть, насколько удалось улучшить SAIFI каждого фидера реконструированной сети по сравнению с ситуацией до реконструкции в пересчёте на один реклоузер

$$\text{ARAE} = \frac{\text{RNRE}-F}{R}, \tag{4.6}$$

где F – количество фидеров, входящих в реконструированную сеть, R – количество установленных в процессе реконструкции реклоузеров.

CAIFI (Customer Average Interruption Frequency Index) – средняя частота отключения одного потребителя.

MAIFI (Momentary Average Interruption Frequency Index) – мгновенный индекс средней частоты отключений.

LOEE (Loss of Energy Expectation) – математическое ожидание годового объёма ограничений потребителей в электрической энергии из-за аварийных длительных ремонтов оборудования (см. EUE).

EUE (Expected Unserved Energy) – математическое ожидание годового объёма ограничений потребителей в электрической энергии $M[\Delta W]$ из-за аварийных длительных ремонтов оборудования (см. LOEE).

LOLE (Loss of Load Expectation) – ожидаемое число суток в году, когда происходит потеря нагрузки или среднее число суток в году, когда возникает дефицит мощности.

LOLH (Loss of Load Hours) – среднее число часов дефицита мощности или длительность потери нагрузки в часах.

LOLP (Loss of Load Probability) – вероятность потери нагрузки; вероятность дефицита мощности на малом (заданном) интервале времени, как правило, в период максимальной нагрузки

$$\text{LOLP} = \frac{P_F}{e},$$

где P_F – вероятность состояния отказа системы – доля времени, в течение которого система находится в состоянии отказа; e – параметр модели [84].

LCOE (Levelized Cost of Electricity) – средняя расчётная (нормированная) себестоимость производства электроэнергии на протяжении жизненного цикла электростанции (включая все возможные инвестиции, затраты и доходы).

LOLD (Loss of Load Duration) – продолжительность потери нагрузки.

LOLF (Loss of Load Frequency) – частота потери нагрузки.

MTBFO (Mean time between forced outages) – среднее время между вынужденными отключениями.

Несмотря на множество предложенных показателей, они позволяют лишь в среднем оценить состояние СЭС на основе не всегда достаточной и достоверной ретроспективной информации. Применение их в целях оценки и (или) прогнозирования функционирования системы на более коротких интервалах, в разных режимах и при переменной структуре практически невозможно.

Но под надёжностью СЭС можно понимать и степень соответствия возможных или фактически достигнутых результатов B требуемым для выполнения стоящих перед ней задач [40]. Тогда

$$R = \{B_{\downarrow} \leq B \leq B^{\uparrow}\}, \tag{4.7}$$

где R – событие, заключающееся в выполнении СЭС заданных функций (задач) в заданном объёме, с соблюдением всех установленных нормативов; $B_{\downarrow}$ и $B^{\uparrow}$ – нижний и верхний пределы необходимого результата функционирования СЭС.

По выражению (4.7) оценивается надёжность одноцелевой (простой) системы или обобщённый результат функционирования многоцелевой системы (например, РГ, ВИЭ). Возможно также определение вероятности P степени соответствия результатов требуемым для выполнения соответствующих задач:

$$P(R) = P\{B_{\downarrow} \leq B \leq B^{\uparrow}\}.$$

При необходимости оценки надёжности многоцелевой системы с представлением результатов выполнения каждой из n целей в отдельности, обобщённая надёжность СЭС может быть представлена как

$$R = \begin{vmatrix} B_{\downarrow 1} \leq B_1 \leq B^{\uparrow 1} \\ \dots\dots\dots\dots\dots\dots \\ B_{\downarrow i} \leq B_i \leq B^{\uparrow i} \\ \dots\dots\dots\dots\dots\dots\dots \\ B_{\downarrow n} \leq B_n \leq B^{\uparrow n} \end{vmatrix}, \tag{4.8}$$

где $B_{\downarrow i}$ и $B^{\uparrow i}$ – нижний и верхний пределы необходимого результата функционирования СЭС при решении i-й задачи; B_i – возможныq или фактический результат функционирования СЭС для выполнения i-й задачи.

Надёжность по (4.8) – составная часть и основная характеристика эффективности функционирования СЭС. Результат функционирования – группа случайных событий, число которых равно числу целей (задач) поставленных перед конкретной СЭС. Здесь возможен анализ следующих событий:

- выполнение СЭС всех n поставленных задач;
- выполнение СЭС ряда наиболее важных $k < n$ задач;
- выполнение СЭС не менее заданного $n_0 < n$ числа задач и др.

Показатели надёжности могут быть определены вероятностями осуществления соответствующих событий: $P_n;\ P_k;\ P_{n_0<n}$, их математическим ожиданиями и дисперсиями, а при наличии достаточного количества информации – функциями распределения вероятностей результатов функционирования.

В общем виде формула (4.8) представляется как

$$P(R_n) = P\left(\begin{vmatrix} B_{\downarrow 1} \le B_1 \le B^{\uparrow 1} \\ \dots\dots\dots\dots\dots\dots \\ B_{\downarrow i} \le B_i \le B^{\uparrow i} \\ \dots\dots\dots\dots\dots\dots\dots \\ B_{\downarrow n} \le B_n \le B^{\uparrow n} \end{vmatrix}\right), \qquad (4.9)$$

где $P(R_n)$ т – вероятность выполнения СЭС всех функций.

Проверка и подтверждение требований к результатам B функционирования СЭС осуществляется на основе нормативных значений соответствующих показателей надёжности. Правильность их выбора (критерий достоверности подтверждения надёжности СЭС) оценивается вероятностью

$$P_R = (R_\text{ф} \le R_\text{н}),$$

где $R_\text{н}$ и $R_\text{ф}$ – нормативное и фактическое значения показателя надёжности.

Если $R_\text{н}^*$ – функционал, значение которого соответствует показателю эффективности, вычисленному при условии, что отказы элементов имеют интенсивности, соответствующие заданным (расчётным) характеристикам, а R^0 – то, что все элементы абсолютно надёжны (интенсивности отказов элементов равны нулю), показатель надёжности сложной системы определится разностью [6]

$$\Delta R_\text{н}^0 = R^0 - R_\text{н}^*, \qquad (4.10)$$

откуда видно снижение эффективности системы из-за отказов её элементов по сравнению с идеальной системой, элементы которой абсолютно надёжны. Поскольку идеальной системы не существует, такая оценка эффективности может быть использована только для сравнения вариантов (по полно-

те и точности исходной информации, структурным особенностям, качеству управляющих алгоритмов и т. п.).

4.3. Надёжностные свойства современных СЭС

В руках человечества оказались гигантские производственные и энергетические мощности, функционирование которых чрезвычайно опасно по целому ряду причин:

- сложность прогнозирования места, времени, развития и последствий техногенных и природных катастроф, научных и технологических прорывов;
- развитость коммуникационных и транспортных средств сокращает лимит времени, отведенный на принятие решений и организацию мер противодействия в случае возникновения опасности;
- отсутствие эффективных средств оказания давления (правовых норм) на неблагоприятные для государства (мирового сообщества) технологические, экологические, социальные и другие угрозы, исходящие от существующих и проектируемых объектов и глобальных проектов;
- достижения в области технологии не всегда способствуют прогрессу, вредя здоровью и экологии, часто обладая непредсказуемыми последствиями.

Подтверждением актуальности проблемы безопасности является принятие в 1992 г. закона РФ «О безопасности», в котором под безопасностью понимается защищенность жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Следовательно, понятие безопасности имеет две стороны: внешнюю, определяющую воздействие объекта на среду, и внутреннюю, характеризующую свойство сопротивляемости объекта по отношению к действиям среды.

Безопасность – один из важнейших показателей качества и эффективности функционирования системы. Другие комплексные показатели, такие, как надёжность, стоимость могут в полной мере применяться для оценки того или иного варианта создания или функционирования системы, тогда как меры по обеспечению безопасности предпринимаются уже на этапе разработки системы. В последние годы термин «безопасность» получил широкое распространение, поскольку защита от многочисленных угроз всего населения Земли и отдельного индивидуума выходит на первое место в системе приоритетов человечества, потеснив проблемы повышения производительности труда и создания новых технологий.

Внутренняя безопасность – характеристика целостности системы, показатель ее гомеостаза. Она определяет способность системы поддерживать

свое нормальное функционирование в условиях внешних и внутренних воздействий.

Внешняя безопасность – способность системы взаимодействовать со средой без нарушения гомеостаза. Другими словами, воздействие системы на среду не приводит к необратимым изменениям или нарушениям важнейших параметров, характеризующих состояние среды, принятое за допустимое.

Живучесть способность СЭС (подсистемы, объекта, элемента) в целом сохранять свойства, необходимые для выполнения требуемых функций, при наличии воздействий, не предусмотренных условиями нормальной эксплуатации. Это способность её полностью или в ограниченном объеме выполнять свои функции при нарушении работоспособного состояния и восстанавливать их полностью или частично за допустимый (нормированный) период времени. Для объектов электроэнергетики – это способность полностью или в ограниченном (договорном или нормированном) объёме выполнять свои функции при воздействиях, не предусмотренных условиями нормальной эксплуатации, а при нарушении работоспособного состояния – восстанавливать его за технологически допустимый период времени. Живучесть определяется также активной реакцией системы на возмущения за счёт рационально организованной структуры, выбором целесообразных режимов функционирования, не допускающих каскадного развития аварий, ограничивая глубину (тяжесть) отказа с возможностью массового нарушения режима электроснабжения потребителей.

Свойство управляемости заключается в приспособленности СЭС к предупреждению и обнаружению выхода значений параметров за допустимую область и возврату их в эту область средствами управления (см. рис. в разделе 3.3) за конечный промежуток времени. Управляемость обеспечивает возможность эффективного управления режимом объекта энергетики, максимально возможную безотказность и восстанавливаемость его, что предполагает наличие достаточных ресурсов и технических средств для осуществления соответствующего управления.

Если при одном и том же внешнем воздействии (или при внутренних отказах элементов) управление системой возможно в вариантах (α, β, …, γ), то показатель эффективности системы определяется значениями функционала R, соответствующими вариантам управления $R_\alpha, R_\beta, \ldots, R_\gamma$. Тогда аналогично (4.10) определяется величина $\Delta R_{\text{у}}^{\alpha\beta}$, представляющая сравнительную оценку вариантов управления α и β:

$$\Delta R_{\text{у}}^{\alpha\beta} = R_\alpha - R_\beta \, . \qquad (4.11)$$

Для получения абсолютной оценки качества управления необходима информация об идеальном его варианте, при котором эффективность максимальна, но этот вариант (также, как и его показатели) в общем случае остаётся неизвестным.

Помеха – воздействие, искажающее сигнал, несущий полезную информацию и вызывающее нежелательное искажающее воздействие на электроустановку или на результаты измерений. Тогда помехозащищённость – способность ослаблять действие случайных или несанкционированных помех за счёт дополнительных средств защиты объекта для выполнения им своих функций в пределах технологических регламентов.

Если значение показателя эффективности R соответствует функционированию системы в условиях помех с заданными характеристиками $R_{\text{п}}^{*}$, а R^{0} относится к работе системы без помех, показатель помехозащищённости определяется аналогично (4.10) и показывает, насколько изменяется эффективность системы под влиянием помех с заданными параметрами

$$\Delta R_{\text{п}}^{0} = R^{0} - R_{\text{п}}^{*} . \qquad (4.12)$$

Устойчиво способность – свойство объекта энергетики непрерывно сохранять устойчивость в течение некоторого времени до выхода значений параметров за допустимую область без повреждения объекта. В теории устойчивость – характеристикой того, что стабильно и стремится сохранить своё равновесное состояние во времени. Устойчивость электрической системы – способность сохранять состояние равновесия в период нормального режима работы, при его возмущениях и в аварийных условиях, возвращаясь в исходный режим после снятия возмущений или режим близкий к нему, допустимый по условиям эксплуатации ЭЭС, если возмущающее воздействие не снято.

Экономичность – совокупность экономических характеристик объекта энергетики, его технологии, эксплуатации и организационно-технических структур, обеспечивающих экономическую целесообразность использования данного объекта в данных условиях. Научно обоснованный минимум суммарных инвестиционных и эксплуатационных расходов энергосистемы или её элементов (электростанций, электрических сетей и др.), включая ущерб от нарушений электроснабжения, представляют экономический критерий надежности. Экономическая эффективность повышения надежности электроснабжения потребителей определяется разностью изменения суммарного ущерба от отказов (или изменения режимов) в системе затрат на осуществление мероприятий по повышению надежности.

Среди множества свойств энергообъектов и влияния их на надёжность выделяются внешние (входные), внутренние и производные от них [33].

Внешние представляют собой:

- ресурсоёмкость, влияющую на надёжность через затраты ресурсов на её обеспечение;
- ресурсозависимость, характеризующую влияние ресурса (первичного энергоносителя) на создание, функционирование, развитие и ликвидацию (утилизацию) объекта энергетики, особенно в условиях хозяйственной, политической или другого вида нестабильности;
- ресурсообеспеченность, обеспечивающую гарантии поставки ресурса в условиях природных, техногенных, социально-экономических возмущений.

К свойству ресурсообеспеченности относится также обеспечение нормальных и аварийных режимов функционирования системы генерирующими мощностями, трудовыми и финансовыми ресурсами.

К основным внутренним свойствам объектов энергетики относятся: производительность, маневренность, инерционность, адаптивность, управляемость, надёжность, наблюдаемость, избыточность и ряд других.

В качестве выходного свойства объекта энергетики выступает технико-экономический ущерб как от внезапных и (или) плановых нарушений электроснабжения, так и от управления режимами генерации и потребления.

Вместе с тем, ещё в [37] наряду с надёжностью уже рассматривались вопросы живучести систем энергетики, получившие развитие в [39]. В этих работах отмечалось, что в ЭЭС возрастает цена отдельных аварий и повышается её уязвимость в целом. Оценка живучести в значительной степени определяется стойкостью элементов (объектов) ЭЭС к внешним воздействиям и возможностями их восстановления.

Для обеспечения возможности управления структурой современные ЭЭС (СЭС) должны обладать свойством гибкости, которое рассматривается как способность с необходимой скоростью изменять свою структуру для обеспечения нормального развития, а также функционирования при возможных возмущениях [36] и при оптимизации режимов функционирования. Прогнозируемое увеличение доли РГ и ВИЭ показывает необходимость учёта гибкости в заранее недостаточно определённых условиях выдачи мощности. При этом системы РГ, включая ВИЭ и накопители энергии, могут выступать как поставщики услуг гибкости.

Один из источников гибкости в СЭС – управление спросом [50, 54]. Это механизм изменения потребления электроэнергии конечными потребителями относительно их нормального профиля нагрузки в ответ на ценовые сигналы ЭЭС или прямые команды СО. Такими сигналами могут быть изменение цен на электроэнергию во времени; стимулирующие выплаты, предусмотренные для снижения потребления в периоды высоких цен опто-

вого рынка; обеспечении динамического регулирования генерации на базе систем РГ и ВИЭ в моменты, когда системная надёжность находится под угрозой. Управление спросом наряду с традиционной, распределённой и возобновляемой генерацией, а также накопителями энергии способно оказывать услуги по регулированию и восстановлению частоты, обеспечивая системную гибкость.

Усиление негативного влияния чрезвычайных ситуаций природного, техногенного, экономического и политического характера потребовали активизации исследований, связанных с обеспечением энергетической безопасности [12, 71]. Таким образом, сложилось пространство свойств ЭЭС, непосредственно связанных с надёжностью.

Создание, развитие и эксплуатация интеллектуальных ЭЭС с активно-адаптивной сетью (ИЭС ААС) сопровождается массовым внедрением цифровых технологий, обеспечивающих функционирование большого количества датчиков сбора, обработки и информационного обмена по вертикальным и горизонтальным уровням ЭЭС, связанного с режимами сети, состоянием основного и вспомогательного оборудования. ИЭС ААС характеризуются наличием интеллектуальных систем оценки текущей и прогнозирования будущей ситуации, быстродействующих автоматических и автоматизированных исполнительных органов управления элементами системы в реальном масштабе времени.

4.4. Проблема кибербезопасности

На данном этапе развития ЭЭС новые компьютерные технологии контроля, управления, измерений и передачи данных, используемые для мониторинга режимов и управления ими увеличивают их уязвимость при кибератаках извне как на отдельные элементы ЭЭС, так и на единую национальную электрическую сеть (ЕНЭС), и на ЕЭС в целом [56]. Внедрение новых технологий в этой связи должно производиться с учётом требований защиты информации и самой информационной системы от неблагоприятных внешних воздействий. Поэтому в ИЭС ААС наряду с традиционными проблемами повышения эффективности производства, преобразования, передачи и распределения электроэнергии, их надёжности, безопасности и живучести возникают задачи обеспечения их кибербезопасности. Решение этих задач в ЭЭС требует дополнения и расширения свойства «надёжность» понятиями «уязвимость», «стойкость», «достоверность» и др., что необходимо для выявления и оценки механизмов воздействия дестабилизирующих факторов на объекты электроэнергетики. Следователь-

но, рациональное решение задач перспективного развития, оперативно-технологического управления, организации эксплуатации и технического обслуживания возможно лишь при учёте и этой относительно недавно возникшей проблемы.

Проблема эффективного и быстрого переноса достижений в одной области науки или техники в другую требует унификации понятий и терминов. Вместе с тем, терминология должна быть достаточно гибкой и, в определённом смысле, не до конца однозначной в целях дальнейшего развития возможных связей со смежными дисциплинами. Представим определения некоторых, не критикуемых в данной работе, понятий, необходимых при решении задач обеспечения эффективной работы ЭЭС, её подсистем и элементов в условиях возможных несанкционированных внешних воздействий [56].

Киберпространство – сложная среда, создаваемая совокупностью информации, информационной среды и информационного взаимодействия субъектов с использованием получаемой (передаваемой) и обрабатываемой информации.

Кибербезопасность – 1) совокупность условий, при которых все составляющие киберпространства защищены от максимально возможных угроз и воздействий с нежелательными последствиями; 2) условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных и других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться нежелательными; 3) комплексное понятие, формирующееся из ряда составляющих, включающих: информационную безопасность систем управления технологическими процессами, устройств РЗиА; мероприятия по исключению социальных уязвимостей; работу с персоналом; изолированность и секретность работы КВО на данный момент; способность оборудования к самовосстановлению и адаптации в информационных пространствах стандарта МЭК-61850; 4) система технологий, процессов, методов, мер реагирования и смягчения последствий, предназначенных для защиты сетей, программ и данных от атак, повреждения или несанкционированного доступа для обеспечения конфиденциальности и целостности.

По отношению к системам энергетики, понятия «киберопасность», «кибербезопасность» предлагается рассматривать как сочетание условий, определяющих ситуацию и характеризующих взаимодействие объекта (системы энергетики) с окружающей средой, которое считается опасным или

безопасным. Выводы о наличии опасности делаются с учётом множества этих взаимосвязей.

Событие информационной безопасности – появление определенного состояния системы, сервиса или сети, указывающее на возможное возникновение ранее неизвестной ситуации, которая может иметь отношение к безопасности объекта энергетики или отказу защит.

Инцидент информационной безопасности – следствие одного или нескольких нежелательных (неожиданных) событий, имеющих значительную вероятность создания угрозы информационной безопасности. Основными инцидентами информационной безопасности считаются:

- отказы технических средств управления, контроля и передачи данных;
- неконтролируемые изменения параметров режима и структуры электрических, технологических и информационных систем;
- утрата услуг, оборудования или устройств;
- несоблюдение политики и (или) рекомендаций по информационной безопасности;
- системные сбои и (или) перегрузки;
- сбои программного обеспечения;
- ошибки пользователей;
- нарушение физических мер защиты;
- нарушение правил доступа.

Угроза – потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации.

Киберугроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность причинения вреда киберпространству.

Термин «уязвимость» связан с понятием кибербезопасности, так как уязвимости систем и объектов позволяют осуществлять кибератаки [17]. Уязвимости – результат недостатков проектирования информационных и операционных систем, ошибок программирования, ненадёжных паролей, воздействия вирусов и вредоносных программ. Наличие уязвимостей позволяет внедряться в коды приложений и выполнять непредусмотренные или несанкционированные действия, нарушая их работу, целостность систем или данных.

Уязвимость – 1) слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами; 2) потенциальная или реально существующая возможность реализации киберугрозы; 3) характеристика элемента проекта, внедрения или функционирования важнейшего объекта инфраструктуры, делающего его восприимчивым к разрушению или выходу из строя в результате угрозы;

4) ошибка или недостаток в разработке системы, реализации или эксплуатации и управлении, которые могут быть использованы для нарушения безопасности.

Программное обеспечение и средства обработки информации уязвимы по отношению к внедрению вредоносной программы, такой как компьютерные вирусы, сетевые «черви», «троянские кони» и логические бомбы. Например, гонка за производительностью обернулась для микропроцессорных устройств РЗиА технологическими, алгоритмическими и архитектурными усложнениями. Сложная архитектура и множество алгоритмов всегда потенциально уязвимы, так как спрогнозировать и протестировать все вероятные последовательности действий, приводящие к утечке или эскалации привилегий и другим нелегитимным действиям, практически невозможно. Наличие уязвимостей на микропроцессорном уровне нельзя не признавать и игнорировать, но не стоит и переоценивать. Взвешенный анализ рисков и качественная организация эшелонированной защиты – действенная стратегия обеспечения безопасности применительно к любым уязвимостям.

Мера (степень) уязвимости – вероятность нанесения ущерба элементу, объекту или системе.

Оценка уязвимости – 1) проверка наличия слабых мест, которые могут быть использованы угрозами; 2) выявление «слабости» одного (нескольких) элементов (объектов), которая может быть использована одной (несколькими) угрозами.

Информационная мишень – множество элементов информационной системы ЭЭС, принадлежащих сфере управления и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Стойкость – 1) способность элементов и ЭЭС противостоять внешним воздействиям и функционировать в штатном режиме (в докритической области) при осуществлении кибератаки; 2) способность сохранять нормальное функционирование (в расчётных или близких к ним режимах) в процессе и после воздействия дестабилизирующих факторов (кибератаки); 3) живучесть системы в докритической области функционирования, под влиянием внешних ненормативных воздействий; 4) надёжность в условиях воздействия дестабилизирующих факторов.

Критерий стойкости – время достижения системой предельного состояния при преднамеренном внешнем воздействии.

Устойчивость системы к кибератакам – система устойчива, если количество её элементов и связей между ними при преднамеренных внезапных и «сильных» информационных воздействиях на неё не испытывает резких колебаний.

Достоверность – степень соответствия сведений об объекте исследования, полученных информационными или инструментальными средствами, его объективному состоянию.

Достоверность функционирования – 1) свойство, характеризующее истинность выходного результата работы цифрового устройства, которая определяется способностью средств контроля фиксировать правильность или ошибочность его работы; 2) свойство цифрового устройства, характеризующее способность средства контроля признать выходной результат работы устройства правильным (при пропуске ошибок средствами контроля) или ошибочными (при выдаче ложных сигналов ошибок средствами контроля).

На основании изложенного очевидно, что создание, развитие, модернизация, реконструкция и даже утилизация объектов энергетики связаны с задачами наделения их определёнными свойствами, количество которых практически не ограничено. Однако реально можно говорить о том, что, например, свойство сейсмостойкости объектов энергетики может быть второстепенным для несейсмических районов и основным для регионов с повышенным уровнем опасности сейсмической деятельности. То же можно отметить и по другим свойствам (уровень безопасности АЭС, плотин разных типов и мощности ГЭС, климатические особенности регионов прокладки ЛЭП; возможности сооружения объектов распределённой генерации и возобновляемых источников энергии; технико-экономические, экологические и социальные ограничения и др.).

Различие учитываемых свойств проявляется и на разных стадиях жизненного цикла, имеющих особенности, присущие конкретному энергетическому объекту. Кроме того, в процессе эксплуатации энергетического объекта возможны «внешние» чрезвычайные ситуации и кризисы, результатом которых являются экстремальные ситуации, требующие надёжной работы систем управления и защиты. Отнесение систем и объектов энергетики к классу критически важных должно обеспечивать их максимально эффективную работу в условиях чрезвычайных ситуаций и системных кризисов.

5 ВОЗМОЖНЫЕ УЯЗВИМОСТИ И СТОЙКОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ ЭЛЕКТРИЧЕСКИХ СИСТЕМ

5.1. Вводные замечания

Понятия уязвимости и стойкости СЭС, приведённые в разделе 4 выдвигают задачи выявления уязвимостей, которые не только актуальны, но и достаточно сложны. Внедрение и развитие технологий ИЭС создаёт и постоянно увеличивает количество возможных точек уязвимости (точек доступа) для нарушения информационной безопасности объекта, практически не требуя физического контакта. Одним из направлений выявления уязвимостей является развитие методов социальной инженерии.

Исходным вектором атак является воздействие на сотрудников: их убеждают открыть почтовые вложения, ответить на вопросы по телефону, ввести учётные данные на поддельном сайте и т. п. Карантинные и изоляционные мероприятия последнего времени, потребовавшие повсеместного перехода на удалённую работу, повлияли на стандартные и устоявшиеся режимы безопасности и стабильности СЭС.

Ряд проблем анализа и минимизации количества уязвимостей связан со сложностью программного обеспечения, имеющегося и используемого энергокомпаниями. Естественно, что чем сложнее система, тем больше вероятность существования в ней потенциальных точек для осуществления кибератак. АСУ, работающие в интеллектуальных электрических системах (ИЭС), могут быть уязвимы, если используются их заводские параметры, или параметры по умолчанию, без внесения изменений, особенно в части используемых паролей, портов и точек доступа по проводным или беспроводным сетям.

Поскольку практически любая СЭС подвержена влиянию внешних воздействий, важно знать, как долго она будет в состоянии выполнять свои функции при полученных в результате этих воздействий структурных и (или) функциональных изменений нормального состояния схемы и ненормативных отклонений параметров. Это соответствует попаданию СЭС в зону форс-мажорных обстоятельств, т. е. под влияние ненормативных, непредусмотренных при проектировании, экстремальных возмущений, имеющих случайный характер.

Наличие разнородных неопределённостей при разработке и функционировании СЭС выдвигает на первый план задачу определения и оценки характеристик стойкости элементов, входящих в её состав.

При этом основной характеристикой считается время достижения СЭС предельного состояния (обеспечение питания аварийной, технологической или функциональной брони потребителей электроэнергии) после воздействия дестабилизирующих факторов. Увеличение этого времени способствует уменьшению риска развития неблагоприятных последствий и обеспечению безопасности функционирования СЭС в результате несанкционированных внешних воздействий.

5.2. Основные уязвимости и стойкость ИЭС

К наиболее часто встречающимся в СЭС уязвимостям относятся:

- неосмотрительность персонала (пароли в доступных местах);
- отсутствие контроля доступа к конфиденциальным данным;
- игнорирование систем защиты (отключение средств защиты);
- недисциплинированность (пользователи не изменяют пароли, используют один и тот же пароль доступа к различным ресурсам).

К основным факторам, определяющим уязвимость информационно-коммуникационных систем (ИКС) от средств информационного воздействия и повышающих значимость проблемы защиты обрабатываемой информации от несанкционированного доступа (НСД), относятся:

- длительный период эксплуатации, присущий информационным и сетевым ресурсам, обусловленный появлением в ИКС новых задач, средств и технологий обработки информации;
- возможность присутствия в программном обеспечении ИКС ошибок и недекларированных возможностей в случае использования программных продуктов, исполненных на закрытых исходных кодах;
- значительная удалённость узлов ИКС друг от друга и возможное взаимодействие их через сети общего пользования (Интернет), что приводит к необходимости организации защищённых компьютерных каналов связи по открытым каналам связи;
- возможность реализации НСД со стороны внешних нарушителей, которые для ИТКС являются высокопрофессиональными специалистами, поддерживаемые на государственном уровне;
- разработка у вероятного противника высокоскоростных систем получения и обработки информации на базе молекулярных компьютеров и искусственного интеллекта.

Злоумышленниками используются уязвимости, позволяющие:

- выдать себя за другого субъекта для использования полномочий последнего и формирования «своей» информации, несанкционированного доступа и санкционирования ложных обменов информацией;
- отказаться от факта формирования информации;
- сформировать утверждение о том, что получателю в определённый момент времени была послана информация, которая не посылалась или была послана в другой момент времени;
- отказаться от факта получения информации, которая на самом деле была получена или ложь по поводу времени её получения.

Наиболее часто уязвимости выявляются в системах управления, что связано со следующими факторами:

- исторически сложившейся неадекватной политикой регулирования безопасности;
- структурой сетей систем управления, в которых отсутствуют механизмы противодействия кибератакам;
- удалённым доступом к системе управления без надлежащего контроля;
- недостаточно чёткой работой механизмов системного администрирования и программного обеспечения;
- использованием недостаточно защищённой беспроводной связи;
- использованием неспециализированного канала связи для управления, контроля или использования полосы пропускания коммуникационной сети в целях, не связанных с управлением;
- недостаточно качественным применением инструментов обнаружения и оповещения об аномальной или неуместной деятельности;
- неавторизованными или несоответствующими приложениями или устройствами, подключаемыми к сетям системы управления;
- неподтверждением подлинности команд и контрольных данных;
- ненадлежащей организацией, управлением или работой инфраструктур поддержки в критических ситуациях.

Так как внешняя среда может непредсказуемо меняться, необходим мониторинг уязвимостей для выявления тех, которые могут использовать вновь появляющиеся угрозы. Уязвимости ИЭС связаны с информационно-коммуникационными сетями и включают:

- уязвимость сетевой структуры;
- уязвимость сетевых аппаратных средств;
- уязвимость сетевого периметра;
- уязвимость сетевого мониторинга;
- уязвимость коммуникаций;

- уязвимость беспроводного подключения.

Повышение кибербезопасности достигается при помощи таких мер, как закрытие уязвимости каналов доступа, внедрение адекватных процедур и процессов информационной безопасности, а также применением специальных технических решений на основе брандмауэров.

Поскольку функционирование СЭС предполагает постоянное взаимодействие входящих в её состав элементов, воздействия дестабилизирующих факторов, приведшие к отказу одних элементов, могут оказать (и в большинстве случаев оказывают) влияние на показатели работоспособности элементов, не подвергнувшихся этому воздействию непосредственно. Следовательно, отказы становятся зависимыми, что отмечалось в разделах 1, 2.

Схемы большинства СЭС – реализованы достаточно «жёсткими» структурами, что позволяет внешнему воздействию распространяться (каскадное развитие). Естественно, что при этом снижаются как показатели надежности отдельных элементов, так и всей СЭС, что может привести к останову технологического процесса потребителя или переходу его в режим частичной работоспособности [50, 54]. В соответствии с известными подходами к повышению надежности СЭС и их элементов, не предоставляется возможным продублировать все наиболее уязвимые для воздействия дестабилизирующих факторов элементы. Поэтому исследование уязвимостей СЭС и её реакций на сторонние воздействия могут существенно уменьшить и даже предотвратить риск возникновения и развития последствий возможных кибератак.

Обеспечение стойкости ИЭС – длительный трудоёмкий итерационный процесс, связанный с учётом различных типов неопределённостей. Сложность оценки показателей стойкости в том, что практически не определены критерии, характеризующие стойкость элементов и подсистем ЭЭС, а имеющаяся исходные данные для их оценки нерепрезентативны и обладают большой степенью неопределённости [3]. Для решения подобных задач требуются обширные знания в различных областях науки и техники, обусловленные необходимостью определения механизмов воздействия дестабилизирующих факторов на объекты электроэнергетики, знаний в области особенностей функционирования ЭЭС, системы электроснабжения (СЭС) потребителя и особенностей его технологического процесса производства, а также наличие модели прогнозирования реакции анализируемого объекта на воздействие, сопровождающееся протеканием физических, экономических и социальных процессов.

Естественно, что при проектировании новых элементов и подсистем ЭЭС (СЭС) возникает необходимость заложить в них такие уровни стойко-

сти, которые могли бы обеспечить их безотказное функционирование на протяжении всего жизненного цикла. Однако это может повлечь за собой негативные последствия, заключающиеся в дополнительных затратах, усложнении схем первичной и вторичной коммутации, релейной защиты и автоматики, технологического процесса потребителя, возможном ухудшении ряда других параметров. Подобная постановка задачи говорит о том, что проблема обеспечения стойкости и проблемы надёжности, безопасности и живучести имеют много общего.

5.3. Основы оценки стойкости СЭС

Стойкость элемента (объекта) энергетики к воздействию дестабилизирующих факторов (ДФ) имеет нелинейную природу порогового вида. Действие механизма поражения проявляется только после того, как уровень воздействия ДФ превысит некоторое пороговое значение. При этом защита от каждого ДФ, как правило, носит индивидуальный характер и требует соответствующих материальных затрат. Основой формирования показателя стойкости служит соотношение «воздействие – реакция на воздействие», которое представляется в двух эквивалентных формах [3]: вероятности сохранения работоспособности за время действия ДФ в расчётной ситуации – $P_{\text{ж}}$ и вероятности поражения (потери работоспособности) $P_{\text{п}} = 1 - P_{\text{ж}}$.

$$P_{\text{ж}} = \int_0^{\infty} p_{\text{р}}(s) P_{\text{ср}}(s) ds \geq \underline{P}_{\text{ж}}; \quad P_{\text{п}} = \int_0^{\infty} p_{\text{р}}(s) P_{\text{пр}}(s) ds \leq A,$$

где $p_{\text{р}}(s) = \dfrac{d(1 - P_{\text{р}}(s))}{ds}$ – плотность вероятности реализации максимального уровня воздействия ДФ s в расчётной ситуации; $P_{\text{р}}(s)$ – вероятность того, что в рассматриваемой ситуации элемент (объект, система) испытает воздействие ДФ с уровнем выше s; $P_{\text{ср}}(s)$ – вероятность сохранения работоспособности при воздействии ДФ с уровнем s; $P_{\text{пр}}(s) = 1 - P_{\text{ср}}(s)$ – вероятность потери работоспособности при воздействии ДФ с уровнем s; $\underline{P}_{\text{ж}}$ – нижняя граница допустимых значений показателя $P_{\text{ж}}$, определяемая из решения задач более высокого иерархического уровня и задаваемая в качестве критериального параметра; $A = 1 - \underline{P}_{\text{ж}}$ – верхняя граница допустимой (исходя из требований к живучести) вероятности поражения.

Увеличение основной характеристики стойкости системы – времени достижения предельного состояния – способствует уменьшению риска развития критической (чрезвычайной) ситуации и обеспечению безопасности.

Поэтому требования к стойкости включают необходимость учёта и раскрытия ряда неопределённостей, связанных с:

- малой вероятностью возникновения критических ситуаций;
- ограниченностью сведений о стратегиях противника;
- ограниченностью знаний о ДФ;
- ограниченностью информации о поражающем воздействии ДФ;
- практическим отсутствием информации о технико-экономических последствиях воздействия ДФ.

5.4. Моделирование противодействия хакерским атакам

Исследование скомпрометированных учётных данных [24] вскрыло интересные факты о популярных паролях, которые устанавливают пользователи. Анализ 15 млрд паролей, фигурировавших в тех или иных утечках информации, показал, что только 2 млрд (≈13 %) оказались уникальными. Большинство используют менее восьми символов и достаточно легко угадываются.

Агрессивные кибератаки направленные на срыв технологических операций в ЭЭС могут привести к разрушению системной инфраструктуры, травмам и гибели людей, нанести ущерб производствам промышленной и сельскохозяйственной продукции, транспорту, ЖКХ, окружающей среде, вызвать экономические и финансовые сбои. Наглядное представление возможного решения проблем, связанных с уязвимостью и стойкостью СЭС к кибератакам рассмотрим на примере игры двух лиц [55].

Допустим, что сторона A (хакер) атакует систему АСУТП электроэнергетического объекта путем заражения вирусом, причем A применяет три варианта вирусов: a_1, a_2, a_3. Сторона B организует защиту в двух вариантах: b_1, b_2.

Ход 1: сторона A выбирает один из вариантов a_1, a_2, a_3 атаки.

Ход 2: сторона B выбирает один из вариантов b_1, b_2 защиты объекта.

Ход 3 (случайный): система информационной защиты b_j уничтожает (**у**) или не уничтожает (**ну**) вирус a_i.

Если вирус a_i нейтрализован, игра окончена.

Если вирус a_i прорвался к системе АСУТП, то следует очередной ход.

Ход 4 (случайный): a_i поражает (**п**) или не поражает (**нп**) АСУТП.

Описанная ситуация (игра) представлена в виде дерева (рис. 5.1), в котором вершинам (кроме висячих) соответствуют ходы, а дугам – выбор на каждом ходу. Висячим вершинам отвечает конец игры.

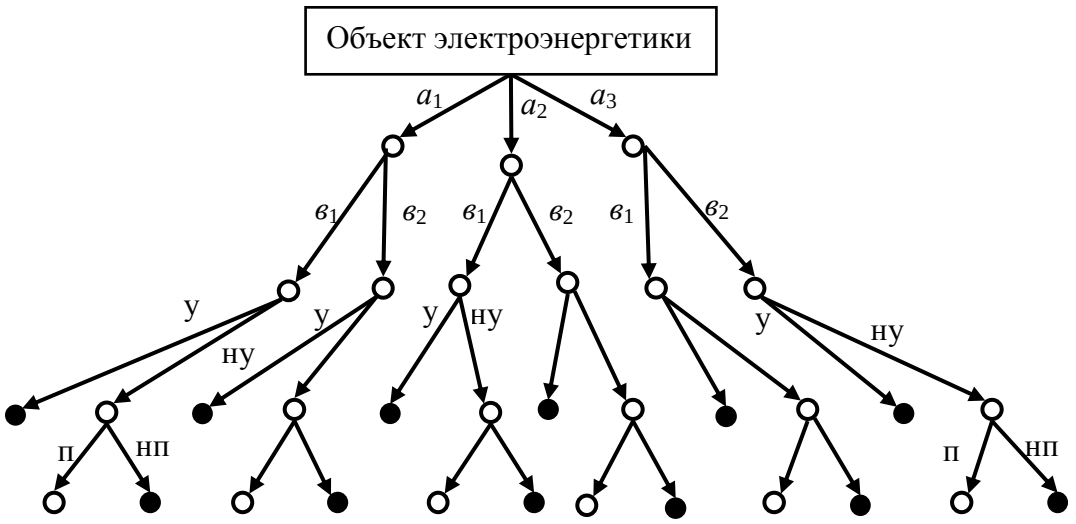


Рис. 5.1. Дерево возможных исходов хакерской атаки

Каждый путь от начальной вершины (корня) до конечной (висячей) соответствует одному из вариантов игры (партии). Количество возможных вариантов игры (партий) равно числу висячих вершин. Как видно из рис. 5.1 в рассмотренной игре 18 возможных партий. Помеченные 12 висячих вершин соответствуют благоприятным исходам игры, когда защита объекта электроэнергетики эффективна. К проблеме оценки уязвимости и стойкости СЭС относится задача проработки фундаментальных основ информационной безопасности [55]. Рассмотрим её на примере системы РГ.

Поскольку последствия несанкционированных воздействий (кибератак) на ЭЭС (СЭС) часто не могут быть вычислены в реальном времени, используются графы атак, позволяющие учитывать взаимосвязи отдельных узлов системы, оценивать параметры их защищенности, анализировать риски, прогнозировать возможные действия злоумышленников, анализировать последствия их прошлых действий, увеличивая точность возможных атакующих действий осуществленных нарушителем [80].

5.5. Графы анализа кибератак

Граф атак – граф, представляющий все возможные последовательности действий нарушителя для достижения угроз (целей). Он представляется риск-ориентированной моделью системы защиты информации (СЗИ) в виде ориентированного графа $G = (V, E)$, где вершины v_i – угрозы объектам со стороны злоумышленников, а дуги e_{ij} – их связи. Дуга e_{ij} обозначает связь угрозы v_i с угрозой v_j, вероятная реализация которой является следствием реализации угрозы v_i. Параметры угроз характеризуются:

- O_i – множеством объектов, на которые направлена угроза v_i;
- ω_i – частотой возникновения угрозы v_i;
- $p(i)$ – вероятностью реализации угрозы v_i (например, вследствие успешной реализации некоторой уязвимости);
- $d(i)$ – коэффициентом разрушения, определяющим ущерб от воздействия угрозы v_i на объект атаки;
- c_i – стоимостью средств и мер защиты от реализации угрозы v_i.

Для такой модели ставится задача: может ли информация из вершины v_i передана в v_j, то есть определить, существует ли путь, от v_i к v_j. Если существует, то v_j достижима из v_i. Наибольший интерес представляет достижимость вершины v_j из v_i на путях, длина которых не превосходят заданной или включает минимальное число вершин графа.

Достижимость вершины в графе рис. 5.2 описывается матрицей достижимости $R = \|r_{ij}\|$, $i, j = 1, 2, \ldots, n$, где n – число вершин, а её элементы: $r_{ij} = 1$, если вершина v_j достижима из v_i; $r_{ij} = 0$, в противном случае.

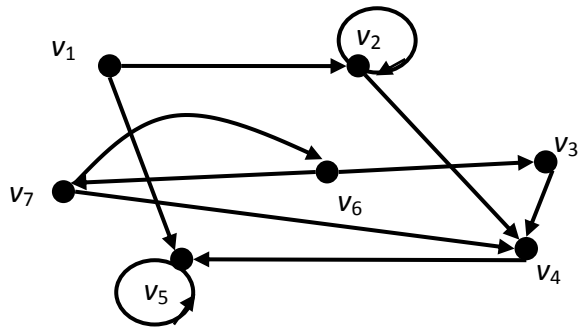


Рис. 5.2. Граф сети

Матрица достижимости строится по матрице смежности S, формируя множество маршрутов из вершин, с которой связана вершина v_i. В каждой строке v_i этой матрицы ставится 1 против того узла v_j, с которым узел v_i связан непосредственно или через другие узлы.

Контрдостижимое множество $Q\ \{v_i\}$ – множество таких вершин графа рис. 5.2, из любой вершины которого можно достичь вершину v_i.

Матрица контрдостижимости строится аналогично матрице достижимости: $Q = \|q_{ij}\|$, $i, j = 1, 2, \ldots, n$, где n – число вершин графа, а её элементы: $q_{ij} = 1$, если вершина v_i достижима из v_j; $q_{ij} = 0$, в противном случае. В каждой v_j ставится 1 против того узла v_i, с которым узел v_j связан непосредственно или через другие узлы.

Анализ графов атак сводится к определению перечня наиболее критичных уязвимостей путём выявления:

- кратчайших маршрутов от источника угроз до объекта защиты;
- маршрутов с наибольшей интенсивностью уязвимостей от источника угроз до объекта защиты;

• маршрутов с наименьшей стоимостью систем защиты информации (СЗИ) объектов.

$$S = \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{matrix} \left\| \begin{matrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{matrix} \right\|$$

$$R = \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{matrix} \left\| \begin{matrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{matrix} \right\| \qquad Q = \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{matrix} \left\| \begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{matrix} \right\|$$

Воздействия угроз и уязвимостей представлены графом (рис. 5.3).

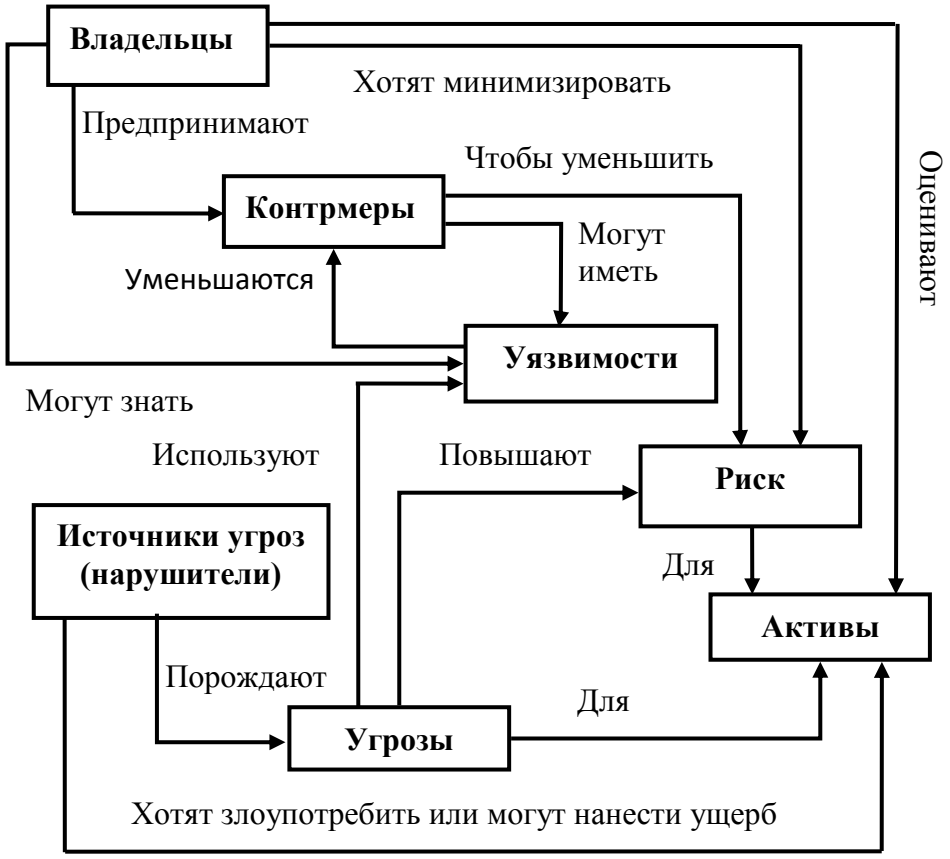


Рис. 5.3. Граф анализа СЗИ технического объекта

В соответствии с этим предлагаются:

- действия по изменению конфигурации графа атак, после чего заново выполняются пересчеты маршрутов, для проверки возможности повышения эффективности изменения уровней защищенности сети;
- пути достижения минимального критического множества атак (с минимальными последствиями (наименьшей мощностью)), что приведёт к их фактическому удалению из графа атак (из арсенала нарушителя), и приведет к невозможности достижения цели нарушителем.

Такие последовательности действий называются трассами атак.

Граф атак являясь компактным хранилищем всех возможных атак в данной модели сети, содержит все априори известные сценарии атак для достижения нарушителем угроз.

Результатом его анализа являются:

- перечень успешных атак;
- соотношение мер безопасности и уровня защищенности;
- перечень наиболее критичных уязвимостей;
- перечень мер, позволяющих предотвратить использование уязвимостей в программном обеспечении, для которого отсутствуют обновления;
- минимальное множество мер, реализация которых делает сеть максимально защищенной.

Под элементарной атакой понимают использование нарушителем уязвимости, что позволяет ему удаленно получить права администратора системы.

Общий граф атак описывает варианты реализации атакующих действий нарушителем с учётом его уровня знаний и умений, первоначальной конфигурации компьютерной сети и реализуемой в ней политики безопасности.

Выделяются следующие виды графов атак:

- граф перечисления состояний – вершинам соответствуют тройки (s, d, a), где s – источник атаки, d – цель атаки, a – элементарная атака (или использование уязвимости); дуги обозначают переходы из одного состояния в другое;
- ориентированный граф зависимостей – вершинам соответствуют результаты атак или элементарные атаки; дуги отображают зависимости между вершинами – условия, необходимые для выполнения атаки и следствие атаки.

Граф атак может строиться в режимах одного объекта-источника, конечного или всех возможных наборов объектов-источников атаки. Отдельно строится список маршрутизаторов и межсетевых экранов, для которых есть хотя бы одно состояние полного влияния на целостность объекта или системы.

Все объекты графа атак подразделяются на базовые (элементарные) и составные. Вершины графа задаются базовыми объектами. Для формирования последовательностей действий нарушителя базовые объекты графа атак связываются дугами. Составные объекты графа строятся на основе объединения дугами элементарных объектов.

К элементарным объектам общего графа атак относятся объекты, принадлежащие к типам «хост» и «атакующее действие».

Хост – любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В частном случае хост – любой компьютер, сервер, подключенный к локальной или глобальной сети. Множество объектов «хосты» включает все обнаруженные нарушителем и атакуемые им сетевые компьютеры (хосты).

Множество объектов «атакующие действия» состоит из различимых элементарных действий нарушителя.

К составным объектам относятся объекты «трасса», «угроза» и «граф».

Трасса атаки – совокупность связанных вершин графа атак (хостов и атакующих действий), первая из которых – хост, соответствующий первоначальному положению нарушителя, а последняя не имеет исходящих дуг.

Угроза атаки – множество трасс атак. Угрозы атакующих действий классифицируются как:

- основные угрозы – угрозы нарушения конфиденциальности, угрозы нарушения целостности, угрозы нарушения доступности;
- дополнительные угрозы – угрозы получения информации о сети (хосте), угрозы получения нарушителем прав локального пользователя, угрозы получения нарушителем прав администратора.

Атакующие действия делятся на:

1) действия по получению информации о сети (хосте), т. е. разведывательные действия;

2) подготовительные действия, служащие для создания условий реализации атакующих действий;

3) действия, направленные на нарушение конфиденциальности;

4) действия, направленные на нарушение целостности;

5) действия, направленные на нарушение доступности;

6) действия по получению прав локального пользователя;

7) действия, приводящие к получению прав администратора.

Для каждого хоста формируется список возможных атакующих действий разбитых в группы по классу атаки, возможности доступа и необходимого уровня знаний нарушителя. Для каждой группы формируется список конкретных атак и уязвимостей, реализующих эти атаки. Кроме отдель-

ных уязвимостей при построении графа атак используются шаблоны, которые выступают не только в качестве входной информации, но и как результат анализа безопасности, оценивая уязвимости системы и действия атакующего [80].

После формирования матрицы потенциальных атак для каждого хоста анализируемой сети выбираются возможные типы нарушителей и точки доступа, в которых они могут его получить.

Далее, для каждой выбранной модели нарушителя составляется список возможных целей. Для внутреннего пользователя это может быть месть (причинение максимального ущерба компании); для внешнего хакера – доступ к конфиденциальной информации расположенной на внутри сети; для червя – распространение инфекции по сети.

Моделью нарушителя является множество пар (тип нарушителя, цель), которые определяют ограничения по использованию атакующих действий и возможные начальные точки доступа в сеть. После этого формируются графы атак для всех выбранных моделей нарушителя.

6 ОЦЕНКА ДОСТОВЕРНОСТИ РАБОТЫ СИСТЕМ РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИКИ

6.1. Вводные замечания

По данным газеты «Энергетика и промышленность России» 31.08.2020 [https://www.eprussia.ru/news/base/2020/8877629.htm] в первом полугодии 2020 г. в ЕЭС России зафиксировано 26747 случаев срабатываний устройств РЗА. Число правильных срабатываний составило 25710 случаев или 96,12 % от их общего количества. Максимальное число случаев некорректной работы устройств РЗА в отчетном периоде было связано с непринятием или несвоевременным принятием мер по продлению срока службы или замене аппаратуры РЗА и ее вспомогательных элементов (18,66 %), ошибочными действиями персонала (10,64 %), конструктивными недостатками устройств технологической защиты или дефектами в процессе их изготовления (9,91 %). К числу главных технических причин неправильных срабатываний устройств РЗА относились дефекты или неисправности вторичных цепей РЗА (17,06 %), электромеханической аппаратуры (14,99 %), а также физический износ оборудования (9, 22 %). Отчеты сформированы на основании анализа работы более 150 тыс. устройств РЗА на объектах электроэнергетики класса напряжения 110 кВ и выше.

В [34] приведены значения интенсивностей потока ложных $\lambda_л$=0,006, излишних $\lambda_и$=0,104 и отказов срабатываний $\lambda_о$=0,012 1/год оборудования РЗА в электрической сети 20 кВ Москвы.

Приведённая статистика некорректной работы, ложных и излишних срабатываний систем РЗА выдвигает на первый план вопрос оценки достоверности их работы.

6.2. Показатели достоверности работы систем защиты

Оценками срабатывания устройств РЗА являются: правильные, неправильные, излишние и ложные срабатывания; отказы и невыясненные срабатывания.

Правильное срабатывание – состоявшееся срабатывание устройства РЗА в соответствии с назначением и при наличии требования срабатывания для ликвидации ненормальных режимов или подача для этой же цели заданных сигналов на другие устройства РЗА.

Излишнее срабатывание – срабатывание устройства РЗА при отсутствии требования срабатывания для данного устройства РЗА при наличии требования срабатывания для другого (других) устройства РЗА. К излишним срабатываниям обычно относят:

- действия устройств РЗА (при наличии требования срабатывания), приведшие к дополнительным (кроме заданных) отключениям, включениям;
- к передаче непредусмотренных (излишних) сигналов;
- к отключению трех фаз вместо одной;
- к реализации действия противоаварийной автоматики с завышенным объемом дозировки и др.

Ложное срабатывание – срабатывание при отсутствии требования срабатывания для данного и для других устройств РЗА, а также передача в этих же условиях сигнала на другое устройства РЗА, происходящее, как правило, из-за различных помех, механических воздействий на устройства РЗА, неправильных действий персонала и др.

Отказ срабатывания – отсутствие срабатывания при наличии требования срабатывания для данного устройства РЗА, а такие отсутствие в тех же условиях заданного выходного сигнала данного устройства РЗА. К отказам срабатывания относятся:

- срабатывания устройств РЗА с неполным выполнением задания (отключение или включение не всех коммутационных аппаратов;
- передача не всех заданных сигналов;
- реализация действия противоаварийной автоматики с заниженной дозировкой и др.).

Невыясненное срабатывание – срабатывание устройства РЗА, которое не может быть отнесено к категории «правильно» или «неправильно», несмотря на тщательный анализ работы устройства, условий повреждений, режимов работы системы и пр. Отнесение срабатываний РЗА к числу невыясненных производится с разрешения вышестоящей службы РЗА, которое при получении дополнительной информации может быть изменено.

В качестве дополнительных показателей могут использоваться периодичность или частота неправильных и правильных срабатываний устройств РЗА.

В качестве одного из основных показателей достоверности работы устройств РЗА принимается процент их правильной работы

$$K = \frac{n_{\text{пс}}}{n_{\text{пс}} + n_{\text{ис}} + n_{\text{лс}} + n_{\text{ос}}} 100\%,$$

где: $n_{\text{пс}}$ – число правильных срабатываний; $n_{\text{ис}}$ – число излишних срабатываний; $n_{\text{лс}}$ – число ложных срабатываний; $n_{\text{ос}}$ – число отказов срабатывания.

Общее число требований срабатывания $n_{\text{тс}}$ определяется суммой

$$n_{\text{тс}} = n_{\text{пс}} + n_{\text{ос}}.$$

Эффективность автоматизированных средств контроля, защиты и управления системами кибербезопасности ИЭС, включающих микропроцессорные устройства РЗ и ПА, информационно-измерительные комплексы, информационно-телекоммуникационные технологии, средства обработки и передачи данных, алгоритмы и программы определяется достоверностью информации, поступающей для обработки в соответствующие цифровые устройства и системы. Достоверность работы этих устройств и систем включает:

1) определение и оценку показателей достоверности их работы в различных режимах;

2) разработку методов построения структуры и разработку алгоритмов, обеспечивающих повышение показателей эффективности.

К показателям достоверности работы систем защиты относятся дефекты, неисправности, сбои, отказы, ошибки цифровых устройств. Истинным результатом работы цифрового устройства является результат, когда оно действительно работает правильно, а сигнал ошибок при этом отсутствует. Также истинным является результат, когда устройство действительно работает неправильно, о чём свидетельствует сигнал ошибки. Средства контроля могут фиксировать и другие результаты работы цифровых устройств, не отражающие его действительного состояния [83]:

1) устройство работает неправильно, но сигнал отсутствует (пропуск ошибки средствами контроля);

2) устройство работает правильно, а средство контроля сигнализирует о наличии ошибки. Все возможные состояния образуют полную группу событий.

$$P_{\text{пр}}(t) + P_{\text{нр}}(t) + P_{\text{но}}(t) + P_{\text{ло}}(t) = 1, \qquad (6.1)$$

где $P_{\text{пр}}(t)$ – вероятность правильной (безошибочной) работы устройства (системы); $P_{\text{нр}}(t)$ – вероятность неправильной работы устройства (получен сигнал ошибки); $P_{\text{но}}(t)$ – вероятность необнаруженного отказа системы,

т. е. вероятность пропуска ошибки средствами контроля (устройство работает неправильно, но сигнал ошибки отсутствует); $P_{\text{ло}}(t)$ – вероятность ложного отказа системы, т. е. вероятность принятия правильного выходного сигнала за неправильный (ложный сигнал ошибки от средств контроля); t – период оценки достоверности работы устройства.

Достоверность работы любого устройства включает понятия достоверности функционирования $D_{\text{ф}}$, достоверности правильного функционирования $D_{\text{пф}}$ и достоверности ошибочного функционирования $D_{\text{оф}}$. Следовательно, достоверность работы цифровых устройств – условная вероятность того, что средства контроля отображают истинный результат работы устройства при условии пропуска ошибки средствами контроля и наличии ложного сигнала ошибки на выходе средств контроля

$$D_{\text{ф}} = \frac{P_{\text{пр}}(t) + P_{\text{нр}}(t)}{P_{\text{пр}}(t) + P_{\text{нр}}(t) + P_{\text{но}}(t) + P_{\text{ло}}(t)}. \qquad (6.2)$$

С учётом (6.1) имеем:

$$D_{\text{ф}} = 1 - P_{\text{но}}(t) - P_{\text{ло}}(t). \qquad (6.3)$$

По (6.3) достоверность функционирования $D_{\text{ф}}$ определяется вероятностями необнаруженного отказа системы $P_{\text{но}}(t)$ и сигнала ложного отказа $P_{\text{ло}}(t)$. Достоверность правильного функционирования $D_{\text{пф}}$ – условная вероятность того, что система работает правильно при условии пропуска отказа средствами контроля:

$$D_{\text{пф}}(t) = \frac{P_{\text{пр}}(t)}{P_{\text{пр}}(t) + P_{\text{нр}}(t)}.$$

Достоверность ошибочного функционирования системы $D_{\text{оф}}(t)$ – условная вероятность неправильной работы при условии выдачи ложного сигнала ошибки средствами контроля:

$$D_{\text{оф}}(t) = \frac{P_{\text{нр}}(t)}{P_{н\text{р}}(t) + P_{\text{ло}}(t)}.$$

6.3. Достоверность функционирования канала связи

Оценка достоверности функционирования канала связи в системах телемеханики представляется следующими простейшими примерами.

1. Для обеспечения достоверности передачи сигнала системой связи необходимо, при требуемой системой ВБР P^*, оценить необходимую ВБР входящих в её состав элементов P_i. Для n последовательно соединённых элементов с равными P_i известно, что

$$P^* = \prod_{i=1}^{n} P_i \quad \text{и} \quad P_i = \sqrt[n]{P^*}.$$

Если, например, система связи состоит из трёх последовательно соединённых элементов: датчик, кодирующее устройство, исполнительный механизм и $P^* = 0{,}9$, то $P_i = \sqrt[3]{0{,}9} = 0{,}965$.

2. Оценку достоверности передаваемого сигнала в последовательной системе передачи данных из n элементов можно получить, выразив требуемую надёжность системы через интенсивности отказов элементов λ_i [25]. Для этого необходимо рассчитать такие величины λ_i^*, что

$$\sum_{i=1}^{n} \lambda_i^* \le \lambda^*, \qquad (6.4)$$

где λ_i^* – задаваемая интенсивность отказов i-го элемента; λ^* – требуемая интенсивность отказов системы.

В соответствии с ретроспективными (или экспертными) данными об интенсивностях отказов элементов λ_i, для каждого задаётся весовой коэффициент γ_i, показывающий его относительную уязвимость

$$\gamma_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i}, \quad \sum_{i=1}^{n} \gamma_i = 1. \qquad (6.5)$$

Тогда требуемая интенсивность отказов элементов системы λ_i^* вычисляется по формуле

$$\lambda_i^* = \gamma_i \lambda^*$$

и неравенство (6.4) рассматривается как равенство.

Для системы из трёх последовательно соединённых элементов статистические оценки интенсивностей отказов: $\lambda_1 = 0{,}05$, $\lambda_2 = 0{,}03$, $\lambda_3 = 0{,}01$. Требуемая ВБР за 1 год работы – $P^* = 0{,}9$.

По формуле (6.5) вычисляются весовые коэффициенты:

$$\gamma_1 = \frac{0{,}05}{0{,}05 + 0{,}03 + 0{,}01} = 0{,}555,$$

$$\gamma_2 = \frac{0{,}03}{0{,}05 + 0{,}03 + 0{,}01} = 0{,}333,$$

$$\gamma_3 = \frac{0{,}01}{0{,}05 + 0{,}03 + 0{,}01} = 0{,}111.$$

На основании экспоненциального закона распределения имеем:

$$P^*(t) = e^{-\lambda t} = P^*(1) = e^{-\lambda^* \cdot 1} = 0{,}9,$$

или $\lambda^* = 0{,}1$.

Следовательно, интенсивности отказов для элементов определяются как

$$\lambda_1^* = \gamma_1 \lambda^* = 0{,}555 \cdot 0{,}1 = 0{,}0555,$$

$$\lambda_2^* = \gamma_2 \lambda^* = 0{,}333 \cdot 0{,}1 = 0{,}0333,$$

$$\lambda_3^* = \gamma_3 \lambda^* = 0{,}111 \cdot 0{,}1 = 0{,}0111.$$

Соответствующие задаваемые значения ВБР элементов определяются в соответствии с экспоненциальным законом распределения

$$P_1^*(t) = e^{-\lambda_1^* t} = e^{-0{,}0555 \cdot 1} = 0{,}946,$$

$$P_2^*(t) = e^{-\lambda_2^* t} = e^{-0{,}0333 \cdot 1} = 0{,}967,$$

$$P_3^*(t) = e^{-\lambda_3^* t} = e^{-0{,}0111 \cdot 1} = 0{,}989.$$

Таким образом, полученные значения ВБР элементов анализируемой системы обеспечат достоверную передачу информации в течение года с вероятностью $P^* = 0{,}9$.

3. Достоверность передачи данных отражает степень соответствия принятого сообщения переданному. Ошибка объясняется появлением посторонних сигналов (помех), вызванных внешними источниками, атмосферными явлениями, или ДФ кибератак. Суждение о правильности передачи выносится по совпадению большинства из принятой информации методами «два из трех», «три из пяти» и т. д. Так, кодовая комбинация 01101 при трехразовой передаче была частично искажена помехами, поэтому приемник принял следующие комбинации: 10101, 01110, 01001. В результате проверки каждой позиции отдельно, правильной считается комбинация 01101.

4. Если передаваемый код состоит из четырёх отдельных сигналов x_1, x_2, x_3, x_4, то в пункте приёма они могут иметь двойное истолкование (рис. 6.1, *а*), где показано, каким образом эти сигналы могут быть приняты [1].

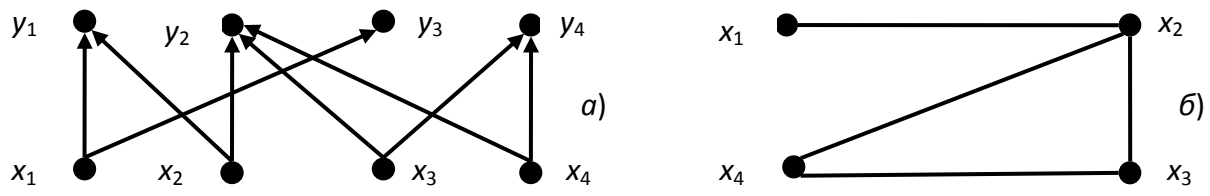


Рис. 6.1. Схема кодирования *а*)
и возможного приёма сигналов *б*)

На рис. 6.1, *б*) представлен граф, вершины которого соответствуют пересылаемым сигналам. Рёбрами соединены вершины (сигналы), которые могут быть перепутаны. Задача отыскания кода, состоящего из однобуквенных сигналов, который исключал бы неправильное понимание, сводится к отысканию в графе максимального внутренне устойчивого множества $\alpha(G)$ (рис. 6.1, *б*). Тогда имеем $\alpha(G) = 2$ и, например, $S = \{x_1, x_3\}$.

То есть, сигналы x_1 и x_3 перепутать нельзя.

5. На вход системы подаются два сигнала x_1 и x_2 [54], которые на выходе принимаются как y_1 и y_2. По условиям работы 40% времени передаётся сигнал x_1 и 60% – x_2. Вероятности гипотез передачи сигналов x_1 и x_2 составляют: $P(H1) = 0{,}4$ и $P(H2) = 0{,}6$. Вероятность безошибочной передачи сигнала x_1 как y_1 – $P(y_1 \mid x_1) = 0{,}75$. Вероятность того, что входной сигнал x_1 будет ошибочно принят как y_2 – $P(y_2 \mid x_1) = 0{,}25$. Аналогично, вероятности того, что сигнал, переданный как x_2 будет принят, как y_2 и y_1 равны $P(x_2 \mid y_2) = 0{,}90$ и $P(x_2 \mid y_1) = 0{,}10$.

При таких условиях могут наблюдаться следующие ситуации:

Выходной сигнал	y_1	y_2	y_1	y_2
Входной сигнал	x_1	x_2	x_2	x_1

Тогда возникают следующие вопросы:

а) получен выходной сигнал y_1 и какова вероятность того, что исходный сигнал x_1?

б) получен выходной сигнал y_2 и какова вероятность того, что исходный сигнал x_2?

На основании теоремы гипотез (теорема Байеса) условная вероятность того, что исходный сигнал действительно x_1:

$$P(H1 \mid y_1) = \frac{P(H1)P(y_1 \mid H1)}{P(H1)P(y_1 \mid H1) + P(H2)P(y_1 \mid H2)} = 0{,}833.$$

Условная вероятность того, что получен сигнал y_2 при условии, что исходный сигнал x_2 равна:

$$P(H2 \mid y_2) = \frac{P(H2)P(y_2 \mid H2)}{P(H2)P(y_2 \mid H2) + P(H1)P(y_2 \mid H1)} = 0{,}844.$$

Следовательно, достоверность правильного функционирования системы при передаче сигнала x_1 – $D_{\text{пф}}x_1 = 0{,}833$, а x_2 – $D_{\text{пф}}x_2 = 0{,}844$.

6. Наблюдение за работой выключателя, находящегося в двух состояниях s_1 (отключён) и s_2 (включён) производится с помощью двух датчиков. 30% времени выключатель находится в состоянии s_1 и 70 % – в состоянии s_2. Датчик № 1 передаёт ошибочные сведения в 2 % всех случаев, а № 2 – в 8 %. В какой-то момент от датчика № 1 пришла информация, что выключатель находится в состоянии s_1, а от датчика № 2 – в состоянии s_2.

Естественно верить тому сообщению, для которого больше вероятность того, что оно соответствует истине. В соответствии с состояниями выключателя s_1 и s_2 вероятности гипотез их состояния $P(H1) = 0{,}3$ и $P(H2) = 0{,}7$. Вероятности ошибочной передачи информации датчиками № 1 и № 2: $q_1 = 0{,}02$ и $q_2 = 0{,}08$, а её безошибочной передачи: $p_1 = 0{,}98$ и $p_2 = 0{,}92$. Условные вероятности полученной информации о состоянии *s* выключателя (событие *A*) определяются как

$$P(A \mid H1) = p_1 q_2 = 0{,}0784; \;\; P(A \mid H2) = p_2 q_1 = 0{,}0184.$$

Применяя теорему Байеса, найдём вероятности истинных состояний выключателя – s_1 и s_2:

$$P(H1 \mid A) = \frac{P(H1)P(A \mid H1)}{P(H1)P(A \mid H1) + P(H2)P(A \mid H2)} = 0{,}646,$$

$$P(H2 \mid A) = \frac{P(H2)P(A \mid H2)}{P(H2)P(A \mid H2) + P(H1)P(A \mid H1)} = 0{,}354.$$

Здесь $P(H2 \mid A) = 1 - P(H1 \mid A)$. Поэтому из двух переданных сообщений более достоверным следует считать сообщение, полученное от датчика № 1.

Отметим, что рассмотренные и другие анализируемые показатели существенно зависят от технических характеристик средств контроля и контролируемых ими параметров. Но они служат лишь ориентировочными критериями, по которым проводится выбор средств контроля на этапах проектирования и (или) модернизации существующих систем ИЭС с оценкой эффективности их работы.

7 ВЕРОЯТНОСТИ КРИТИЧЕСКИХ И КАТАСТРОФИЧЕСКИХ СИТУАЦИЙ В СИСТЕМАХ ЭНЕРГЕТИКИ И ЭЛЕКТРОСНАБЖЕНИЯ

7.1. Вводные замечания

Проблема обеспечения безопасности человека и потенциально опасных объектов была и остаётся весьма актуальной. Она перешла в научную категорию в связи с выявлением серьёзности последствий редких событий, которые возникают с вероятностью «почти ноль». В связи с социальными изменениями в обществе, развитием техники и технологии число зон появления редчайших событий постоянно увеличивается. Расходы, связанные с их ликвидацией год от года возрастают. Прошлое всегда кажется более стабильным и менее опасным, чем оно было в действительности, однако это должно настораживать, так как ни одно действительно редкое событие не повторяет предыдущее, поскольку не происходит дважды. Повторение гарантировано, если только существует заверение «больше никогда!».

В России с начала 90-х годов XX века сохраняется влияние чрезвычайных ситуаций природного и техногенного характера на энерго- и электроснабжение потребителей. По причинам постоянного усложнения структуры, режимов работы и эксплуатации ЭЭС и СЭС увеличивается их уязвимость. При этом погрешность любых статистических моделей оценки малых вероятностей резко увеличивается, так как в соответствии с законами симметрии крайне невероятное событие – эквивалент отсутствия крайне вероятного события. Крайне невероятное событие с серьёзными последствиями означает, что оно:

1) аномально, так как ничто в прошлом его не предвещало;

2) сопровождается катастрофическими (технологическими, экономическими, социальными, экологическими и др.) последствиями;

3) воспринимается как предсказуемое после анализа случившегося.

В этой связи роль маловероятных событий с существенными технико-экономическими, социальными и экологическими последствиями постоянно растёт.

В связи с возможными катастрофическими последствиями отказов и происшествий в работе сложных технических систем (СТС), в том числе

ЭЭС и СЭС, проблема оценки надёжности их функционирования как на стадии проектирования и выбора основных технических решений, так и в период эксплуатации, является одной из приоритетных при исследовании проблем обеспечения безопасности населения и окружающей среды. Задача существенно усложняется для уникальных СТС ввиду отсутствия или ограниченности статистических данных по надёжности таких систем в реальных условиях эксплуатации и неизбежных неопределённостях в оценках их поведения при возникновении редких проектных и «запроектных» ситуаций, связанных с отказами оборудования, ошибками персонала, различными внешними воздействиями, обусловленными неполнотой знаний о реальных условиях эксплуатации.

Безопасность в большинстве случаев определяется как состояние, в котором, при наличии возникшей угрозы, уровень возможного вреда имуществу или персоналу оценивается через категорию риска, значения которого не превышают допустимой (стандартной) величины» [31]. Суть проблемы составляют количественная оценка степени опасности (риска) и его приемлемых уровней. При этом опасность рассматривается как объективно существующая возможность негативного воздействия на общество, личность, окружающую среду, в результате которого им может быть причинён ущерб – социальный, технологический, экономический, экологический. Риск здесь – характеристика потенциальной опасности, возможность реализации негативных событий (худших альтернатив), причиняющих вред.

7.2. Особенность прогнозирования экстремальных ситуаций

Оценка риска экстремальных, аварийных и катастрофических ситуаций, возникающих в системах энергетики, состоит в необходимости оценки их вероятностей. Основная сложность такой оценки заключается в малом количестве, неопределённости относительной недостоверности ретроспективной информации, что практически не позволяет получить эффективные, несмещённые и состоятельные статистические оценки показателей надёжности, безопасности, живучести. Угроза, стихийных бедствий, природных и техногенных катастроф, терроризма, кибератак, разного рода конфликтов и других достаточно редких событий, превратились в системную закономерность конца XX начала XXI века [54]. Это обусловлено современным технологическим укладом при котором создаются новые технические, экономические, социальные, политические и другие искусственные системы, которые из-за своей сложности могут быть более уязвимыми по отношению к

разного рода случайным и преднамеренным возмущениям и, соответственно, менее стойкими, менее надёжными, менее безопасными.

Существующие методы долгосрочного прогнозирования позволяют приближённо оценить возможность появления экстремальных ситуаций при функционировании СТС, хотя, как показывает практика, происходят они достаточно редко. Обобщённая теоретическая кривая надёжности прогнозов R и соответствующая кривая риска возможных при этом ущербов в зависимости от исследуемого показателя П (внешние условия, длительность эксплуатации, режимы, нагрузка и т. п.) соответствуют [86] и приведены на рис. 7.1.

На основании рис. 7.1 очевидно, что в пределах нормальных (стабильных, устойчивых) значений анализируемого показателя

$$\Pi_{min} + \Delta_1 \leq \Pi \leq \Pi_{max} - \Delta_2$$

за счёт относительно большого количества однородных данных (аналогий) статистика даёт приемлемые результаты, обеспечивающие надёжность прогнозов и стабильность значений возможных последствий (ущерба).

В диапазонах близких к экстремальным

$$\Pi_{min} \leq \Pi \leq \Pi_{min} + \Delta_1 \text{ и } \Pi_{max} - \Delta_2 \leq \Pi \leq \Pi_{max}$$

надёжность прогнозов резко уменьшается.

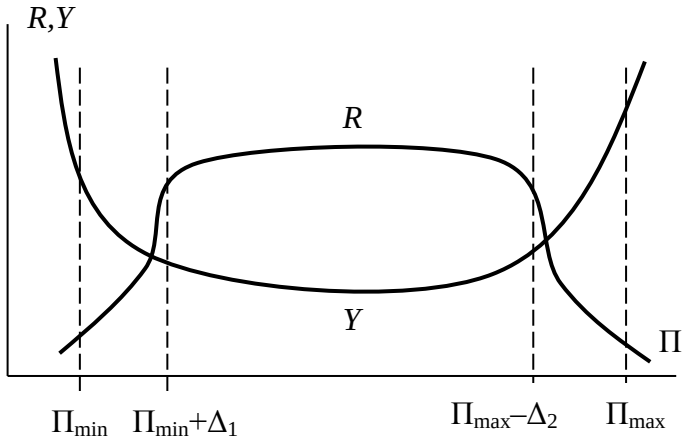


Рис. 7.1. Распределение надёжности прогноза R и риска возможного ущерба Y по показателю П

Так, например, нормальное функционирование каскада ГЭС периодически нарушается событиями двух видов: экстремальным маловодьем и экстремальными паводками. Один из возможных способов повышения надёжности прогнозов – уменьшение интервалов

$$\Pi_{min} + \Delta_1 \text{ и } \Pi_{max} - \Delta_2,$$

но дополнительную информацию при этом получить ещё более сложно и надёжность прогнозов вряд ли существенно повысится.

7.3. Постановка задачи

Экстремальные (катастрофические) события связаны с редкими выбросами случайного процесса, по которым не существует достоверной статистики. Время наступления импульса и его амплитуда являются случайными и неопределёнными величинами. Поэтому статистическая оценка параметров, связанных с экстремальными событиями неизбежно связана с более или менее обоснованной экстраполяцией на основе «осторожных» экспертных оценок.

Традиционные показатели возможности редкого (непредсказуемого) события являются неопределёнными. Значения ряда динамических величин, определяющих их, лежат на «хвостах» распределений, попадая в маловероятную (критическую) область, которая в общем случае является «размытой». Поэтому приходится переходить к методам Fuzzy Sets, ограничиваясь осторожной оценкой этой области, заведомо расширяя её за счёт неопределённости, которая неизбежно связана с более или менее обоснованной экстраполяцией на основе «осторожных» экспертных оценок.

Увеличение риска возникновения опасных ситуаций на объектах электроэнергетики, сопровождается резким возрастанием стоимости компенсации их технико-экономических и социальных последствий при одновременном снижении безопасности как эксплуатационного персонала, так и населения в целом.

После аварии на Чернобыльской АЭС (1986) предприняты экстраординарные меры безопасности во всём мире. Риски существенно и резко снизились. Есть надежда, что аварии такого масштаба будут случаться нечасто. Вопрос в том, насколько нечасто? Статистический анализ 216 аварий и происшествий, проведённый математиками Великобритании и Швейцарии зарегистрированных за всю историю ядерной энергетики показал, что аварии действительно стали значительно более редкими. Тем не менее, на основе имеющихся данных [81] предполагается, что аварии типа Фукусимы или крупнее будут происходить каждые 60–150 лет с вероятностью $p = 0{,}5$.

Причина запроектных и гипотетических аварий – цепочка событий или сценарий с попаданием системы в опасное состояние, вероятность возникновения которого не имеет никакого значения, если ущерб значим и недопустим для пользователей систем [54, 72]. Более того, в случае редких событий некорректно вводить понятие «среднее время до катастрофы». Основная задача, связана с поиском «окон уязвимости», а решение её осуществляется методами многокритериальной оценки обобщённых показате-

лей типа «эффективность», «надёжность», «безопасность», «уязвимость», «стойкость», «приемлемость», «экономичность», «эргономичность», «конкурентоспособность» и т. п. [31].

Опасность характеризуется не только вероятностью (относительной частотой) наступления кризисной (чрезвычайной) ситуации, но и тяжестью её последствий. В ранее опубликованных работах [54], показано, что численное значение риска R при нарушении нормального режима работы оборудования систем электроэнергетики может быть оценено как

$$R = pY,$$

где – p – вероятность реализации опасного события (авария, отказ, инцидент и т. п.); Y – математическое ожидание ущерба, причинённого в результате этого события.

Количественная мера риска согласуется с интуитивным представлением о нём и делит процедуру его оценки на два этапа:

1) определение вероятностей неблагоприятных исходов;

2) определение ущербов, сопровождающих эти исходы.

В решении проблемы техногенной безопасности существуют две концепции [11]: детерминистическая («абсолютной» безопасности) и вероятностная (приемлемого риска).

Первая основана на нормативном подходе и логическом анализе особенностей технологических процессов и источников возможных аварий, выработке системы обязательных мер (противоаварийная автоматика, инструкции, обучение персонала). Основным недостатком этой концепции является отсутствие количественной оценки безопасности и чувствительности к особенностям конкретного объекта, так как истинная эффективность набора обязательных мер по обеспечению безопасности остаётся неопределённой.

Вторая концепция основана на статистическом анализе степени опасности (риска), результатах имитационного моделирования для выявления возможных путей перехода аварийных ситуаций в аварии, установление приемлемых уровней риска. Для этого необходима информация о вероятностях возникновения исходных событий и готовности средств защиты, репрезентативность которой явно недостаточна. При анализе риска здесь возникают трудности, связанные с полнотой и достоверностью исходных данных, адекватностью моделей перехода объекта в аварийное состояние.

Вместе с тем, обе концепции содержат по крайней мере два вида неопределённостей [11]:

1) неопределённость в оценке достаточности принятых мер безопасности;

2) неопределённость, связанная с неперечислимостью исходных событий аварий на объектах электроэнергетики.

Эти неопределённости отражаются и в рекомендациях по оценке критических рисков. Так в [66] отмечается, что уход ключевых показателей безопасности за критический уровень считается катастрофическим, а в [82] – уровень риска возникновения опасных ситуаций, устраивающий на данный момент общество с точки зрения допустимого ущерба и затрат, является приемлемым или допустимым. Выявление и предупреждение его позволяет снизить ущерб до 10 % от ожидаемого.

7.4. Несколько примеров

В искусственно созданных (элементы и объекты электроэнергетики) технических системах время от времени возникают экстремальные ситуации с быстрым, почти мгновенным развитием событий.

При решении задач обеспечения надёжности важное место отводится статистическим методам оценивания. Но статистические оценки показателей надёжности дают приемлемые результаты только в том случае, если оцениваемое событие характеризуется массовостью и однородностью, чего в ряде рассматриваемых задач не наблюдается.

1. На морских буровых платформах вероятность расчётной аварии оценивалась как одна авария в 20 миллионов лет (p=0,00000005). Однако уже произошли аварии на 15 буровых платформах, в том числе крупнейшая в 2010 г. в Мексиканском заливе [66].

2. Расчётная вероятность, связанная с возможностью переполнения водохранилища Зейской ГЭС составляла p=0,001. Однако в 2007 г. в результате обильных дождей это событие произошло.

3. В Нидерландах [82] к началу XX в был установлен никогда не наблюдаемый уровень защитных сооружений 390 см. Однако при их строительстве высота была принята 340 см – на 12 см выше максимума, зарегистрированного за 25 лет наблюдений (1 раз в 70 лет с вероятностью p=0,014). Удешевление строительства обернулось трагедией 1953 г. Погибло около 2000 человек плюс огромные разрушения. Сейчас гидротехнические сооружения в Нидерландах строятся в расчёте на максимальный уровень 500 см (1 раз в 10 000 лет (p=0,0001)).

4. Москва, май 2005 г. Авария на подстанции «Чагино-500 кВ». Последствия: пострадали 4 млн жителей, ущерб превысил 3 млрд руб.

5. Август 2009 г. Саяно-Шушенская ГЭС. Последствия: погибли 75 человек, ущерб превысил 40 млрд руб.

6. Снежный циклон 20.11.2020 во Владивостоке привёл к беспрецедентной аварии, при которой отключёнными оказались более 180 тысяч человек. Энергетика Приморья имела нормативную степень защиты, однако было выведено из строя более 150 ЛЭП разного класса напряжения, повалено более 600 опор.

7. Предполагалось, что вероятность аварии на АЭС при нормальном законе распределения $p = 1 \cdot 10^{-7}$ год$^{-1}$, т.е. одна авария за 10 миллионов лет. Однако, как показало время, оценки должны быть другие.

Приведённые примеры – случайные события, объективная оценка вероятностей которых затруднена из-за достаточно высокой надёжности функционирования уникальных энергетических объектов и ограниченной ретроспективной информации.

7.5. Элементарная оценка вероятности редких событий

При элементарной оценке вероятности редких событий, после выявления принципиально возможных рисков, оценивается их вероятность и возможные последствия.

1. Предположим, что расчётный максимум мощности узла нагрузки электрической системы составляет P_m=500 МВт. Известно, что его превышение на ΔP=1 МВт (0,2%) возможно с вероятностью p=0,01. При этом все питающиеся от этого узла потребители отключаются от перегрузки вводов. Очевидно, в целом ряде случаев такой вероятностью (возможностью) подобного режима можно пренебречь. Однако при решении вопросов надёжности систем электроснабжения взрыво- или пожароопасного производств, систем жизнеобеспечения о максимальной пропускной способности ЛЭП вероятность p=0,01, должна быть сочтена достаточно большой и учитываться при проектировании структуры систем электроснабжения. Кстати, в США, отключение ЛЭП, с нагрузкой около 2,5 % мощности связываемых ею частей энергосистемы в 1965 г., привело к крупнейшей аварии и длительному перерыву электроснабжения в районе с населением 30 млн человек.

2. Кроме обычно рассматриваемой числовой характеристики положения случайной величины (СВ) X – математического ожидания $M(X)$ – часто возникает необходимость использования начальных моментов её распределения. Начальный момент s-го порядка СВ X определяется математическим ожиданием s-й степени этой СВ как

$$a_s(X) = \sum_{i=1}^{n} p_i x_i^s.$$

Проанализируем последствия внезапного нарушения электроснабжения разной длительности для условного производства, приводящих к его простою $t_{\text{пр}}$ со следующим распределением вероятностей

$t_{\text{пр}}$	0,1	0,5	1,0	8,0
p_i	0,5	0,3	0,15	0,05

Математическое ожидание СВ $t_{\text{пр}}$:

$$M(t_{\text{пр}i}) = \sum_{i=1}^{4} t_{\text{пр}i} p_i = 0{,}75.$$

Математическое ожидание квадрата СВ $t_{\text{пр}}^2$:

$$M(t_{\text{пр}}^2) = \sum_{i=1}^{4} t_{\text{пр}i}^2 p_i = 3{,}43.$$

Таким образом переход от $M(t_{\text{пр}})$ к $M(t_{\text{пр}}^2)$ позволяет с меньшей степенью риска учесть влияние возможного значения $t_{\text{пр}}$, которое велико и имеет малую вероятность. Если бы СВ X имела несколько больших и маловероятных значений, то переход к вычислению начальных моментов более высоких порядков $a_3(X)$, $a_4(X)$и т. д. позволил бы ещё больше усилить их роль.

3. Рассмотрим случай, когда на анализируемом объекте электроэнергетики за предполагаемое время его эксплуатации $t_{\text{эк}} = 50$ лет не должно произойти ни одного экстремального события. Тогда в соответствии с [54, 77, 78] и законом распределения Пуассона можно определить нижнюю доверительную границу времени безотказной работы $t_{\text{н}}$ для доверительной вероятности α. Если принять $\alpha = 0{,}95$, что характерно для большинства технических решений, то нижняя граница времени безотказной работы составит $t_{\text{н}} = 16{,}6$ лет. В более жёстких условиях, при $\alpha = 0{,}99$ получим $t_{\text{н}} = 10{,}8$ года.

4. Система (двухтрансформаторная подстанция) состоит из двух параллельно работающих элементов. Каждый из них отказывает в соответствии с экспоненциальным законом распределения и параметром λ. При независимых отказах вероятность отказа за время *t* составит

$$q(t) = (1 - e^{-\lambda t})^2. \qquad (7.1)$$

В соответствии с [28, 29] предположим, что с интенсивностью λ_0 возникают независимые отказы элементов, а с интенсивностью λ_1 – критические, под воздействием которых каждый элемент может отказать с вероятностью $\alpha = 1 - \beta$. При $\lambda_0 + \lambda_1 \alpha = \lambda$ свойство экспоненциальности сохраняется, но при $\alpha > 0$ надёжность системы существенно изменяется. Если $p_i(t)$, $i = 0{,}1$ – вероятность наличия i отказавших элементов в момент t, то в [28, 29] приводится система двух дифференциальных уравне-

ний Колмогорова, решение которых при начальных условиях $p_0(0) = 1$; $p_1(0) = 0$ имеет вид

$$p_0(t) = e^{-[2\lambda_0+(1-\beta^2)\lambda_1]t}$$
$$p_1(t) = 2e^{-(\lambda_0+\alpha\lambda_1)t}[1 - e^{-(\lambda_0+\alpha\beta\lambda_1)t}], \quad (7.2)$$

откуда вероятность отказа системы определяется как:

$$q(t) = 1 - p_0(t) - p_1(t). \quad (7.3)$$

В предельном случае $\lambda_0 = 0$, $\alpha = 1$, имеем: $p_0(t) = e^{-\lambda t}$; $p_1(t) = 0$, то есть, $q(t) = 1 - e^{-\lambda t}$.

Если отказы независимы, и $\lambda t = 0{,}01$, то по (1) $q(t) \approx 10^{-4}$. В действительности, по (7.3) с учётом (7.2) $q(t) \approx 10^{-2}$.

Результаты говорят сами за себя. Поэтому необходима проверка условий и возможности возникновения катастроф при потере работоспособности объекта электроэнергетики под воздействием некоторого потока поражающих факторов.

7.6. Сравнительные результаты

В идеале суммарное действие множества не поддающихся учёту факторов (внезапные отказы, приводящие к каскадному развитию аварий; выбросы вредных веществ, взрывы, пожары; количество дождей, их интенсивность; тепло- и влагообмен атмосферы с поверхностью и т. п.), согласно центральной предельной теореме теории вероятностей соответствует нормальному распределению.

Для большинства технических систем характерны нормальное (Гаусса) и экспоненциальное распределения случайных параметров «с короткими хвостами». Так, распределение максимумов мощности электрической нагрузки стабильно работающих потребителей близко к нормальному и их численные значения, как правило, не укладываются в диапазон ±3σ, с вероятностью $p = 0{,}0028$. При этом за границу 5σ их значения выходят с вероятностью $p \approx 0{,}000001$.

Именно с этой ситуацией сталкиваются и при оценке вероятностей катастрофических событий в ЭЭС. Но если использовать для обработки временных рядов нормальное распределение, то очевидно, что катастрофические ситуации будут всегда неожиданными.

В [9] на примере ОАО «МРСК Северо-Запада» показано, что фактическое распределение недоотпуска электроэнергии и экономического ущерба при отключении любого узла нагрузки противоречит нормально-

му закону и является резко ассиметричным. Среднее арифметическое и медиана отличаются более чем в 20 раз, а величина стандартного отклонения существенно превышает пороговые значения, что подтверждает выводы о неоднородности данных и необходимости детального анализа особенностей потребителя.

События «исключительной силы» последних лет убедительно показали, что расчёт необходимо вести на основании иных вероятностных закономерностей. Крупные аварии, катастрофы, эпидемии невозможно разложить на набор независимых подпроцессов. Здесь требуется их целостное (системное) исследование и описание.

В [66] рекомендуется использовать экспоненциальный или степенной закон распределения, которые относят к классу распределений с «тяжёлыми (или длинными) хвостами», так как статистика большинства крупных природных и техногенных аварий, катастроф, бедствий таких, как землетрясение, наводнение, лавина, ураган, торнадо, засуха имеют степенной закон распределения вероятностей. Это вызвано тем, что все природные и техногенные системы, склонные к крупным авариям, катастрофам, кризисам являются достаточно сложными, содержат множество взаимосвязанных и взаимозависимых элементов, подверженных воздействию многих случайных факторов с широким спектром значений параметров. Их описание не может быть сведено к простой сумме большого числа независимых слагаемых и нормальному закону распределения, так как последствия таких событий невозможно разложить на набор независимых подпроцессов. Известно, что даже малые нелинейности динамической системы существенно изменяют именно «хвосты» распределений и, следовательно, оценки вероятностей катастроф. Здесь требуется их целостное (системное) исследование и описание.

Так как маловероятные аварии и катастрофы в ограниченном периоде времени весьма возможны, пренебрежение значениями случайных величин, попадающих в «хвост» таких распределений, уже недопустимо. В качестве иллюстрации изложенного, на рис. 7.2 показан типичный вид распределений плотностей вероятностей случайной величины при нормальном, экспоненциальном и степенном законах распределения, откуда видно, что «хвост» степенного распределения существенно «тяжелее», изменяясь очень медленно.

Степенной закон распределения плотности вероятностей имеет вид:

$$P(x) \sim x^{-(1+\alpha)}, \quad \alpha \sim 1.$$

Чем меньше α, тем опаснее процесс. Для рассматриваемых задач $\alpha < 1$.

Разница между нормальным и степенным распределениями носит принципиальный характер. В терминах оценки безопасности и риска «хвост» распределения соответствует так называемым гипотетическим авариям и катастрофам, возможность которых практически равна нулю. Но так как при отсутствии статистики зона «хвоста» не определена, а достоверность аналитических расчётов вызывает «недоверие» приходится принять, что фактическое значение функций плотности распределения в этой области неизвестно.

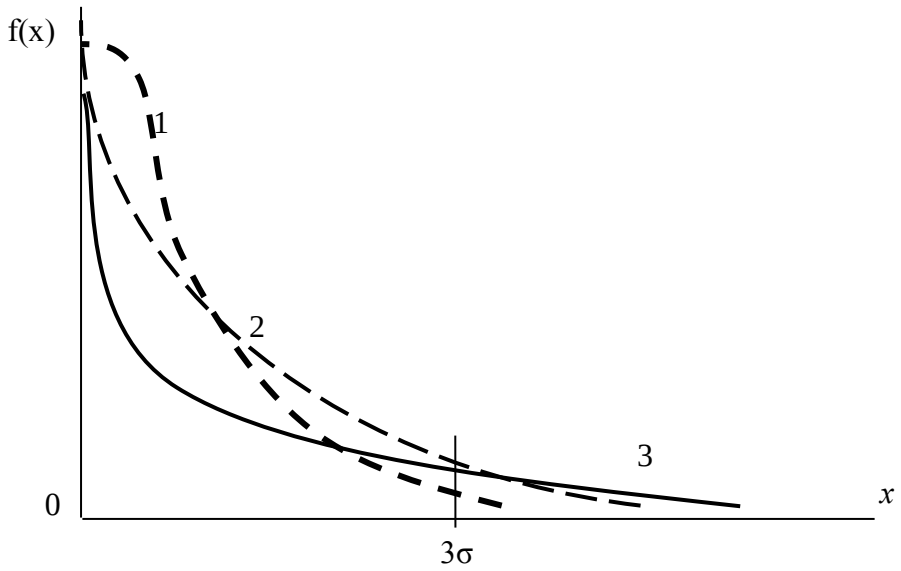


Рис. 7.2. Сравнительные плотности: нормального – 1, экспоненциального – 2, степенного – 3 законов распределения случайной величины

Наличие степенного закона распределения вероятностей в корне изменяет представления о надёжности системы, возможных последствиях экстремальных событий, риске. Статистика, описываемая степенными распределениями, отличается тем, что редкие события, приходящиеся на «хвост» распределения, происходят не настолько редко, чтобы их можно было не учитывать. Для степенного распределения вероятность катастрофических последствий может на порядок и больше превышать вероятности, вычисленные на основании экспоненциального или нормального распределения.

Для иллюстрации приведём сравнительные результаты анализа катастрофических нелинейных эффектов. В ряде публикаций [19, 31, 82] проведены расчёты вероятностей возникновения катастрофических событий, связанных с экстремальными наводнениями в соответствии со степенным и гамма-распределением вероятностей. Сравнение их представлено таблицей 7.1.

Таблица 7.1

Расчётные вероятности аномальных событий

Объект	1	2	3	4	5
Гамма-распределение	0,00005	0,00036	0,001	0,025	0,000036
Степенное	0,015	0,0039	0,059	0,009	0,012
Объект	6	7	8	9	10
Гамма-распределение	0,00011	0,0015	0,0055	0,0019	0,01
Степенное	0,098	0,006	0,026	0,0114	0,029

В работах [19, 82] отмечается, что плотности экспоненциального и гамма-распределения в анализируемой области малых вероятностей практически совпадают, но гамма-распределение обладает большей «гибкостью» и поэтому предпочтительнее. Плотности степенного и гамма-распределения хорошо совпадают в средней части и сильно различаются в области аномальных событий. Именно этим объясняется разница в их ожидаемой повторяемости. Другими словами, произошедшие катастрофические наводнения не являются почти невероятными событием, а имеют достаточно большую вероятность повториться даже при жизни нынешнего поколения. Поэтому подобные распределения необходимо учитывать при оценке надёжности и безопасности объектов и систем, имеющих жизненно важное значение.

8 ОЦЕНКА НАДЁЖНОСТИ И ЭФФЕКТИВНОСТИ СТРУКТУРНЫХ СХЕМ СИСТЕМ РАСПРЕДЕЛЁННОЙ ГЕНЕРАЦИИ

8.1. Вводные замечания

Специфическая черта систем РГ – сложность их энергетической, технологической и организационной структуры. Это позволяет, с одной стороны, решать комплекс задач обеспечения надёжного и эффективного электроснабжения потребителей, с другой – обеспечивать устойчивую работу при нарушении работоспособности отдельных ГУ и их групп. Изменения в структуре системы РГ из-за отказов отдельных ГУ и их связей приводят, как правило, лишь к снижению показателей её функционирования, так как границы между исправным и неисправным, а также работоспособным, частично работоспособным и неработоспособным состоянии ми размыты и часто условны [54]. Это связано с избыточностью структуры, наличием резерва ГУ (перекрытие зон действия), коммутационными возможностями и связями, особенностями работы устройств релейной защиты (РЗ) и противоаварийной автоматики (ПА), средств коррекции режимов (компенсации реактивной мощности и регулирования напряжения), возможных ошибок оперативного персонала. Поэтому для подобных систем не существует общепринятого понятия «отказ» [54, 76].

Поскольку системы РГ представляются структурами с несколькими перекрывающимися зонами действия, это определяет особенности их работы, которые можно оценить некоторой интегральной характеристикой – эффективностью функционирования – степенью целесообразности использования системы РГ в различных режимах. Однако вопросы, связанные с особенностями расчёта эффективности функционирования систем с перекрывающимися зонами исследованы недостаточно полно [21, 62, 68, 74–76], что обусловливает актуальность темы и необходимость практической реализации метода перекрывающихся зон.

Даже формально находясь в состоянии полной работоспособности, система РГ может и не выполнить все требуемые от неё функции. Это происходит из-за неблагоприятного стечения обстоятельств (неравномерность выдачи мощности возобновляемыми источниками энергии (ВИЭ), перегрузка при повышенном спросе потребителей, несанкционированные внешние воздействия (кибератаки)) [56].

Следует учесть, что поведение автономно работающих ГУ систем РГ существенно отличается от их поведения в составе системы. В последнем случае могут проявиться особенности построения иерархической структуры, режимов и коммутационных возможностей сети; взаимозависимость отказов отдельных элементов; взаимозависимость (очерёдность) их восстановлений, и т. п. Это приводит к необходимости учёта поведения отдельного k-го элемента x_k, определяющегося предысторией части или даже всех остальных элементов [74]:

$$x_k(t + dt) = f_k[x_k(0, t),\ x_1(0, t), \dots, x_n(0, t)]\ ,$$

где f_k – функция, определяемая конкретными особенностями системы.

Тогда, состояние системы определяется n-мерной случайной величиной

$$X(t) = [x_1(t), x_2(t), \dots, x_n(t)],$$

траектория поведения которой в интервале $(t, t + \theta)$ будет n-мерной случайной функцией

$$X(t, \theta) = [x_1(t, \theta\ ), x_2(t\theta), \dots, x_n(t\theta)].$$

Поэтому появляется необходимость в расширении понятия «надёжность» [52] и переход к показателям эффективности функционирования системы с РГ при выполнении ею определённых задач в конкретных условиях [6, 68, 74–76].

8.2. Условия работоспособности простейших структур СЭС

1. По аналогии с [45] рассмотрим простейшую (автономную) радиальную систему электроснабжения (СЭС), состоящую из условно безотказного источника I (шины бесконечной мощности), однородных потребителей m и одинаковых ЛЭП w (рис. 8.1). Вероятность отказа непосредственно m_i-го потребителя по причинам, не связанным с его электроснабжением, определим как $s = 1 - r$. Вероятность отказа ЛЭП – $q = 1 - p$.

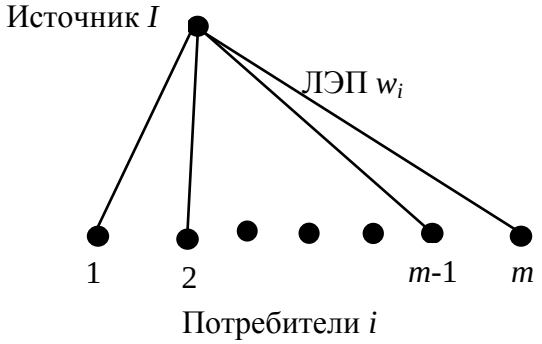


Рис. 8.1. Радиальная СЭС с источником питания

Вероятность отказа m_i-го потребителя по причинам, не связанным с его электроснабжением, определим как $s = 1 - r$. Вероятность отказа ЛЭП – $q = 1 - p$. В силу независимости отказов потребителей и ЛЭП заключаем, что вероятность связи потребителя i с источником есть $P = rp$. Вероятность противоположного события – $Q = 1 - rp$.

Здесь распределение числа потребителей, подключённых к источнику, подчиняется биномиальному закону, для которого математическое ожидание $M[m]$ и среднее квадратическое отклонение σ_m определяются как

$$M[m] = mrp; \quad \sigma_m = \sqrt{D[m]} = \sqrt{mrp(1 - rp)}\,.$$

2. С развитием ВИЭ и систем РГ возникает задача оценки условий работоспособности автономных электрических систем, состоящих из нескольких источников. Рассмотрим схему автономной ЭЭС (рис. 8.2) для которой требуется оценить надёжность обеспечения питанием ответственных потребителей, подключённых к распределительному щиту РЩ [42].

Структурная схема этой ЭЭС (без учёта выключателей) представлена графом на рис. 8.3. Потребители получают питание (работоспособность этой ЭЭС), если выполняются следующие условия нормальной работы: *a*) $П_1$ – исправны: генератор G_1, главный распределительный щит ГРЩ$_1$, кабельная линия W_1, распределительный щит РЩ; *b*) $П_2$ – исправны: G_1, ГРЩ$_1$, W_3, ГРЩ$_2$, W_2, РЩ; *c*) $П_3$ – исправны: G_2, ГРЩ$_2$, W_2, РЩ; *d*) $П_4$ – исправны: G_2, ГРЩ$_2$, W_3, ГРЩ$_1$, W_1, РЩ.

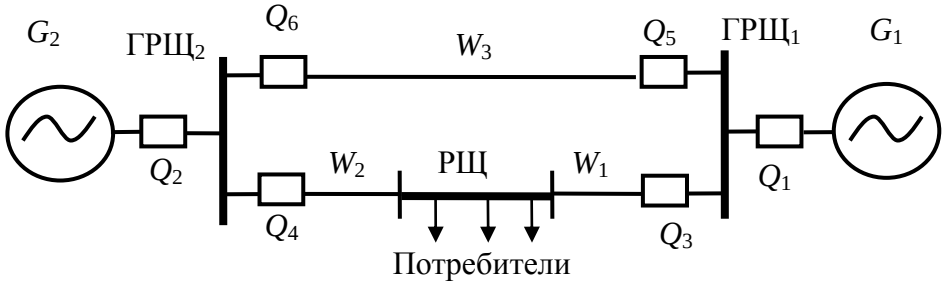


Рис. 8.2. Схема автономной ЭЭС

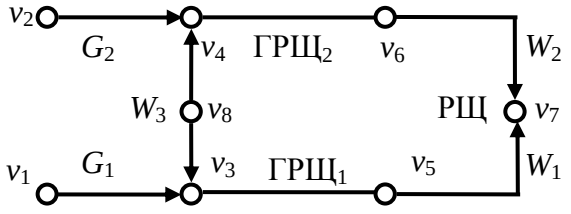


Рис. 8.3. Граф схемы рис. 2

Эти же условия в матричной форме запишутся как

$$A(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8) = \left\| \begin{matrix} \Pi_1 \\ \Pi_2 \\ \Pi_3 \\ \Pi_4 \end{matrix} \right\| = \left\| \begin{matrix} v_1 & v_3 & v_5 & v_7 & & \\ v_1 & v_3 & v_8 & v_4 & v_6 & v_7 \\ v_2 & v_4 & v_6 & v_7 & & \\ v_2 & v_4 & v_8 & v_3 & v_5 & v_7 \end{matrix} \right\|.$$

3. Развитие замкнутых сетей в системах РГ требует оценки вероятности связности сети. На рис. 8.4 представлен граф подобной системы, у которого вершины – узлы генерации, распределения или потребления электроэнергии, а параметры ЛЭП – веса рёбер, равные вероятностям их работоспособного состояния. При такой постановке интерес представляет оценка вероятности связности сети между узлами, например, *A* и *B*. В целях упрощения предполагается, что все узлы абсолютно надёжны [45].

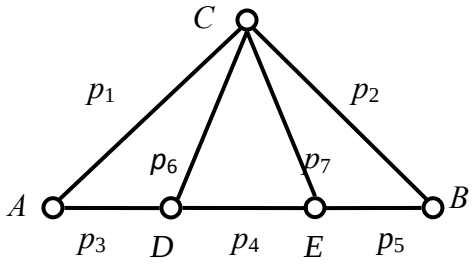


Рис. 8.4. Схема условной автономной ЭЭС

Предположим, что для связи между узлами *A* и *B* можно использовать все пути, состоящие из трёх и менее последовательно включённых рёбер. Тогда

$$\left\| \begin{matrix} \Pi_1 \\ \Pi_2 \\ \Pi_3 \\ \Pi_4 \end{matrix} \right\| \begin{matrix} AC & CB & 0 \\ AD & DE & EB \\ AD & DC & CB \\ AC & CE & EB \end{matrix} \Bigg\|.$$

Отсутствие связи узлов *A* и *B* сводится к вычислению вероятности

$$Q_{\mathrm{AB}} = (1 - p_1 p_2) \cdot (1 - p_3 p_4 p_5) \cdot (1 - p_3 p_6 p_2) \cdot (1 - p_1 p_7 p_5).$$

8.3. Системы РГ с перекрывающимися зонами действия

Поскольку любая электроэнергетическая система (ЭЭС), включая РГ, относится к классу больших систем с несколькими уровнями функционирования, обладает сложной структурой, многофункциональностью, избыточностью она не может быть представлена единичными классическими показателями надёжности. Отказы отдельных её элементов (в данном случае ГУ

и связей между ними) не приводят, как правило, к отказу системы, а только понижают эффективность её функционирования.

В простейшем случае [21] эффективность – вероятность выполнения автономной ГУ задачи по бесперебойному электроснабжению потребителей. Коэффициент эффективности E при этом дополнительно приобретает смысл вероятности того, что выполнение этой задачи не будет сорвано из-за невозможности реализации некоторых режимов (отказов). Считаем, что N_Σ – множество всех возможных режимов работы ГУ, реализуемых для обеспечения электроснабжения потребителей; N – множество реально существующих режимов. Однако возможны некоторые дополнительно допустимые режимы, образующие вместе с N множество N_0. Тогда $N \in N_0 \in N_\Sigma$ (рис. 8.5).

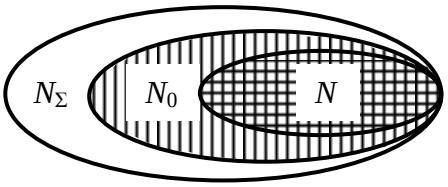


Рис.8.5. Возможное соотношение режимов ГУ

Эффективность здесь есть вероятность p того, что режим n принадлежит множеству N, то есть $E = p\{n \in N\}$.

Аналогично $E_0 = p\{n \in N_0\}$. Вероятность того, что режим работы ГУ одновременно принадлежит двум множествам N и N_0 составит

$$p\{n \in N, n \in N_0\} = p\{n \in N\},$$

так как $N \subset N_0$ (рис. 8.5).

В соответствии с теоремой умножения вероятностей получим

$$p\{n \in N, n \in N_0\} = p\{n \in N_0\} \cdot p\{n \in N | n \in N_0\}.$$

Коэффициент эффективности при этом определится как

$$E = \frac{p\{n \in N\}}{p\{n \in N_0\}} = \frac{p\{n \in N, n \in N_0\}}{p\{n \in N_0\}} = p\{n \in N | n \in N_0\}. \qquad (8.1)$$

Полученное выражение (8.1) есть вероятность того, что электроснабжение потребителей будет осуществлено практически в любом режиме работы ГУ.

Учитывая сложность получения оценок эффективности функционирования систем РГ, возникает необходимость разработки и совершенствования соответствующего математического аппарата. В общем виде эффективность системы РГ $E_{\text{сист}}(t)$ сводится к расчёту по формуле, предложенной в [76]

$$E_{\text{сист}}(t) = \sum_{k=1}^{2^n} p_{X_k}(t) E_{X_k}, \qquad (8.2)$$

где $X = (x_1, x_2, \dots, x_n)$ – состояния системы РГ; n – количество элементов системы, находящихся в двух состояниях ($x_i = 1$ – работоспособное, $x_i = 0$ – отказ); $p_{X_k}(t)$– вероятность того, что система находится в состоянии X_k в момент времени t; E_{X_k} – эффективность системы при условии, что она в состоянии X_k.

Когда n велико, то расчёт эффективности по (8.2) достаточно сложен. Поэтому рассмотрим подход, предложенный в [68, 75, 76]. Основа его заключается в том, что на некоторой территории размещено несколько объединённых в систему ГУ, обеспечивающих электроснабжение потребителей не только непосредственно присоединённых к «своей» ГУ, но и (при достаточном резерве мощности и пропускной способности сети) других, территориально близких и находящихся в зонах перекрытия смежными ГУ.

Если в системе из n элементов i-й элемент с вероятностью p_i находится в исправном состоянии, то результаты его функционирования распространяются на зону S_i. Зоны действия двух, трёх и т. д. элементов могут пересекаться, образуя области $S_{i,j}, S_{i,j,k}, \dots, S_{i,j,k,\dots,n}$ с соответствующими элементами влияния. В общем случае таких зон может быть 2^n. Область действия всей системы представляется объединением всех зон действия элементов $S = \bigcup_{i=1}^{n} S_i$ [76].

Предположим, что условный энергорайон, представляющий систему РГ, состоит из четырёх ГУ (электростанций), каждая из которых обеспечивает работу потребителей электроэнергии «своей» зоны. $\Omega = \bigcup_{i=1}^{4} Z_i$. В каждой зоне выделяются области, пересекающиеся с соседними двумя или более зонами. Следовательно, образуется система с перекрывающимися зонами действия.

Часть зоны, не пересекающаяся с другими, обозначается как S_i, ($i = \overline{1,4}$), а области пересечения – $S_{i,j}$, $S_{i,j,k}$ ($i = j = k = \overline{1,4}$). Все выделенные зоны определяют район S действия ГУ исследуемой системы РГ (рис. 8.6).

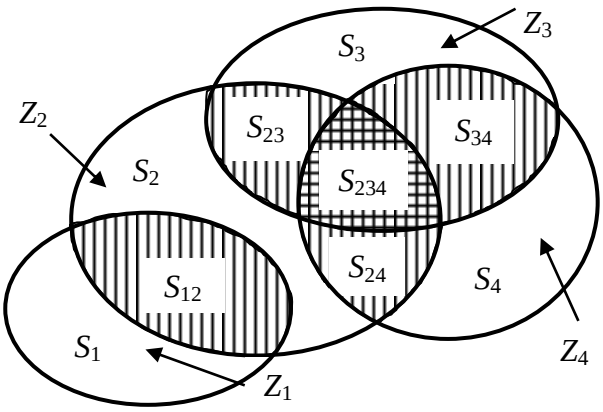


Рис. 8.6. Зоны работы ГУ системы РГ

Коэффициенты эффективности выделенных областей обозначим через E с соответствующими индексами. Если, например, отказывает ГУ, основные потребители которой расположены в зоне Z_2, коэффициенты эффективности областей, покрываемых этой зоной, изменятся.

Вместо E_{12}, E_{23}, E_{24}, E_{234} получаем E_1, E_3, E_4, E_{34}. Естественно, что в каждой практической задаче коэффициенты эффективности для областей пересечения определяются индивидуально.

Подобное разбиение энергорайона функционирования системы РГ, состоящего из n ГУ может существенно сократить число выделенных областей относительно величины 2^n, то есть, упрощает вычисление E системы РГ. Расчёт его сводится к вычислению коэффициентов эффективности каждой из областей и их взвешенному суммированию с учётом:

- мощности, выдаваемой генерирующими агрегатами;
- коммутационных возможностей схем электроснабжения;
- режимных сетевых параметров;
- состава, особенностей работы и уставок систем РЗ и ПА;
- потребляемой мощности и технологических особенностей потребителей, находящихся в соответствующей зоне;
- других показателей, характеризующих переход системы РГ в режим ограничений.

Составляющая коэффициента эффективности e_i в результирующей сумме для области S_i без перекрытия S с другими зонами определяется как

$$e_i = S_i E_i p_i,$$

где p_i – вероятность отказа ГУ в области Z_i с нарушением электроснабжения потребителей в зоне S_i.

Составляющая для области перекрытия зон Z_i и Z_j равна

$$e_{ij} = S_{ij}\left(E_{ij} p_i p_j + E_i p_i q_j + E_j q_i p_j\right).$$

Составляющая, образованная перекрытием трёх зон Z_i, Z_j и Z_k

$$e_{ijk} = S_{ijk}(E_{ijk} p_i p_j p_k + E_{ij} p_i p_j q_k + E_{ik} p_i q_j p_k + E_{jk} q_i p_j p_k + \\ + E_i p_i q_j q_k + E_j q_i p_j q_k + E_k q_i q_j p_k)\ .$$

Оценка коэффициентов эффективности каждой из областей при наличии большего числа зон производится аналогично.

Отметим, что коэффициент эффективности определяет средний уровень качества функционирования системы, обусловленный надёжностью входящих в неё элементов. Он может быть безразмерным (вероятность выполнения требований потребителя) и иметь размерность (величина генерируемой мощности, объём электропотребления, прибыль, ущерб и др.) При отказе ГУ в зоне Z_i потери (ущерб) определяются последствиями от нару-

шения электроснабжения потребителей расположенных в области S_i. В остальных областях перекрытия с другими зонами будет (или может) наблюдаться некоторое снижение эффективности функционирования потребителей (снижение производительности, изменение параметров технологического процесса и (или) качества выпускаемой продукции), находящихся в этих зонах [54]. Ущерб Y_i в зоне S_i оценивается по выражению

$$Y_i = S_i E_i + S_{ij}\left(E_{ij} - E_i\right) + S_{ijk}\left(E_{ijk} - E_i\right) + \cdots .$$

Приближённая оценка величины суммарного ущерба Y_Σ с учётом вероятности p_i отказов ГУ в различных зонах систем РГ составит

$$Y_\Sigma = \sum_{i=1}^{n} p_i Y_i.$$

8.4. Оценка эффективности систем РГ с перекрывающимися зонами действия

Система РГ, состоит из двух одинаковых ГУ, каждая из которых может работать в двух режимах: x_1 и x_2.

Если возможны оба режима $x_1 \cup x_2$, то эффективность системы РГ – $E = S_2$.

Если $\bar{x}_1 \cup x_2$ или $x_1 \cup \bar{x}_2$, то $E = S_1$, (при $\bar{x}_i$, $i = 1{,}2$ режим не выполняется) и $S_1 < S_2$.

Если $\bar{x}_1 \cup \bar{x}_2$, то $E = 0$ [62].

Состояние системы РГ характеризуется вектором с компонентами

$$\left\{x_1^{(1)} x_2^{(1)} x_1^{(2)} x_2^{(2)}\right\}, \qquad (8.3)$$

где верхние индексы – номер ГУ, нижние – соответствующий режим.

Каждая компонента (3) принимает два значения: x_i^j – режим электроснабжения потребителей осуществляется; $\bar{x}_i^j$ – режим неосуществим.

Когда $E = 0$ имеем:

$$\left\{\bar{x}_1^{(1)} \bar{x}_2^{(1)} \bar{x}_1^{(2)} \bar{x}_2^{(2)}\right\}.$$

Когда $E = S_1$ могут быть два режима: *а*) произвольная, но только одна компонента вектора (8.3) принимает значение x_i^j, а остальные – $\bar{x}_i^j$; *б*) состояние системы РГ характеризуется одним из векторов

$$\left\{\bar{x}_1^{(1)} x_2^{(1)} \bar{x}_1^{(2)} x_2^{(2)}\right\}, \quad \left\{x_1^{(1)} \bar{x}_2^{(1)} x_1^{(2)} \bar{x}_2^{(2)}\right\}. \qquad (8.4)$$

Когда $E = S_2$ также возможны два режима: *а*) не менее трёх компонент вектора (3) принимают значение x_i^j (одна ГУ полностью исправна); *б*) состояние системы РГ характеризуется одним из векторов

$$\left\{\bar{x}_1^{(1)} x_2^{(1)} x_1^{(2)} \bar{x}_2^{(2)}\right\}, \quad \left\{x_1^{(1)} \bar{x}_2^{(1)} \bar{x}_1^{(2)} x_2^{(2)}\right\}. \tag{8.5}$$

Сравнение выражений (8.4) и (8.5) показывает, что в обоих случаях система состоит из двух ГУ, работающих в одном из возможных режимов; число невозможных режимов также одинаково, но показатели эффективности различны. Отличие определяется характером выполнения условий по электроснабжению потребителей. В соответствии с (8.4) за счёт двух частично работоспособных ГУ система РГ оказывается полностью работоспособной.

Оценка эффективности систем РГ должна, прежде всего, основываться на фундаментальных знаниях об их конструктивных, технологических и организационных особенностях, принципах работы основных и элементов управления, систем релейной защиты и автоматики, входящих в их состав [20, 23]. Порядок даже предварительной оценки эффективности систем РГ определяется следующей последовательностью:

- получение информации об основных схемно-режимных характеристиках и технико-экономических показателях работы системы РГ;
- выяснение возможных задач функционирования системы РГ;
- выяснение условий работы системы РГ параллельно с ЭЭС, автономно и в комбинированном режиме;
- оценка ожидаемой частоты повторений задач и режимов функционирования системы РГ;
- составление функциональной схемы системы;
- разбиение системы РГ на отдельные элементы (зоны, области);
- выбор приемлемой для данной системы РГ количественной меры качества функционирования;
- вычисление показателей надёжности элементов, характеризующих вероятность состояния каждого элемента в различные моменты времени;
- на основании вероятностей состояний отдельных элементов вычисление вероятностей средних (при необходимости допустимых и (или) предельных) состояний системы РГ;
- оценка показателей эффективности возможных состояний системы РГ.

Если для каждого состояния системы РГ возможно оценить «мгновенное» значение её эффективности функционирования (выходного эффекта), то коэффициент эффективности определяется как среднее значение выходного эффекта по всем состояниям системы [76].

8.5. Примеры ориентировочной оценки эффективности систем РГ

Непересекающиеся зоны действия ГУ в системе РГ

Каждая из двух одинаковых ГУ в системе РГ обеспечивает электроснабжение потребителей в своей зоне с вероятностью $p = 0{,}9$. Коэффициент готовности каждой ГУ – $K_г = 0{,}95$. (рис. 8.7).

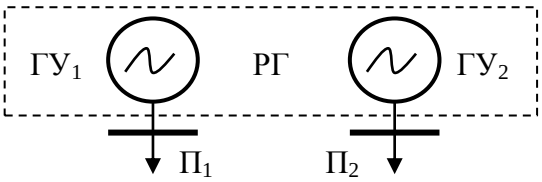


Рис. 8.7. Непересекающиеся зоны действия ГУ в системе РГ

Для того, чтобы система была работоспособна не только в любой требуемый момент времени, но и была бы в состоянии безотказно проработать в течение требуемого интервала $t + t_0$ вводится коэффициент интервальной готовности

$$K_г^*(t, t + t_0).$$

В общем случае $p^*(t) \neq p$, поскольку p – вероятность безотказной работы, начиная с состояния полной работоспособности, а $p^*(t)$ – вероятность безотказной работы, начиная с одного из возможных промежуточных состояний. В целях упрощения допустим, что $t \to \infty$ и $p^*(t) = p = 0{,}9$. Тогда

$$K_г^*(t) = K_г p^*(t).$$

При отказе одной из ГУ система РГ распадается на две независимые подсистемы, каждая из которых может обеспечить лишь половину нагрузки потребителей. Коэффициент эффективности одной ГУ при этом определяется как

$$e_{гу}(t) = 0{,}5 K_г p = 0{,}5 \cdot 0{,}95 \cdot 0{,}9 = 0{,}4275.$$

Следовательно, рассматриваемая система РГ обеспечивает коэффициент эффективности равный $E_\Sigma = 2e_{гу} = 0{,}855$.

Точечная оценка эффективности функционирования системы РГ в случае простейших ГУ.

Система электроснабжения (РГ) состоит их двух одинаковых электростанций (ГУ): *Sa* и *Sb*, обеспечивающих питание потребителей максимально потребляемой мощностью $P_\Sigma = 36$ МВт. Станция *Sa* работает в режиме выдачи мощности в пределах от $P = 0$ до $P = 22$ МВт, а станция *Sb* – от $P = 14$ до $P = 36$ МВт. Зоны выдачи мощности этими станциями показаны на рис. 8.8.

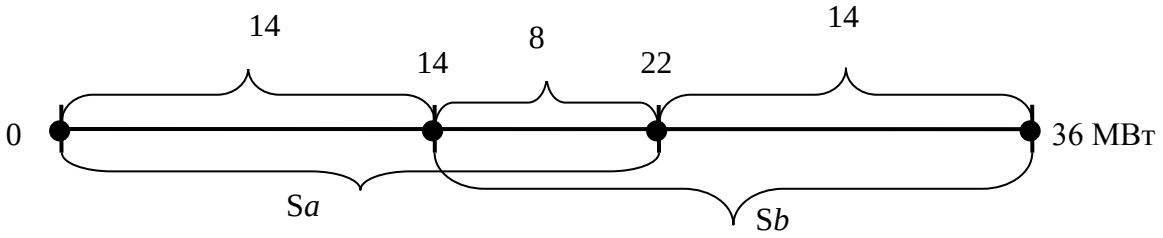


Рис. 8.8. Зоны выдачи мощности ГУ

Требуется найти вероятность обеспечения появляющейся в любой момент времени нагрузки потребителей в диапазоне $0 \le P \le 36$ МВт, если надёжность обеспечения необходимой мощностью этими станциями в этот момент: $R_a = R_b = 0{,}95$. При этом вероятность надёжного электроснабжения потребителей, находящихся в зоне действия каждой из ГУ – $R_1 = R_2 = 0{,}9$, а в зоне одновременного действия обеих станций (в зоне перекрытия)

$$\mathcal{P} = 1 - (1 - R_1)^2 = 0{,}99.$$

Предположим, что нагрузка потребителей в данный момент времени составляет P_0 МВт. Вероятность того, что система РГ в этот момент времени будет в состоянии её обеспечить

$$\mathcal{P}_0 = R_a \cdot R_b = 0{,}95 \cdot 0{,}95 \approx 0{,}9.$$

При $P = 14$ до $P = 22$ МВт (зона перекрытия – $P_{\text{п}} = 8$ МВт) нагрузку потребителя обеспечивают обе станции, а в пределах зон (от $P = 0$ до $P = 14$ и от $P = 22$ до $P = 36$ МВт) – по одной ГУ.

Показатель эффективности E_0 состояния системы РГ при заданной нагрузке P_0 МВт определяется средневзвешенной величиной

$$E_0 = \frac{P_{S_a \cap S_b}}{P_\Sigma}\mathcal{P} + \frac{P_{S_a - (S_a \cap S_b)} + P_{S_b - (S_a \cap S_b)}}{P_\Sigma}\mathcal{P}_0 = \frac{8}{36} \cdot 0{,}99 + \frac{14 + 14}{36} \cdot 0{,}9 = 0{,}92.$$

Отметим, что «вес» здесь имеют состояния системы РГ, а не отдельные её элементы (ГУ). В одной и той же системе РГ «вес» элемента существенно зависит от того, для какого состояния он рассматривается. Если при всех работоспособных элементах произошёл отказ i-го элемента, то очевидно, что он сопровождается последствиями, отличающимися от случая, когда этот i-й элемент отказал после того, как перед этим событием произошёл отказ одного j $(i \ne j)$ или нескольких элементов этой системы. Однако для РГ во многих случаях элемент, более важный в одном состоянии системы, оказывается более важным и в другом её состоянии.

Вероятность состояния системы, когда в пределах нагрузки $0 < P_a < 22$ МВт действует одна станция Sa, а в интервале $22 < P < 36$ МВт – ни одной,

$$\mathcal{P}_a = R_a(1 - R_a) = 0{,}95 \cdot 0{,}05) \approx 0{,}05.$$

Показатель эффективности E_a состояния системы РГ при нагрузке P_a МВт определится как

$$E_a = \frac{22}{36} \cdot 0{,}9 + \frac{14}{36} \cdot 0 = 0{,}55.$$

Поскольку в условиях рассматриваемого примера состояния *Sa* и *Sa* абсолютно идентичны, в результате получаем результирующую эффективность работы анализируемой системы РГ:

$$E_\Sigma = \mathcal{P}_0 E_0 + 2\mathcal{P}_a E_a = 0{,}9 \cdot 0{,}92 + 2 \cdot 0{,}05 \cdot 0{,}55 = 0{,}883.$$

Оценка технической эффективности функционирования системы РГ на определённом интервале времени.

Система электроснабжения (РГ) состоит их двух одинаковых электростанций (ГУ).

В случае работоспособности обеих станций обеспечиваемая ими нагрузка составляет *P* МВт.

В случае отказа одной из них величина обеспечиваемой нагрузки снижается до значения 0,3*P*.

При отказе двух станций электроснабжение потребителей нарушается полностью.

Отказы ГУ – независимые события. Вероятность безотказной работы каждой ГУ подчиняется экспоненциальному закону распределения

$$p(t) = e^{-\frac{t}{T}} = e^{-\lambda t}.$$

Рассматривая системы РГ подобного типа необходимо учитывать, что ГУ не будут выдавать требуемую потребителям мощность при останове в результате профилактических работ, а также воздействии каких-либо внешних факторов (погодные условия, если в состав ГУ определяется ВИЭ). Однако в целях упрощения задачи примем, что закон распределения при этом остаётся экспоненциальным.

Если принять длительность расчётного периода $\tau = t$ равной среднему времени безотказной работы каждой ГУ $t = T = 1$ год, то вероятность безотказной работы ГУ составит

$$p = e^{-\frac{t}{T}} = e^{-1} = 0{,}368.$$

Показатели технической эффективности состояний системы РГ определяются произведением передаваемой мощности на время функционирования:

1) техническая эффективность функционирования системы РГ, когда обе станции работоспособны в течение расчётного периода τ

$$E_0 = P\tau;$$

2) техническая эффективность функционирования системы РГ, когда в момент t_i отказала одна из ГУ

$$E_i(t_i) = 0{,}3P\tau + 0{,}7Pt_i \quad t_i < \tau; \quad i = a, b;$$

3) техническая эффективность функционирования системы РГ, когда одна ГУ отказала в момент t_i, а вторая – в момент t_j

$$E_{ij}(t_i, t_j) = 0{,}3Pt_j + 0{,}7Pt_i \quad t_i < t_j < \tau, \quad i, j = a, b.$$

Результирующая оценка эффективности анализируемой системы РГ в соответствии с теорией, изложенной в [74] получена по формуле

$$E = p^2P\tau + 2p\{0{,}3P\tau(1-p) + 0{,}7P\tau[1 - p(1+\lambda\tau)]\} +$$
$$+2\{0{,}3P\tau[0{,}75 - p(1+\lambda\tau) + 0{,}25p^2(1+2\lambda\tau)] +$$
$$+0{,}7P\tau[0{,}25 - p + (0{,}75 + 0{,}5\lambda\tau)p^2]\} =$$
$$= 0{,}368^2P\tau + 2 \cdot 0{,}368\{0{,}3P\tau(1-0{,}368) + 0{,}7P\tau[1 - 0{,}368(1+1)]\} +$$
$$+2\{0{,}3P\tau[0{,}75 - 0{,}368(1+1) + 0{,}25 \cdot 0{,}368^2(1+2)] +$$
$$+0{,}7P\tau[0{,}25 - 0{,}368 + (0{,}75 + 0{,}5)0{,}368^2]\} =$$
$$= (0{,}135 + 0{,}28 + 0{,}138)P\tau = 0{,}553P\tau.$$

Анализируемая система РГ может рассматриваться как система с аддитивными показателями технической эффективности [74, 75], поскольку каждая ГУ этой системы вносит свою независимую долю c_k в общий выходной эффект. Тогда эффективность системы определится в соответствии со следующими выражениями

$$E_0 = P\tau\mathcal{P}_0 = P\tau[1 - (1-p)^2] = P\tau[1 - (1 - 0{,}368)^2] = 0{,}6P\tau;$$

$$E_i(t_i) = 0{,}3P\tau\mathcal{P}_0 + 0{,}7Pt_i(1 - e^{-\frac{t_i}{\tau}});$$

$$E_{ij}(t_i, t_j) = 0{,}3Pt_j\left(1 - e^{-\frac{t_j}{\tau}}\right) + 0{,}7Pt_i\left(1 - e^{-\frac{t_i}{\tau}}\right);$$

$$E(t) = \sum_{k=1}^{n} E_k c_k = E_0c_0 + E_i(t_i)c_i + E_{i,j}(t_{i,j})c_{i,j}, \quad \sum_{k=1}^{n} c_k = 1,$$

где c_k – коэффициент долевого участия каждой ГУ, работающей в системе РГ.

Оценка эффективности системы РГ с четырьмя ГУ

а) Две подсистемы ГУ общей системы РГ

Рассмотрим систему РГ, включающую две независимые подсистемы, каждая из 2-х ГУ, которые обеспечивают электроснабжение потребителей в каждой из двух зон двумя ГУ (рис. 8.9.).

Коэффициент готовности каждой ГУ – $K_г = 0{,}95$. Вероятность безотказной работы ГУ в своей Z_i зоне – $p = 0{,}9$.

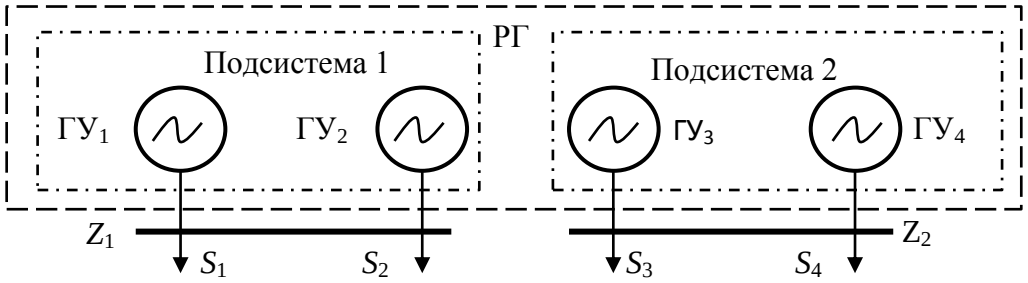


Рис. 8.9. Две независимые подсистемы общей системы РГ

Поскольку каждая из подсистем обеспечивает электроснабжение двух областей ($S_{i,i+1}$), возможны несколько ситуаций. На рис. 8.10 показано по одному варианту выбора одной отказавшей ГУ (рис. 8.10, *б*); двух ГУ в одной Z_i зоне (рис. 8.10, *в*) и по одной ГУ в разных зонах (рис. 8.10, *г*); трёх отказавших ГУ (рис. 8.10, *д*) и режим нормальной работы всех ГУ (рис. 8.10, *а*). В действительности отказ одной ГУ может произойти четырьмя способами; отказ двух ГУ – двумя способами в каждой из зон Z_i (рис. 8.10, *в*) и четырьмя способами, если отказ каждой ГУ происходит в разных Z_i и Z_j зонах (рис. 8.10, *г*); отказ трёх ГУ – двумя способами. Отметим, что в общем случае последствия отказов ГУ в каждой из рассмотренных ситуаций могут существенно отличаться, так как технологический процесс и электропотребление в областях S_i имеют свои особенности.

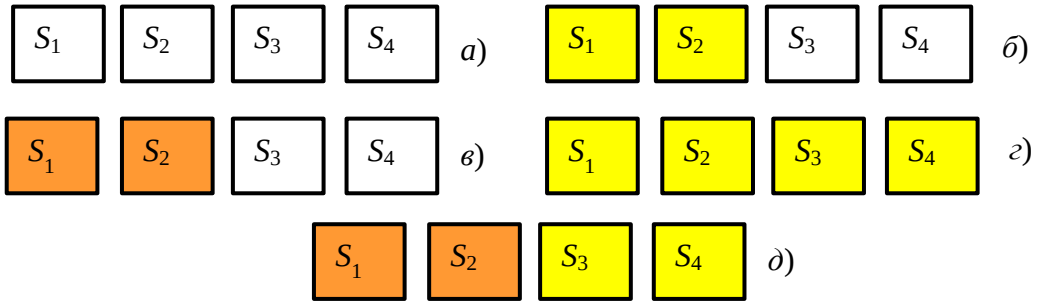


Рис. 8.10. Возможные ситуации отказов ГУ в двух подсистемах общей системы РГ
Условные обозначения: области S_i без заливки означают, что электроснабжение потребителей осуществляется от двух ГУ; светлая заливка – электроснабжение потребителей S_i осуществляется от одной ГУ; тёмная – соответствует нарушению электроснабжения потребителей

В соответствии с биномиальным распределением вероятностей отказ одной из четырёх ГУ происходит с вероятностью

$$q_{1,4} = C_4^1 q^1 p^3 = 4 \cdot 0{,}1 \cdot 0{,}9^3 = 0{,}29.$$

В любой зоне Z_i, электроснабжение которой обеспечивается двумя ГУ, их ВБР (мера эффективности) составляет

$$P = 1 - (1-p)^2 = 1 - (1-0{,}9)^2 = 0{,}99.$$

Следовательно, вероятность одновременного отказа двух любых ГУ

$$q_2 = 1 - P = 0{,}01.$$

Вероятность отказа q_{2Z_i}, двух ГУ одной Z_i зоны

$$q_{2Z_i} = 2q_2 P = 0{,}02.$$

Вероятность отказа $q_{2Z_{ij}}$, двух ГУ в разных Z_i и Z_j зонах

$$q_{2z_{ij}} = 4(qp)^2 = 4(0{,}1 \cdot 09)^2 = 0{,}03.$$

Отказ трёх ГУ происходит с вероятностью

$$q_{3,4} = C_4^3 q^3 p^1 = 4 \cdot 0{,}1^3 \cdot 0{,}9 = 0{,}036.$$

Если каждая из подсистем вносит половину «вклада» в эффективность общей системы РГ, расчёт её эффективности производится по [76], учитывая, что обе подсистемы работоспособны:

$$E = [1 - (1-p)^2] K_{\text{г}}^2 = 0{,}99 \cdot 0{,}9025 = 0{,}893.$$

Качественный анализ ситуаций, представленных на рис. 8.10 и относительно малые значения вероятностей отказов двух и трёх ГУ позволяют оценить наиболее неблагоприятные режимы функционирования исследуемой системы РГ.

б) *Качественный анализ эффективности системы РГ с четырьмя ГУ и потребителями, расположенными в четырёх зонах.*

Электроснабжение потребителей четырёх зон Z_i $(i = \overline{1,4})$ обеспечивает система РГ состоящая из четырёх однотипных ГУ. Как и ранее, ВБР каждой ГУ – $p_{\text{гу}} = 0{,}9$. При перекрытии ГУ двух зон система РГ работает в оптимальном режиме и коэффициент эффективности принят $e_2 = 0{,}99$. Структура анализируемой системы РГ представлена на рис. 8.11.

Поскольку каждая из ГУ обеспечивает электроснабжение двух зон (Z_{ij}), возможны несколько ситуаций. На рис. 8.12 показано по одному варианту выбора одной отказавшей ГУ (рис. 8.12, *б*), двух соседних ГУ (рис. 8.12, *в*), двух «противоположно» расположенных ГУ (рис. 8.12, *г*), трёх отказавших ГУ (рис. 8.12, *д*) и режим нормальной работы всех ГУ (рис. 8.12, *а*).

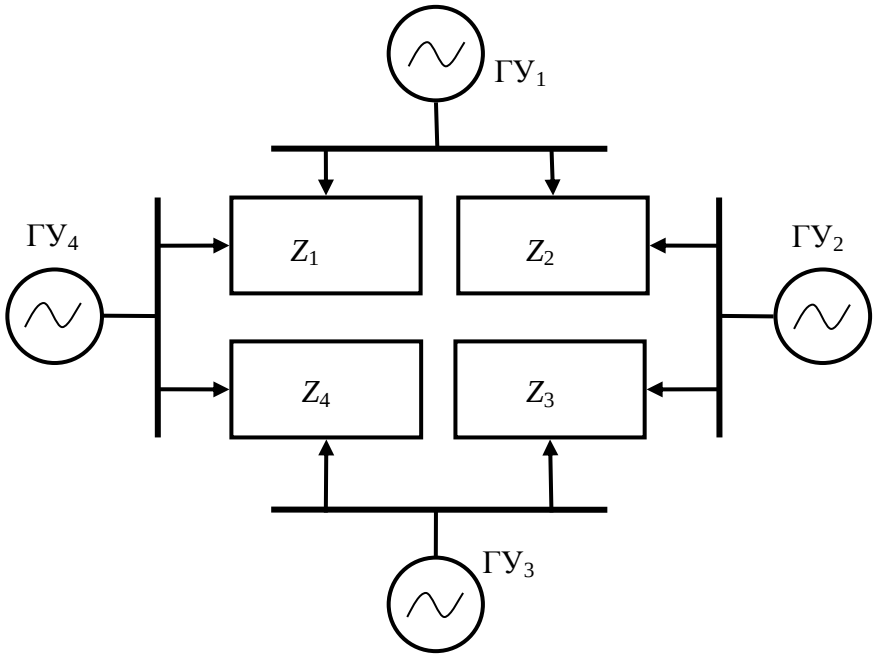


Рис. 8.11. Структура схемы электроснабжения

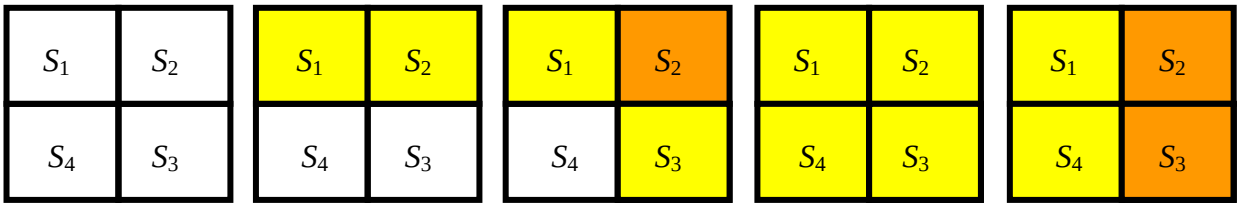


Рис. 8.12. Возможные ситуации при отказах ГУ системы РГ
Условные обозначения: области S_i без заливки обозначают,
что электроснабжение потребителей осуществляется от двух ГУ
(перекрытие зон);
светлая заливка – электроснабжение потребителей зоны осуществляется
от одной ГУ; тёмная заливка соответствует нарушению
электроснабжения потребителей в данной зоне

В действительности отказ одной ГУ может произойти четырьмя способами, отказ двух соседних ГУ и трёх ГУ тоже четырьмя, а отказ двух смежных – двумя способами.

При $p_{\text{гу}} = 0{,}9$ ВБР системы РГ составит

$$P_{\text{рг}} = 1 - q^4 = 1 - 0{,}1^4 = 0{,}9999.$$

Как и в предыдущем примере отказ одной из четырёх ГУ происходит с вероятностью

$$q_{1,4} = C_4^1 q^1 p^3 = 4 \cdot 0{,}1 \cdot 0{,}9^3 = 0{,}29.$$

Вероятность отказа $q_{2\text{сос},4}$ двух соседних ГУ определяется как

$$q_{2\text{сос},4} = 4 \cdot q^2 p^2 = 4 \cdot 0{,}1^2 \cdot 0{,}9^2 = 0{,}0324.$$

Вероятность отказа $q_{2\text{см},4}$ двух противоположно расположенных ГУ определяются аналогично

$$q_{2\text{пр},4} = 2 \cdot q^2 p^2 = 2 \cdot 0{,}1^2 \cdot 0{,}9^2 = 0{,}0162.$$

Вероятность отказа $q_{3,4}$ трёх ГУ составляет

$$q_{3,4} = C_4^3 q^3 p^1 = 4 \cdot 0{,}1^3 \cdot 0{,}9^1 = 0{,}0036.$$

Очевидно, что при одновременном отказе двух ГУ с разным структурным расположением эффективность системы РГ может существенно различаться. При отказе двух противоположно расположенных ГУ сохраняется электроснабжение всех областей S_i ($i = \overline{1,4}$), хотя и электроснабжение их осуществляется только от одного источника, а отказ двух соседних ГУ приводит к полному нарушению электроснабжения потребителей в одной из зон S_i.

Хотя одновременный отказ трёх ГУ маловероятен, происходит полное нарушение электроснабжения потребителей, расположенных в двух зонах, а потребители двух других получают питание только от одной ГУ, что говорит о максимальном снижении эффективности системы РГ.

9 ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ЗАДАЧ РИСК-МЕНЕДЖМЕНТА В СИСТЕМАХ ЭЛЕКТРОСНАБЖЕНИЯ

9.1. Вводные замечания

При решении задач риск-менеджмента в СЭС возникают три основные задачи: минимизация вероятности возникновения чрезвычайных ситуаций; стремление предотвратить или уменьшить их последствия; объединение в понятии «риск» вероятности и последствий.

1. Имеется одно или несколько приводящих к аварии в СЭС исходных событий, с тяжёлыми последствиями. В качестве риска здесь – вероятность реализации рассматриваемого события. Все усилия направляются на снижение или вероятности его возникновения.

2. Постулируется одно или несколько исходных событий, приводящих к определенным последствиям. Решается задача минимизации их. Показателем риска – последствия конкретно заданных событий.

3. На рассматриваемом объекте происходят события, приводящие к определенным последствиям. События происходят с разной вероятностью, и соответствующие им последствия отличаются по масштабу. Оценка риска здесь – сумма произведений вероятности на последствие по всем ситуациям.

Безопасность СЭС – многоплановый процесс защиты, который должен анализироваться в разных аспектах. Набор угроз постоянно меняется и, как правило, известен только частично. Меняется и окружающая среда, что влияет на природу угроз и вероятность их возникновения. Следовательно, модель безопасности должна отображать:

- состояние окружающей среды;
- уязвимости объекта СЭС;
- меры защиты;
- приемлемые для организации остаточные риски.

Модель безопасности рекомендуется представлять рядом сценариев.

1. Защитная мера S может быть эффективна для снижения рисков R, связанных с угрозой T, способной использовать уязвимость объекта V.

2. Защитная мера S может быть эффективной для снижения риска R, связанного с угрозой T, использующей группу уязвимостей объекта $\{V_1, V_2, \ldots V_n\}$.

3. Группа защитных мер $\{S_1, S_2, \ldots S_m\}$ может быть эффективна в снижении рисков $\{R_1, R_2, \ldots R_k\}$, связанных с угрозами $\{T_1, T_2, \ldots T_l\}$, использующими уязвимость объекта V. В ряде случаев требуется несколько групп G защитных мер $G\{S_1, S_2, \ldots S_m\}$ для снижения риска до приемлемого уровня и получения допустимого остаточного риска $R_{\text{ост}}$.

4. Риск R считают приемлемым, и никакие меры S_i не реализуются даже в присутствии угроз T_l и при наличии уязвимостей объекта V_n.

5. Существует уязвимость объекта V, но неизвестны угрозы T_l, которые могли бы её использовать.

Очевидно, что построение системы защиты основано на принципах обеспечения целостности и доступности технологического процесса для изменения режимов функционирования с учётом специфики автоматизированных систем управления (АСУ ТП) в ИЭС, а также систем телемеханики, релейной защиты и автоматики, коммерческого и технологического учёта электроэнергии.

9.2. Постановка задачи принятия решений при неопределённости исходной информации

Формальная математическая модель принятия решения в условиях неопределенности и наиболее простой однокритериальной задачи, формализующей понятие гарантированного по риску решения представляется [65, 66] как

$$X, Y, f(x, y) ,$$

где выбор решения (альтернативы) $x \in X$ из множества $X \in \Omega$, находится в распоряжении лица, принимающего решение (ЛПР), цель которого – обеспечить возможно большее значение критерия $f(x, y)$. При этом ЛПР должен учитывать действия помех, ошибки и другие виды неопределенностей $y \in Y$, о которых известно, что они принимают значения из множества $Y \in \Omega$.

Однако, как правило, конкретное решение неоднозначно определяет исход для ЛПР. Неизбежны помехи, возмущения, ошибки измерений, недостаток информации и другие неопределенности. В ряде случаев известны лишь границы возможных изменений параметров, а статистические характеристики либо отсутствуют, либо их получение затруднено.

Принятие решения может основывается на принципе гарантированного результата (максимина Вальда). ЛПР выбирает и использует свое решение $x \in X$. Одновременно и независимо от этого реализуется некоторая кон-

кретная неопределенность $y \in Y$. Решения x и неопределенности y образуют декартово произведение множеств $X \times Y$. На полученной паре $(x, y) \in X \times Y$ критерий $f(x, y)$ принимает конкретное значение – исход. Обычно ЛПР стремится к возможно большему исходу. Но если выбранный критерий $f_1(x, y)$ оценивает сумму ущерба, то $f(x, y) = -f_1(x, y)$, так как

$$\max_{x \in X} f(x, y) = \max_{x \in X}[-f_1 9x, y)] = -\min_{x \in X} f_1(x, y).$$

В качестве неулучшаемого решения $x^* \in X$ здесь выбирается максиминная стратегия, определяемая как

$$\max_{x \in X} \min_{y \in Y} f(x, y) = \min_{y \in Y} f(x^*, y) = f^*.$$

Смысл принципа максимина заключается в том, что если ЛПР выбрал и использовал какое-либо произвольное решение $x \in X$, то он гарантирует значение критерия $\min_{y \in Y} f(x, y) = f[x]$ при любой неопределенности $y \in Y$, что следует из неравенства

$$f[x] = \min_{y \in Y} f(x, y) \le f(x, y), \quad \forall y \in Y.$$

Естественно стремление ЛПР к наибольшей гарантии такого результата. Она реализуется на решении $x^* \in X$, так как $f(x^*, y) \ge f^*, \ \forall y \in Y$ и

$$f[x] = \min_{y \in Y} f(x, y) \le f^* = \min_{y \in Y} f_1(x^*, y), \ \forall x \in X.$$

Таким образом, применение ЛПР принципа максимина приводит к гарантированному результату (исходу) $f(x^*, y)$, который при реализации любой неопределенности $y \in Y$ не может стать меньше гарантированного значения f^* – наибольшего (максимального) из всех возможных гарантий $f[x]$.

В качестве усовершенствования максиминного критерия Сэвиджем предложен принцип минимаксного риска (минимаксного сожаления). Здесь каждой неопределенности ставится в соответствие число $\max_{x \in X} f(x, y^*)$, где y^* – фиксированная неопределенность.

Тогда ЛПР определяет для себя наибольшее значение критерия при каждой возможной неопределённости $y^* \in Y$. Далее строится разность между указанным наибольшим значением критерия $f(x, y^*)$ и значением этого же критерия при любом решении $x \in X$, то есть

$$\max_{x^* \in X} f(x^*, y^*) - f(x, y^*),$$

которая и составляет риск ЛПР.

Тем самым численно оценивается сожаление о том, что используется значение x. Естественно стремление ЛПР к выбору такого решения, при котором риск был бы возможно меньшим, гарантированным Φ^*. Тогда

$$\Phi^* = \min_{x \in X} \max_{y \in Y} \Phi(x, y) = \max_{y \in Y} \Phi(x^*, y),$$

где $\Phi(x, y) = \max_{x^* \in X} f(x^*, y) - f(x, y)$ – функция риска (сожаления) ЛПР на паре $(x, y) \in X$ x Y при использовании им альтернативы $x \in X$ и реализации неопределенности $y \in Y$.

Таким образом, с помощью функции $\Phi(x, y)$ ЛПР оценивает свой риск как разность между «самым хорошим» (максимальным) значением критерия $f(x, y)$ и значением, реализованным в действительности, который при реализации любой неопределенности $y \in Y$ не может стать больше его гарантированного результата Φ^*.

Естественно формализовать решение задачи принятия решения при неопределенности в виде пары – альтернатива и гарантия. Альтернативу $x \in X$ ЛПР выбирает, а гарантия – тот результат, который он обеспечивает себе подходящим выбором альтернативы. Использование ЛПР принципа максимина – ориентация на реализацию «самой плохой» для него неопределенности, на катастрофу. Использование принципа максиминного сожаления – это ориентация на «самую хорошую» реализацию неопределенности. Фактически, это разница между оптимизмом и пессимизмом. Обычно такая реализация маловероятна, но применение максиминного критерия оправдано, если:

- о появлении неопределенностей ничего не известно, но необходимо учесть их влияние;
- решение реализуется один раз;
- ни при каких условиях исход больший, чем f^*, недопустим.

Критерий минимаксного риска имеет смысл использовать, если:

- о неопределенности известна лишь область возможных значений, а статистические данные либо отсутствуют, либо получение их слишком дорого;
- решение реализуется один раз;
- «благоприятность исхода» ЛПР оценивает величиной потерь, вызванных своим же действием.

Одна из особенностей рынка электроэнергии состоит в изменяющейся в течение суток цене, что создает дополнительные стимулы рассмотрения риск-менеджмента как одного из основных звеньев в функционировании субъекта рыночных отношений. В условиях полного информационного обеспечения предположим, что имеются несколько вариантов n инвестирования различных энергосберегающих мероприятий при известных вероятностях p_i получения прибыли $П_i$ в каждом варианте. Тогда ожидаемое получение средней прибыли $\overline{П}_i$ для каждого из вариантов от вложения капитала K_i будет

$$\overline{П}_i = П_i p_i .$$

Вероятность наступления события может быть определена объективным или субъективным методом.

Объективный – основан на вычислении вероятности, с которой происходит данное событие

$$p_i^* \approx p_i = \frac{m}{N},$$

где m – количество зафиксированных случаев наступления желаемого события; N – общее количество случаев (измерений); при $N \to \infty$ частота события p_i^*, стремится к своей вероятности p_i.

Субъективный – на использовании субъективных критериев, которые основываются на предположениях экспертов и (или) ЛПР. При таком подходе разные ЛПР могут устанавливать разное значение p_i^* для одного и того же события и, таким образом, делать различный выбор.

При исследовании и проектировании СЭС предполагается возможность минимизации некоторой функции, определяющей условия оптимальности её функционирования при отсутствии внешних возмущений. Это означает стремление системы к состоянию равновесия, которому соответствует минимум, природа которого может быть различной. Например, возможны два варианта A и B режимов работы какого-либо объекта электроэнергетики или технологического процесса производства при необходимости изменения им режима электропотребления. Двоичный выбор зависит от значений функции полезности $U(x, a, b)$, где x – переменная, описывающая выбор; a и b – параметры, от которых этот выбор зависит. При этом предлагается [26] ввести функцию бесполезности $E(x, a, b) = -U$ и построить модель, в которой она минимизируется.

Известна стоимость осуществления этих вариантов – C_A и C_B соответственно. Параметры a и b – функции разности стоимостей $\Delta C = C_B - C_A$. Предположим, что $x < 0$ соответствует выбору варианта A, а $x > 0$ – вари-

анту *B*. Далее строятся функции $a(\Delta C)$ и $b(\Delta C)$ такие, что найдётся такое число λ, при котором возможны следующие ситуации.

Если $\Delta C > 0$ и велико по модулю, то однозначно выбирается режим *A* и, следовательно, $x < 0$.

Если $\Delta C < 0$ и велико по модулю, то однозначно выбирается режим *B* и, следовательно, $x > 0$.

Если $0 < \Delta C < \lambda$, то наиболее вероятным является выбор режима *A*, хотя возможен и выбор режима *B*.

Если $-\lambda < \Delta C < 0$, то наиболее вероятным является выбор режима *B*, хотя возможен и выбор режима *A*.

Если $\Delta C = 0$, то вероятности выбора одинаковы.

Для решения подобных задач необходима лишь функция бесполезности $E(x, a, b)$, точный вид которой несущественен, так как описание внутренней динамики процесса не требуется. Для количественного моделирования подобной ситуации требуется признание факта существования такой функции, информация о стоимости осуществления вариантов C_A и C_B и наперёд заданное число λ, являющееся, по сути, критерием выбора соответствующего варианта.

В условиях приведённого примера рис. 9.1 [26] наглядно показывает возможности двоичного выбора рассмотренных вариантов.

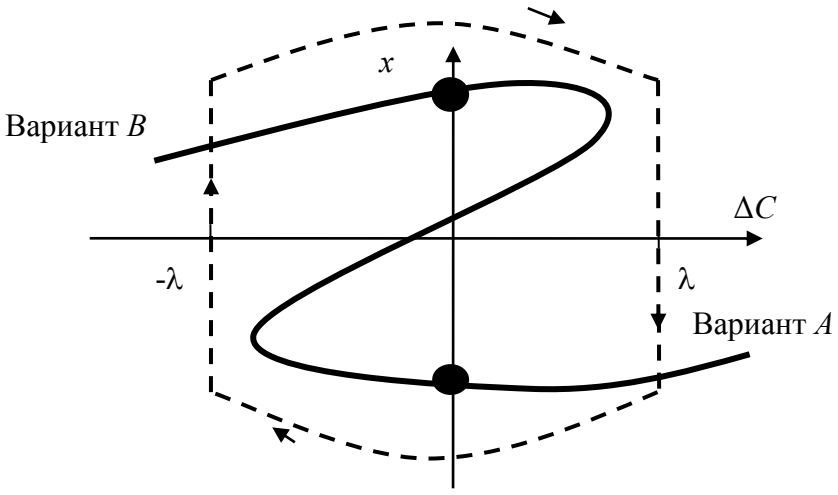


Рис. 9.1. Двоичный выбор вариантов

Неопределенность даже конкретной ситуации определяется отсутствием полной информации, случайностью, противодействием внешних и внутренних факторов. Поэтому в реальных условиях риск вложения капитала в функционирование и развитие СЭС K_i характеризуется оценкой разности максимального $П_{i\,\max}$ и минимального $П_{i\,\min}$ дохода (ущерба $У_{i\,\max}$

$У_{i\ \min}$) от данного вложения капитала. Чем больше диапазон между этими значениями

$$\Delta П = П_{i\max} - П_{i\min} \quad \text{или} \quad \Delta У = У_{i\max} - У_{i\min}$$

при равной вероятности их получения, тем выше степень риска, то есть вероятность наступления случая потерь и возможного ущерба от него.

Более полно степень риска характеризуется математическим ожиданием (средним значением) анализируемой случайной величины $M[X]$, которое представляет обобщенную количественную характеристику, но не позволяет принять решение в пользу какого-либо варианта вложения капитала и изменчивостью (рассеянием) возможного результата (дисперсией $D[X]$, среднеквадратическим отклонением $\sigma_x = \sqrt{D[X]}$), определяющим точность прогноза.

Имея такую информацию и предполагая нормальное распределение исследуемых случайных величин, можно воспользоваться известным принципом Г. Марковица. Из двух вариантов A и B наиболее предпочтительным считается вариант A, если:

$M[A] > M[B]$ и $D[A] < D[B]$;

$M[A] = M[B]$ и $D[A] < D[B]$ (непринятие риска);

$M[A] > M[B]$ и $D[A] = D[B]$.

Однако в реальных условиях принятие решений на основе этого принципа не всегда возможно. Рассмотрим пример сравнения инвестиционных проектов покупки электроэнергии у двух генерирующих компаний, которая осуществляется в соответствии с проектами A и B.

Проект A с вероятностью $p_A = 0{,}7$ обеспечивает прибыль $П_A = 16$ млн руб. и с вероятностью $(1 - p_A) = 0{,}3$ покупатель может понести потери (ущерб) $У_A = 6$ млн руб.

Для проекта B те же параметры составляют: $П_B = 11$ млн руб., обеспечивается при $p_B = 0{,}8$, а при $(1 - p_B) = 0{,}2$ возможен (ущерб) $У_B = 5$ млн руб. Математические ожидания возможной прибыли по проектам A и B составляют:

$$M[A] = p_A П_A + (1 - p_A) У_A = 0{,}7 \cdot 16 + 0{,}3 \cdot (-6) = 9{,}4 \text{ млн руб.}$$

$$M[B] = p_B П_B + (1 - p_B) У_B = 0{,}8 \cdot 11 + 0{,}2 \cdot (-5) = 7{,}8 \text{ млн руб.}$$

Средние квадратические отклонения:

$$\sigma_A = \sqrt{D[A]} = \sqrt{p_A (П_A - M[A])^2 + (1 - p_A)(У_A - M[A])^2} =$$

$$\sqrt{0{,}7(16 - 9{,}4)^2 + 0{,}3(-6 - 9{,}4)^2} = 10{,}08 \text{ млн руб.}$$

$$\sigma_B = \sqrt{D[B]} = \sqrt{p_B(П_B - M[B])^2 + (1-p_B)(У_B - M[B])^2} =$$

$$\sqrt{0{,}8(11-7{,}8)^2 + 0{,}2(-5-7{,}8)^2} = 6{,}4 \text{ млн руб.}$$

По критерию среднеквадратического отклонения более предпочтителен проект *B*. Но проект *A* обеспечивает большую среднюю прибыль.

Следовательно, если $M[A] > M[B]$ и $D[A] > D[B]$ или $M[A] < M[B]$ и $D[A] < D[B]$, то принятие решения зависит от отношения к риску лица, принимающего решение (ЛПР).

9.3. Оценка и управление риском при обеспечении надёжности СЭС

Известно, что обоснованный риск практически всегда повышает эффективность конечного результата, а оптимальная величина его C_{opt} лежит внутри некоторого диапазона предельных изменений – коридора, при котором система функционирует в устойчиво стабильном или устойчиво квазистабильном режиме. При этом система энергетики любого уровня устойчиво и надежно функционирует, если $C_{min} < C_{opt} < C_{max}$. Однако следует учитывать, что субъект либо интуитивно, либо на базе имеющейся информации устанавливает свои представления о границах C_{min} и C_{max} на момент *t* принятия конкретного решения [54, 58, 59].

В постановке задач, связанных с электроэнергетикой риск – гипотетическая возможность ущерба от нарушений нормального режима электроснабжения. Это потенциальная, численно измеримая возможность возникновения неблагоприятных ситуаций, способных дезорганизовать деятельность субъектов электроэнергетики и связанных с этим последствий, в виде снижения эффективности функционирования из-за разных видов технико-экономических потерь, социального и экологического ущерба, структурных изменений.

Поскольку не только в отечественных, но и в зарубежных исследованиях недостаточно полно формализована задача, позволяющая корректно исчислять обобщенный показатель риска, отметим, что в теоретическом плане риск $C = C(s, y)$ некоторого действия субъекта рыночных отношений есть функция от состояния среды *s*, представленного *m*-мерной случайной величиной $s \equiv (s_1, s_2, \ldots, s_m)$, и решения *y*, представленного *r*-мерной величиной $y \equiv (y_1, y_2, \ldots, y_r)$.

Решение *y* принимается на основе информации *x*, представленной *n*-мерной случайной величиной $x \equiv (x_1, x_2, \ldots, x_n)$, которая связана с состояни-

ем среды s через совместное распределение $f(s,x)$. Функция риска C совместно с распределением $f(s,x)$ представляет действие каждого субъекта для любой комбинации состояния среды s и решения y. Таким образом, практическая задача сводится к минимизации ожидаемого риска $C = C(s,y) \to \min$ путем оптимального выбора решающей функции $y(x)$.

Сложность как внешних, так и внутренних связей энергетики вряд ли позволит корректно и быстро оценить, какая из конкретных причин привела к росту риска. Конкретизация должна начинаться с информации о заинтересованных субъектах рынка, оказывающих наибольшее влияние друг на друга и на нормальное функционирование отрасли в целом. Так определяется матрица $\| C_{it} = \varphi(\Pi_i) \|$ – поле рисков, где C_{it} –риск, зависящий от показателя фактора риска Π_i, определяющегося на основании данных x в момент t. Таким образом, становится возможным анализ номенклатуры и величин рисков с учётом динамики изменения исходной информации. Но в условиях поставленных задач приходится учитывать и так называемую аксиому неповторяемости – любое поле рисков изменяется во времени, не повторяясь даже для близких ситуаций и аналогичных структур систем независимо от их идентичности. Поскольку задача оценки рисков не может быть формализована, это – основа для экспертного анализа и оценки факторов.

Для оценки величины риска используются методы анализа экспертной информации, среди которых наиболее распространенным и наглядным является оценка важности каждого фактора по шкале относительной значимости в диапазоне 1 – 10, когда можно выбирать не только целые, но и дробные числа.

Тогда коллективная оценка риска C, произведенная n экспертами, от воздействия конкретного фактора Π_j оценивается как

$$C_j = \frac{\sum_{i=1}^{n} \Pi_{ji}}{\sum_{i=1}^{n} \sum_{j=1}^{m} \Pi_{ji}}, \qquad \Pi_{ji} = \frac{P_{ji}}{\sum_{j=1}^{m} P_{ji}},$$

где P_{ji} – оценка весомости j-го фактора i-м экспертом.

Для оценки степени согласованности мнений экспертов используют методы ранговой корреляции и коэффициент конкордации, что позволяет судить об их неслучайном совпадении.

Когда в качестве количественного критерия риска используется среднее значение $\overline{X}$ и среднее квадратическое отклонение σ_X, для оценки прием-

лемости отклонения применяется коэффициент вариации $\gamma = \frac{\sigma_X}{\overline{X}}$. При этом считается, что при $\gamma \le 0{,}1$ возможные отклонения (колеблемость результатов) слабые, при $0{,}1 \le \gamma \le 0{,}25$ – умеренные, а если $\gamma \ge 0{,}25$ высокие. Отметим, что точечные оценки риска обладают свойствами транзитивности и аддитивности.

Субъективность и недостаточная точность анализа рисков в сочетании с большой долей непредсказуемых факторов ведут к тому, что управление рисками ограничивается их диагностикой, а выбор в рамках операционной деятельности энергокомпании происходит не между двумя вариантами действия, а между действием и бездействием, поэтому оценки рисков должны ложиться в основу определения факта и момента совершения действия.

Риски того или иного объекта рассматриваются как воздействие на него и его элементы непредвиденных событий, которые могут нанести определенный ущерб и препятствовать достижению целей этого объекта. Такие риски $C = \{A, P, У\}$ характеризуются тремя факторами: событиями A, оказывающими негативное воздействие на объект; вероятностью появления таких событий P; оценкой ущерба $У$, нанесенного объекту такими событиями. Достаточно подробный перечень специфических для ЭЭС и СЭС возможных рисков дан в [87].

Работоспособность объектов и систем электроэнергетики обеспечивается, если расчетный параметр X не превышает предельного значения X^*: $X \le \frac{X^*}{n}$, где n – коэффициент безопасности, задаваемый из условий работоспособности. Величины X и X^* часто рассматриваются как детерминированные, хотя они случайные. При этом мерой работоспособности P, и соответственно неработоспособности системы $Q = 1 - P$, становятся вероятности выполнения условий

$$P = p\left(X \le \frac{X^*}{n} \right); \quad Q = 1 - P = p\left(X > \frac{X^*}{n} \right).$$

Переход СЭС в состояние неработоспособности приводит к ущербу или полной потере работоспособности. Пусть c – максимально возможный ущерб при превышении расчетным показателем X величины $\frac{X^*}{n}$. Значение фактических потерь – величина, которая может принимать два значения 0 или 1 с вероятностями P и Q соответственно. Тогда средние потери или

средний риск R системы: $R = cQ$. В предположении о нормальном законе распределения X и X^* с параметрами (m, σ) и (m^*, σ^*) соответственно, величина Q определяется как

$$Q = 0{,}5 + \Phi_0\left(\frac{m - \frac{m^*}{n}}{\sqrt{\sigma^2 + \frac{\sigma^{*2}}{n^2}}}\right),$$

где $\Phi_0 = \frac{1}{\sqrt{2\pi}}\int_0^t e^{-\frac{x^2}{2}}\,dx$ – табулированная функция Лапласа [10].

Предположим, что суточный максимум нагрузки потребителя – нормально распределенная случайная величина с числовыми характеристиками $m = 80$ МВт и $\sigma = 10$ МВт. Предельно возможная нагрузка характеризуется параметрами $m^* = 100$ МВт и $\sigma^* = 2$ МВт. Превышение её приводит к штрафу за невыполнение договора в размере $c = 10^6$ руб. В целях упрощения примем $n = 1$. Определим риск потребителя заплатить штраф за превышение договорного максимума.

Вероятность превышения предельно возможной нагрузки с определением значения Φ_0 по [10] составит:

$$Q = 0{,}5 + \Phi_0\left(\frac{m - m^*}{\sqrt{\sigma^2 + \sigma^{*2}}}\right) = 0{,}5 + \Phi_0\left(\frac{80 - 100}{\sqrt{10^2 + 2^2}}\right) =$$
$$= 0{,}5 + \Phi_0(-1{,}96) = 0{,}5 - 0{,}4750 = 0{,}025.$$

Ожидаемый риск определяется средней величиной штрафа

$$R = cQ = 10^6 \cdot 0{,}025 = 24930 \text{ руб.}$$

Если расчетный параметр X и его предельное значение X^* зависят от времени, то вероятность неблагоприятного события (средний риск системы) также являются функциями времени

$$Q(t) = p\left(X(t) > \frac{X^*(t)}{n}\right); \quad R(t) = cQ(t).$$

Таким образом, средний риск может быть получен как произведение потерь при наступлении неблагоприятного события на вероятность этого события.

Реальное множество возможных состояний любой системы энергетики $E=\{S_j\},\ j=1,2,...,m$ можно разбить на два непересекающихся подмножества $E=E_+\cup E_-$, где E_+ – множество благоприятных и E_- – неблагоприятных состояний. $p_j(t)$ – вероятность пребывания системы в состоянии S_j. Допустим, что возможны переходы только из E_+ в E_-. Переход системы из E_+ в $S_j\in E_-$ сопровождается потерями (ущербом) c_j.

Рассмотрим схему подстанции, где переход в неблагоприятное состояние S_j может быть вызван двумя причинами: отказом элемента релейной защиты с вероятностью $p_{j1}(t)$ или отказом силового элемента с вероятностью $p_{j2}(t)$. Этот переход может сопровождаться соответственно крупной аварией и относительно небольшими последствиями. Поэтому и при оценке потерь c_j возникают некоторые сложности. Для их устранения состояние S_j предлагается разбить на два: S_{j1} и S_{j2}, соответствующих указанным причинам. При этом упрощается оценка и потерь c_{j1} и c_{j2}. Оценка среднего значения технологического риска производится по формуле полной вероятности

$$R(t)=c_1p_1(t)+c_2p_2(t),$$

которая в общем виде представляется как

$$R(t)=\sum_{S_j\in E_-}c_jp_j(t),$$

где суммирование производится по множеству неблагоприятных состояний.

Предположим, что процесс функционирования системы состоит из случайных времен пребывания в некоторых состояниях и мгновенных переходов из одного состояния в другое. Случайное время пребывания в состоянии *i* характеризуется вероятностью $p_i(t)$, а переход из состояния *i* в состояние *j* – параметром перехода $\omega_{i,j}(t)$, который при фиксированном времени *t* – случайная величина, принимающая целочисленные значения. Между вероятностями пребывания системы в различных состояниях и средним числом переходов $M_{i,j}(t)$ между состояниями существует зависимость [63]

$$p_j(t)=\sum_{S_i\to S_j}M_{i,j}(t)-\sum_{S_j\to S_i}M_{j,i}(t),$$

где $M_{i,j}(t)=\omega_{i,j}(t)$, $M_{j,i}(t)=\omega_{j,i}(t)$.

Следовательно, вероятность $p_j(t)$ состояния S_j равна общему числу пере-

ходов $M_{i,j}(t)$ из всех состояний S_i в данное состояние S_j за исключением общего числа переходов из данного состояния S_j во все другие S_i.

Если система работает до первого попадания в неблагоприятное состояние, то, попав в любое из неблагоприятных состояний S_j, она навсегда в нем остается (поглощающее состояние). Вероятность этого состояния

$$p_j(t) = \sum_{S_i \to S_j} M_{i,j}(t) = \sum_{S_i \in E_+} M_{i,j}(t).$$

Здесь суммирование производится по всем благоприятным состояниям $S_i = E_+$, из которых имеется непосредственный переход в состояние $S_j = E_-$. Выражение для вычисления технологического риска принимает вид

$$R(t) = \sum_{S_j \in E_-} c_j \sum_{S_i \in E_+} M_{i,j}(t).$$

Таким образом, средний риск системы равен сумме произведений потерь от перехода в каждое неблагоприятное состояние, умноженных на общее среднее число переходов в него.

В ряде случаев, попав в какое-либо из неблагоприятных состояний S_j, система может перейти в другие, более тяжелые состояния, оставаясь в E_- и не переходя, по условиям, оговоренным выше, в множество E_+. Такая ситуация характерна для каскадного развития аварий в электроэнергетических системах. Величина риска при таких условиях определяется по формуле

$$R(t) = \sum_{S_j \in E_-} c_j \sum_{S_i \in E_+} M_{i,j}(t) + \sum_{S_k \in E_-} \sum_{S_j \in E_-} (c_j - c_k) M_{k,j}(t).$$

Второе слагаемое в этом выражении обусловлено переходными процессами в множестве неблагоприятных состояний E_-. Оно обращается в нуль, если потери системы для каждого неблагоприятного состояния одинаковы: $c_j - c_k$ для любых $S_k, S_j \in E_-$.

При допущении экспоненциального распределения времени до перехода системы, состоящей из m элементов в неблагоприятное состояние, величина риска определяется как

$$R(t) = \sum_{i=1}^{m} \omega_i c_i \frac{1 - e^{-\omega_c t}}{\omega_c},$$

где $\omega_c = \sum_{i=1}^{m} \omega_i$ – частота перехода системы в неблагоприятное состояние.

Ещё пример. В годовом договоре на электроснабжение предусмотрены возможные отключения четырех подстанций потребителя с частотами: $\omega_1 = 3$ год$^{-1}$, $\omega_2 = 5$ год$^{-1}$, $\omega_3 = 7$ год$^{-1}$, $\omega_4 = 9$ год$^{-1}$. В соответствии с особенностями технологического процесса ущерб при погашении каждой из подстанций составляет: $c_1 = 650$ тыс. руб., $c_2 = 1430$ тыс. руб., $c_3 = 800$ тыс. руб., $c_4 = 920$ тыс. руб. Тогда возможное количество отключений:

$$\omega_c = \sum \omega_i = 3 + 5 + 7 + 9 = 24 \text{ год}^{-1}.$$

Вычислим: $\sum_{i=1}^{m} \omega_i c_i = 3 \cdot 650 + 5 \cdot 1430 + 7 \cdot 800 + 9 \cdot 920 = 22980$ тыс. руб.

Риск системы: $R(t) = 22980 \dfrac{1 - e^{-24t}}{24} = 957{,}5(1 - e^{-24t})$.

С течением времени (с момента заключения договора сроком на один год) средний риск системы изменяется, возрастая от $R(t = 0) = 0$ до $R(t = 1) \approx 957{,}5$ тыс. руб. Из четырех подстанций самой критичной является четвертая, поскольку для нее $\omega_4 c_4 = 9 \cdot 920 = 8280$ тыс. руб.

Одним из показателей ответственности потребителей электрической энергии является допустимая длительность перерыва электроснабжения, которая в зависимости от особенностей производства колеблется от десятых долей секунды (химические производства и установки нефтеперерабатывающих заводов) до десятков минут (отдельные стадии металлургического производства). Последствия внезапных нарушений электроснабжения ответственных потребителей, их характер, результаты и проявления зачастую неясны, причинно-следственные связи в них сложны и запутанны, их оценка весьма субъективна, многим из них присуща неопределенность. Одно и то же воздействие, происходящее в различные периоды времени, не обязательно оценивается одинаково. В большой степени это зависит от попадания момента внезапного нарушения электроснабжения на ту или иную стадию технологического процесса, а также длительности восстановления электроснабжения при отказе или ограничении в электропотреблении. Практически в качестве сигнала на выходе системы выступает не стандартный набор известных функций, а вероятностный сигнал.

9.4. Основы теории потенциальной эффективности

Постоянная реализация мероприятий по повышению эффективности функционирования как СЭС, так и технологического процесса позволяет

снизить вероятности нахождения производственной системы в неблагоприятных состояниях. В настоящее время имеется несколько предложений по подходу к оценке показателей надежного и безопасного функционирования производственных систем при внезапных нарушениях их электроснабжения. Наиболее логичным является вероятностный подход. Он устраняет элементы субъективизма, неизбежно присутствующие при разделении всех ситуаций на вероятные и невероятные. Такой подход включает [50]:

- определение условной вероятности аварийных ситуаций;
- оценку вероятности нарушения электроснабжения;
- определение вероятности попадания события в критические области.

Известно, что каждый несчастный случай уникален вследствие редкости и специфичности характера аварий, поэтому статистических данных для прямого определения их вероятности недостаточно. Долговременные статистические ряды, составленные при весьма изменчивых условиях, дают лишь кажущуюся, ложную точность, поэтому воспользоваться этим методом практически невозможно из-за отсутствия информации по конкретным событиям. Привлечение высококвалифицированных экспертов сопряжено со значительными трудностями. Кроме того, среди экспертов существуют разногласия относительно риска при предельных значениях вероятностей катастрофических последствий. Риск, когда имеется один шанс на миллион, что произойдет катастрофа при нарушении электроснабжения на химическом предприятии, оценивается как гораздо больший, чем четыре таких шанса в машиностроении, хотя последствия могут быть и соизмеримыми. Поэтому использование оценок степени риска позволяет сделать хотя бы ориентировочную оценку вероятностей катастрофических последствий.

В отличие от классического экспертного метода существует подход, основанный на принципах теории потенциальной эффективности. В рамках этой теории предлагается нестатистический метод, основанный на концепции предельно возможного события. При этом рассматривается наихудшее из возможных событий, вероятностью которого нельзя пренебречь. Если проводимым анализом будет показано, что последствия аварийной ситуации меньше некоторого допустимого, заранее заданного значения, то считается, что производственный объект удовлетворяет предъявляемым требованиям надёжной эксплуатации. Ориентируясь на международную практику, можно считать, что интервал $10^{-5}...10^{-8}$ является разумным для ежегодного индивидуального риска.

Некоторой модификацией предельного метода является следующий подход. Из практических соображений целесообразности, опыта проектирования и эксплуатации экспертами (или исходя из данных статистики)

назначается допустимая вероятность достижения цели объектом электроснабжения R_0. В качестве цели рассматривается безотказность технологического процесса при нарушениях в системе его электроснабжения за практически приемлемое время функционирования T_0 рассматриваемого объекта. Эта пара параметров называется порогами осуществимости [77, 78]. Порядок величин для их задания выбирается в зависимости от последствий, к которым может привести внезапное нарушение электроснабжения. Однако очевидна тенденция выбора R_0 близким к единице, а T_0 в пределах срока службы основного технологического оборудования. Потребители, нарушение электроснабжения которых приводит к указанным последствиям, работают, как правило, на объектах с экстремальными технологическими и конструкционными параметрами.

Исходя из опыта эксплуатации таких объектов, а также темпов научно-технического прогресса, сроков физического и морального износа электрооборудования, предположим, что предельное значение T_0 не превышает $T_0 \le 25$ лет.

Одним из главных показателей, который может повлиять на выбор более удобной величины $P_0 = 1 - R_0$, является условная вероятность возникновения указанных последствий при внезапных нарушениях электроснабжения.

Например, по данным наблюдений или экспертного опроса, в результате 100 условных нарушений электроснабжения произошло (или ожидается) 10 повреждений определенного вида технологического оборудования. Такая информация не позволяет однозначно восстановить значение параметра $\overline{P_{\text{то}}}$ – вероятности отказа вследствие случайной зависимости единичного $P_{\text{то}i}$ и среднего $\overline{P_{\text{то}}}$ значений. Тем не менее, ясно, что при данном результате наблюдений значения параметра $\overline{P_{\text{то}}}$ порядка 0,1 должны быть более вероятными, чем порядка 0,8. Параметр $\overline{P_{\text{то}}}$ является неизвестной, но фиксированной константой. Ему можно приписать некоторое распределение, называемое фидуциальным, которое бы отражало имеющуюся о $\overline{P_{\text{то}}}$ информацию.

Так, оценка вероятности повреждения технологического оборудования $P_{\text{то}i}$ отдельных установок нефтеперерабатывающих заводов, по данным статистики и экспертного опроса, достигает $P_{\text{то}i} = 0{,}4$.

Порог осуществимости для процессов, срывы которых не связаны с риском для жизни людей, $P_0 = 10^{-3}$ год$^{-1}$. При заданных границах порогов осуществимости и условии, что допустима единственная реализация небла-

гоприятного события, надежная работа технологического объекта будет обеспечена на всем интервале T_0, если

$$P_{\text{то}i}\, p_{\text{эс}} \le P_0 T_0,$$

где $p_{\text{эс}}$ – оценка вероятности нарушения электроснабжения на периоде T_0.

Следовательно, вероятность нарушения электроснабжения анализируемого потребителя за период его эксплуатации составит

$$p_{эс} = \frac{P_0 T_0}{P_{\text{то}i}} = \frac{10^{-3} \cdot 25}{0{,}4} = 0{,}0625.$$

Переходя к общепринятому среднему параметру потока отказов

$$\omega = \frac{p_{\text{эс}}}{T_0} = \frac{0{,}0625}{25} = 0{,}0025 \text{ год}^{-1}.$$

Такая оценка определяет требуемый уровень надёжности сборных шин, от которых питается рассматриваемый объект, с учетом риска получения расчетных последствий внезапных нарушений электроснабжения и создает предпосылки для принятия решений по структуре и параметрам схемы электроснабжения. Принятие или обоснование этих значений можно производить исходя либо из того, «что нужно» для выполнения заданных функций, либо из того, «что можно» сделать при существующем уровне техники и имеющихся ограничениях. Определив требования по принципу «что нужно», следует проверить, соответствует ли это тому, «что можно».

Уровень надёжности существующих объектов сравнивается с полученными оценками риска неблагоприятных ситуаций для принятия соответствующих мер, а принцип «что нужно» – учитывается при проектировании подобных или близких к ним объектов.

9.5. Вопросы страхования рисков в СЭС

Специальный механизм перераспределения риска между сторонами при заключении сделки – страхование. В качестве покупателя риска (возможного ущерба) выступает страховая компания – страховщик. Продавцы риска – клиенты (страхователи), каждый из которых в соответствии со своими предпочтениями оценивает угрозу реализации своего риска. Время предъявления страхового случая (момент предъявления претензии страховщику, выплаты возмещения, урегулирования претензии), моделируется пуассоновским процессом с интенсивностью λ=const. Если $N(t)$ – число

страховых убытков, появившихся за период [0,*t*], то эта величина имеет распределение Пуассона

$$P[N(t)=k]=\frac{(\lambda t)^k}{k!}e^{-\lambda t}$$

с числовыми характеристиками математического ожидания и дисперсии

$$M[N(t)]=\lambda t,\ \ D[N(t)=\lambda t\ .$$

Суммарный убыток (ущерб) за период [0, *t*] обозначим $Y_t=\sum_{i=1}^{N(t)} y_i$. При постоянной интенсивности поступления страховых взносов *c* за период *t* сумма их составит $C=ct$. Тогда риск разорения для резервного фонда страховщика V_t

$$V_t=V_0+C-Y_t\ ,$$

где V_0 – начальный резерв страхового фонда.

Вид траекторий этого процесса представлен на рис. 9.2. Ущерб появляются в случайные моменты времени t_1, t_2, …t_i. В каждый из них – t_i размер V_t уменьшается на случайную величину y_i, а в промежутках $[t_i, t_{i+1}]$ линейно возрастает в соответствии с постоянной интенсивностью *c* поступления страховых взносов. Распределение времени между моментами двух убытков (выплат возмещений) для пуассоновского процесса – экспоненциальное, с параметром λ. Поэтому среднее время ожидания очередного страхового случая – $T_{\text{ср}}=1/\lambda$.

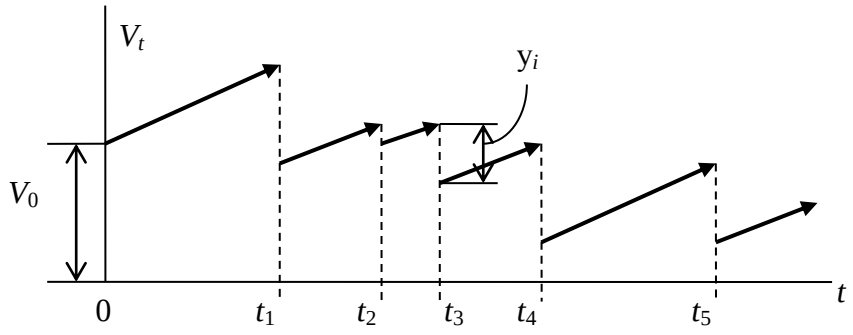


Рис. 9.2. Случайный процесс использования фонда страховщика

Страхование рисков перерыва в производстве энергетической продукции и электроснабжении потребителей является важным звеном общей системы управления рисками. В настоящее время достаточно широко используется система *BI* (Business Interruption). В момент возникновения имущественного ущерба срабатывает так называемый trigger *BI*. Заканчивается *BI*,

когда оборудование технически готово к продолжению застрахованной деятельности и объект энергетики достигает экономических показателей, существовавших перед отказом. Максимальный период возмещения ущерба лимитируется предельно возможным сроком восстановления наиболее важного для деятельности оборудования или всей системы в целом (6–24 месяца). Картина *BI* представлена на рис. 9.3.

Наиболее прогрессивную часть этого подхода представляет предложение по введению страховой схемы с обратной связью для услуги «надежность электроснабжения». Под надежностью здесь понимается электроснабжение потребителя с требуемыми ему параметрами технологического процесса в течение базового (расчетного) периода. Количественно она определяется числом отключений (ограничений) потребителя в течение базового периода и средней их длительностью. В то же время должна фиксироваться общая длительность простоев основных технологических объектов. При этом неважно, является ли нарушение электроснабжения следствием отключений ЛЭП, её перегрузки, отключения части генерирующих мощностей, недопустимого по условиям технологического процесса потребителя падения напряжения в сети и т. п.

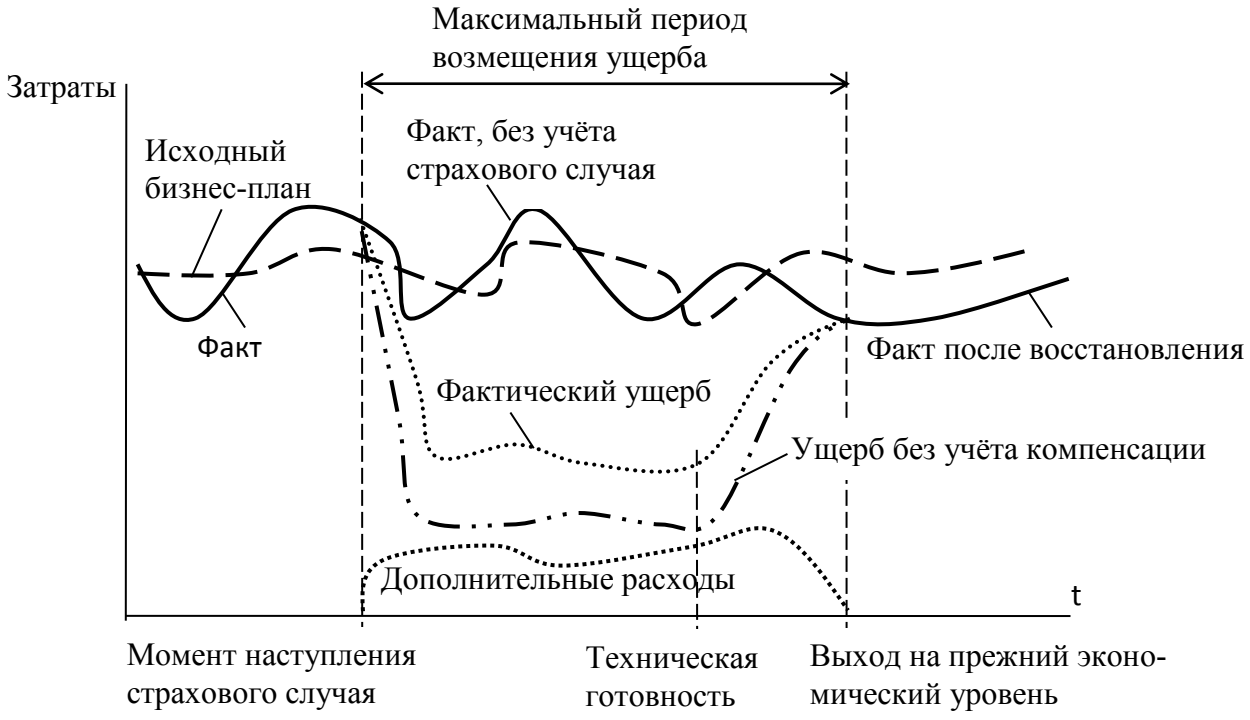


Рис. 9.3. Иллюстрация системы *BI* страхования рисков

Например, начальными условиями первого шага решения такой задачи допускается, что количество нарушений электроснабжения потребителей может составлять до $n = 10$ при средней суммарной длительности простоев

t = 10 часов за базовый период. Эффект увеличения надежности моделируется как параметр, связанный с длительностью простоев потребителя.

Предполагается, что система управления электропотреблением позволяет в зависимости от типа потребителя, режима его работы и нагрузки сокращать длительность нарушения нормального режима электроснабжения без срыва параметров основного технологического процесса [50].

Средняя длительность возможных простоев потребителя изменяется в соответствии с инвестициями, направленными им на увеличение надежности питающей сети. Потребитель сам определяет требуемый ему уровень надежности.

Если он не вкладывает средств в увеличение надежности электроснабжения и не предпринимает никаких мер по управлению режимом электропотребления, договорная длительность каждого отключения (ограничения) может составлять t_0 = 2 часа. При управления нагрузкой – $t_{0у}$ = 1 час. При вложении средств в надежность системы его электроснабжения $t_{0ус}$ = 0,5 часа. Одновременное выполнение программ вложения инвестиций и управление нагрузкой сокращает договорную длительность нарушений электроснабжения до $t_{0\Sigma}$ = 0,1 часа.

Потребителю может быть рекомендовано вкладывать средства в изменение топологии сети (увеличение надежности) с целью минимизации или предотвращения экономических потерь в результате воздействий со стороны ЭСО или те же средства вкладывать в новое технологическое оборудование для максимизации прибыли независимо (в допустимых пределах) от режимов электропотребления, устанавливаемых ЭСО.

Для усреднённого показателя надежности существующей сети ЭСО может установить среднее предложение по его стоимости. Если потребитель желает получить более высокий (или низкий) по отношению к среднему показатель, он может быть получен при соответствующей оплате услуги. Потребителям предлагается меню из, например, трех вариантов: существующий уровень надежности; уровень выше существующего и ниже его. В таблице 9.1 приведен пример такого тарифного меню.

Таблица 9.1

Пример тарифного меню

Уровень надежности электроснабжения	Величина, %	Относительная стоимость 1МВт.ч	Страховой взнос, % от стоимости 1 МВт.ч
Высокий	99,95	5	0,5
Базовый	99,90	2	0,2
Низкий	99,80	1	0,1

Потребители выбирают наиболее подходящий договор страхования в зависимости от цены предоставляемой услуги и получают в случае нарушения условий договора возмещение потерь, соответствующее оценке ущерба от нарушения договорного режима электроснабжения.

Из зарубежного опыта страхования рисков нарушения энергоснабжения известно, что в августе 2003 г. электроснабжение большинства пострадавших от отключения потребителей Калифорнии (США) было восстановлено в течение оговоренного времени, авария не привела к появлению большого числа требований о возмещении ущерба. В страховых полисах домовладельцев США предусмотрено возмещение ущерба, вызванного отключением электроэнергии до 500$, а также из-за простоя системы насосов закачки воды и откачки сточных вод, если насос не мог работать из-за отключения электроэнергии.

ЗАКЛЮЧЕНИЕ

Потребность в электроэнергии растёт во всём мире, но в ещё большей степени, в условиях высокой конкуренции, растут требования к эффективности, надёжности и качеству электроснабжения потребителей. Закономерности функционирования и развития современных СЭС, подходов к управлению их режимами, формируют и закономерности развития энергетики в целом, а также её составляющих в отраслевом и территориальном аспектах. Результаты анализа этих тенденций и закономерностей наряду со структурными и функциональными свойствами СЭС являются основой формирования энергетической политики на региональном и государственном уровнях. В настоящее время перед энергетическими компаниями страны поставлено множество стратегических задач, приоритетными из которых являются задачи обеспечения энергетической безопасности, повышения надёжности и качества электроснабжения, формирования и расширения спектра потребительских сервисов. Повышение эффективности функционирования СЭС возможно за счёт развития и совершенствования интеллектуальных систем управления структурой, режимами и параметрами СЭС совместно с технологическими режимами и параметрами потребителя. Модернизация релейной защиты и автоматики, систем контроля и управления режимами СЭС и электропотреблением, должна сопровождаться объективной оценкой технико-экономической эффективности мероприятий по повышению надёжности.

Естественно, что для решения поставленной задачи необходимо владение соответствующим математическим аппаратом, включающим теорию систем и системный анализ, теорию надёжности.

Развитие систем РГ и ВИЭ выдвигает требования по обеспечению надёжности электроснабжения от этих источников, отличающиеся от классических оценок. Для их успешного внедрения требуется интегрированная инфраструктура безопасности. Множество технологических решений, используемых в проектах по созданию РГ может стать источником уязвимостей всей инфраструктуры интеллектуальной сети электроснабжения.

На приведённых примерах рассмотрены особенности современных СЭС и возможности их формализованного описания; предложено расширение надёжностных свойств СЭС; показаны возможности повышения эффективности функционирования СЭС и потребителей; уточнены модели участков производственных систем для оценки технико-экономических потерь

потребителей при нарушениях электроснабжения; показано, что катастрофические события (блекауты, системные аварии и катастрофы на объектах энергетики) не являются исключительными, а имеют достаточно большую вероятность, с которой необходимо считаться. Предложения, сформулированные в настоящей работе, открывают перспективу дальнейшего исследования чрезвычайно важной проблемы оценки вероятностей редких событий и катастроф в электроэнергетике.

Анализ, формализация и решение поставленных в монографии и других задач, возникающих в условиях интеллектуализации систем энергетики, их увязка и согласование в рамках системного подхода являются предметом дальнейших исследований.

СПИСОК ЛИТЕРАТУРЫ

1. *Авондо-Бодино Дж.* Применение в экономике теории графов. М.: Изд-во «Прогресс», 1966.
2. *Андриенко А.Я., Портнов-Соколов Ю.П.* Формирование риска при обеспечении безопасности сложных технических систем // Приборы и системы управления. 1996. № 12. С. 11–14.
3. *Бакулин В.М., Малков С.Ю., Гончаров В.В., Ковалёв В.И.* Управление обеспечением стойкости сложных технических систем. М.: ФИЗМАТЛИТ, 2006.
4. *Бартоломей П.И., Паниковская Т.Ю.* Оптимизация режимов энергосистем. Екатеринбург: УГТУ–УПИ, 2008.
5. *Биллинтон, Р., Алан Р.* Оценка надёжности электроэнергетических систем. М.: Энергоатомиздат, 1988.
6. *Бусленко Н.П.* Моделирование сложных систем. М.: Главная редакция физико-математической литературы изд-ва «Наука», 1968.
7. *Бусленко Н.П., Калашников В.В., Коваленко И.Н.* Лекции по теории сложных систем. М.: изд-во «Советское радио», 1973.
8. *Ван дер Варден.* Математическая статистика. М: Изд-во Иностранной литературы, 1960.
9. *Васильев А.П.* Методы и средства управления надёжностью и безопасностью электрических сетей и установок электроэнергетических систем. СПб.: Изд-во Политехн. ун-та, 2014.
10. *Вентцель Е.С.* Теория вероятностей. М.: Наука, 1969.
11. *Волик Б.Г.* О концепциях техногенной безопасности. Автоматика и телемеханика. 1998. № 2. С. 165–170.
12. *Волков Л.И.* Безопасность и надёжность систем. М.: Изд-во СИП РИА, 2003.
13. *Волкова В.Н., Денисов А.А.* Теория систем: учебник для студентов вузов. М.: Высшая школа, 2006.
14. *Воропай Н.И.* Надежность систем электроснабжения: конспект лекций. Новосибирск: Наука, 2006.
15. *Воропай Н.И.* Надежность систем электроснабжения. Новосибирск: Наука, 2015.
16. *Горнштейн В.М.* Наивыгоднейшее распределение нагрузок между параллельно работающими электростанциями. М.; Л: Государственное энергетическое издательство, 1949.

17. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

18. *Гук Ю.Б.* Теория надежности в электроэнергетике. Л.: Энергоатомиздат. Ленингр. отделение, 1990.

19. *Гумбель Э.* Статистика экстремальных значений. М.: Мир, 1965.

20. *Гуревич Ю.Е., Илюшин П.В.* Особенности расчётов режимов в энергорайонах с распределённой генерацией. Н. Новгород: НИУ РАНХиГС, 2018.

21. *Дзиркал Э.В.* Задание и проверка требований к надёжности сложных изделий. М.: Радио и связь, 1981.

22. *Дженкинс Г., Ватс Д.* Спектральный анализ и его приложения. Вып. 1. М.: Мир, 1971.

23. *Илюшин П.В., Куликов А.Л.* Автоматика управления нормальными и аварийными режимами энергорайонов с распределённой генерацией. Н. Новгород: НИУ РАНХиГС, 2019.

24. URL: https://www.anti-malware.ru/news/2020-12-07-111332/34426?utm_source=google&%3Butm_medium=email&%3Butm_campaign=amdelivery.

25. *Капур К., Ламберсон Л.* Надёжность и проектирование систем. М.: Изд-во «Мир», 1980.

26. *Касти Дж.* Большие системы. Связность, сложность и катастрофы. М.: Мир, 1982.

27. *Китушин В.Г.* Надежность энергетических систем. Ч. 1. Теоретические основы. Новосибирск: Изд-во НГТУ, 2003.

28. *Коваленко И.Н.* Анализ редких событий при оценке эффективности и надёжности систем. М.: Изд-во «Советское радио», 1980.

29. *Коваленко И.Н., Кузнецов Н.Ю.* Методы расчёта высоконадёжных систем. М.: Радио и связь, 1988.

30. *Конторов Д.С., Голубев-Новожилов Ю.С.* Введение в радиолокационную системотехнику. М.: Советское радио, 1971.

31. *Куклев Е.А.* Определение рисков возникновения опасных сближений морских судов в аварийных ситуациях путём прогнозирования нечётких «окон уязвимости». Транспорт Российской Федерации. 2016. № 4 (65). С. 28–31.

32. *Куликов А.Л., Осокин В.Л, Папков Б.В.* Проблемы и особенности распределённой электроэнергетики // Вестник НГЭИ 2018. № 11 (90). С. 123–136.

33. *Манов Н.А.* Концепция расширенной совокупности надёжностных свойств объектов электроэнергетики. Препринт Коми НЦ УрО РАН, 1992. Вып. 296.

34. *Майоров А.В.* Оценка надёжности системы защиты и автоматики электрической сети 20 кВ мегаполиса при внедрении дифференциальных защит // Энергия единой сети. 2019. № 5. С. 52–58.

35. *Махутов Н.А., Гаденин М.М., Чернявский А.О., Шатов М.М.* Анализ рисков отказов при функционировании потенциально опасных объектов // Проблемы анализа риска. 2012. Т. 9. № 3. С. 8–20.

36. *Мелентьев Л.А.* Системные исследования в энергетике. Элементы теории, направления развития. М.: Наука, 1983.

37. Методические вопросы исследования надёжности больших систем энергетики. Вып. 20. Живучесть систем энергетики. Иркутск: СЭИ СО АН СССР, 1980.

38. Методические указания по расчету вероятности отказа функционального узла и единицы основного технологического оборудования и оценки последствий такого отказа. Приложение к приказу Минэнерго России от 19.02.2019 г. № 123.

39. Методы и модели исследования живучести систем энергетики. Новосибирск: Наука. Сиб. отд-ние, 1990.

40. Методы определения и контроля надёжности больших систем / под ред. А.А. Червоного. М.: Энергия, 1976.

41. *Михайлов В.В.* Тарифы и режимы электропотребления. М.: Энергоатомиздат, 1986.

42. Надёжность и эффективность в технике: справочник. В 10 т. Т. 5: Проектный анализ надёжности. М.: Машиностроение, 1988.

43. Надёжность систем энергетики: Проблемы, модели и методы их решения / А.Ф. Дьяков, В.А. Стенников, С.М. Сендеров [и др.]; отв. ред. Н.И. Воропай. Новосибирск: Наука, 2014.

44. Надежность систем энергетики и их оборудования / под общ. ред. Ю.Н. Руденко. В 4-х т. Т. 2: Надежность электроэнергетических систем: справочник / под ред. М.Н. Розанова. М.: Энергоатомиздат, 2000.

45. Надёжность технических систем: справочник / под ред. И.А. Ушакова. М.: Радио и связь, 1985.

46. *Непомнящий В.А.* Учет надежности при проектировании энергосистем. М.: Энергия, 1978.

47. *Непомнящий В.А.* Экономические потери от нарушения электроснабжения потребителей. М.: Издательский дом МЭИ, 2010.

48. *Нечипоренко В.И.* Структурный анализ систем (эффективность и надёжность). М.: Сов. радио, 1977.

49. Оптимальные задачи надёжности / под ред. И.А. Ушакова. М.: Изд-во комитета стандартов, мер и измерительных приборов при СМ СССР, 1968.

50. *Папков Б.В.* Надёжность и эффективность электроснабжения. Нижний Новгород: Нижегород. гос. техн. ун-т, 1996.

51. *Папков Б.В.* Становление и развитие электротехники и электроэнергетики: краткая хроника событий и фактов. Нижний Новгород: Изд-во «Кварц», 2011.

52. *Папков Б.В.* Уязвимость и стойкость объектов электроэнергетики. Методические вопросы исследования надежности больших систем энергетики: Вып. 68: Исследование и обеспечение надежности систем энергетики. Иркутск: ИСЭМ СО РАН, 2017. С. 441–452.

53. *Папков Б.В.* Сложность систем электроснабжения. Методические вопросы исследования надежности больших систем энергетики: Вып. 71: Надежность энергоснабжения потребителей в условиях их цифровизации. В 3-х кн. Кн. 2. Иркутск: ИСЭМ СО РАН, 2020. С. 9–18.

54. *Папков Б.В., Куликов А.Л.* Теория систем и системный анализ для электроэнергетиков. М.: Изд-во Юрайт, 2016.

55. *Папков Б.В., Куликов А.Л.* Элементы теории графов в задачах электроэнергетики. Н. Новгород: НИУ РАНХиГС, 2019.

56. *Папков Б.В., Куликов А.Л., Осокин В.Л.* Проблемы кибербезопасности электроэнергетики. М.: НТФ «Энергопрогресс», 2017 [Библиотечка электротехника, приложение к журналу «Энергетик». Вып. 9 (225)].

57. *Папков Б.В., Куликов А.Л., Осокин В.Л.* Вероятности редких случайных событий в электроэнергетике // Электричество, 2019. № 2. С. 4–9.

58. *Папков Б.В., Осокин В.Л.* Вероятностные и статистические методы оценки надёжности элементов и систем электроэнергетики: теория, примеры, задачи. Старый Оскол: ТНТ, 2017.

59. *Папков Б.В., Осокин В.Л.* Теоретические основы надёжности и эффективности электроснабжения. Старый Оскол: ТНТ, 2019.

60. *Папков Б.В., Осокин В.Л.* Особенности оценки структурной надежности систем с объектами распределенной генерации // Известия РАН. Энергетика. 2020. № 2. С. 75–84.

61. *Папков Б.В., Осокин В.Л., Куликов А.Л.* Развитие понятия «надежность» в современной электроэнергетике // Оперативное управление в электроэнергетике. 2018. № 6. С. 43–52.

62. *Плямоватый В.В.* К теории «выживания» сложных систем. В сб. тр. семинара научного совета по проблемам надёжности отделения механики и процессов управления АН СССР «Основные вопросы теории и практики надёжности». М.: Советское радио, 1980. С. 283–292.

63. *Половко А.М., Гуров С.В.* Основы теории надёжности. СПб.: БХВ-Петербург, 2006.

64. *Порфирьев Б.Н.* Управление в чрезвычайных ситуациях: проблемы теории и практики // «Проблемы безопасности: чрезвычайные ситуации». Т. 1. М.: ИНТ, 1991.

65. *Прангишвили И.В.* Системный подход и общесистемные закономерности. М.: СИНТЕГ, 2000.

66. *Прангишвили И.В.* Системный подход и повышение эффективности управления. М.: Наука, 2005.

67. *Радаев Н.Н.* Повышение точности прогноза вероятности катастроф за счет учета неоднородных статистических данных по ущербу // АиТ. 2000. № 3. С. 183–189.

68. *Райншке К., Ушаков И.А.* Оценка надёжности систем с использованием графов. М.: Радио и связь, 1988.

69. *Руденко Ю.Н., Ушаков И.А.* Надежность систем энергетики. Новосибирск: Наука. Сиб. отд-ние, 1989.

70. *Рябинин И.А.* Основы теории и расчёта надёжности судовых электроэнергетических систем. Л.: Судостроение. 1971.

71. *Рябинин И.А.* Надёжность и безопасность структурно-сложных систем. СПб.: Политехника, 2000.

72. Снижение рисков каскадных аварий в электроэнергетических системах. Новосибирск: Изд-во СО РАН, 2011.

73. *Солодовников В.В., Тумаркин В.И.* Теория сложности и проектирование систем управления. М.: Наука. Гл. ред. физ.-мат. лит., 1990.

74. *Ушаков И.А.* Эффективность функционирования сложных систем // О надёжности сложных технических систем. М.: Советское радио, 1966. С. 26–56.

75. *Ушаков И.А.* Методы исследования эффективности функционирования технических систем. М.: Изд-во «Знание», 1976.

76. *Ушаков И.А.* Курс теории надёжности систем. М.: Дрофа, 2008.

77. *Флейшман Б.С.* Элементы теории потенциальной эффективности сложных систем. М.: Советское радио, 1971.

78. *Флейшман Б.С.* Основы системологии. М.: Радио и связь, 1982.

79. *Хенли Э.Дж., Кумамото Х.* Надежность технических систем и оценка риска. М.: Машиностроение, 1984.

80. *Чечулин А.А., Котенко И.В.* Построение графов атак для анализа событий безопасности // Безопасность информационных технологий. 2014. Т. 21. № 3. С. 135–141.

81. *Чура Н.Н.* Техногенный риск. М.: КНОРУС, 2015.

82. *Шоломицкий А.Г.* Теория риска. Выбор при неопределённости и моделирование риска. М.: Изд. Дом ГУ ВШЭ, 2005.

83. *Щербаков Н.С.* Достоверность работы цифровых устройств. М.: Машиностроение, 1989.

84. *Эндрени Дж.* Моделирование при расчётах надёжности в электроэнергетических системах. М.: Энергоатомиздат, 1983.

85. Энергетическая безопасность России. Новосибирск: Наука. Сибирская издательская фирма РАН, 1998.

86. Системные исследования проблем энергетики / под ред. Н.И. Воропая. Новосибирск: Наука. Сибирская издательская фирма РАН, 2000.

87. *Папкова М.Д., Папков Б.В.* Риски субъектов электроэнергетического рынка. Нижний Новгород: ННГАСУ, 2007.

88. *Вуколов В.Ю., Колесников А.А., Пнёв Е.Р., Папков Б.В.* Управление конфигурацией распределительных электрических сетей 6–35 кВ // Электричество. 2019. № 2. С. 10–17.

89. *Виноградов А.В.* Понятие и принципы управления конфигурацией интеллектуальных электрических сетей // Агротехника и энергообеспечение. 2020. № 4 (29). С. 5–14

Научное издание

Борис Васильевич Папков
Павел Владимирович Илюшин
Александр Леонидович Куликов

НАДЁЖНОСТЬ И ЭФФЕКТИВНОСТЬ СОВРЕМЕННОГО ЭЛЕКТРОСНАБЖЕНИЯ

Монография

Издается в авторской редакции

Технический редактор *С.Е. Речнова*
Комп. верстка *Н.Ю. Студеникина*

Сдано в набор 8.02.2021. Подписано в печать 2.03.2021.
Формат 60×84/16. Печать офсетная. Бумага офсетная.
Уч.-изд. л. 9,8. Усл. печ. л. 9,3. Тираж 500 экз.

Научно-издательский центр «XXI век»
603081, Нижний Новгород

Отпечатано в Типографии «Игуана»
Нижний Новгород, ул. Деловая, 19

ISBN 978-5-6045837-5-3