УДК 510.65; 65.011.56; 699.8

СИНЕЩУК Ю.И., ФИЛИППОВ А.Г., ТЕРЕХИН С.Н., НИКОЛАЕВ Д.В., САЕНКО И.Б.

СТРУКТУРНО-ЛОГИЧЕСКИЙ МЕТОД АНАЛИЗА БЕЗОПАСНОСТИ ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ

Синещук Ю.И., Филиппов А.Г., Терехин С.Н., Николаев Д.В., Саенко И.Б. **Структурно-логический метод анализа безопасности потенциально опасных объектов.**
Аннотация. В статье авторами предлагается алгоритм проведения качественного анализа безопасности и надежности систем, технологических процессов, а также вероятного риска и возможных потерь, путем использования специального метода анализа, который направлен на уменьшение вероятности аварий и несчастных случаев, человеческих жертв и экономических потерь. Рассмотрены основные преимущества данного метода, его система и составные элементы, причины отказа составных элементов, предложена процедура построения данного метода, приведены формулы для расчетов.
Ключевые слова: система безопасности, надежность, опасные состояния, авария, несчастный случай, экономические потери, уровень безопасности.

Sineshchuk Y.I., Philippov A.G., Terehin S.N., Nikolaev D.V., Saenko I.B. **Structural-logical method of the safety analysis of the potentially dangerous objects.**
Abstract. In article authors propose the algorithm of carrying out of the qualitative analysis of safety and reliability of systems, technological processes, and also of probable risk and possible losses, by using of a special method of the analysis which is directed on reduction of probability of failures and accidents, human victims and economic losses. The basic advantages of the given method, its system and components, and causes of failures of components are considered, procedure of construction of the given method is proposed, formulas for calculations are presented.
Keywords: safety system, reliability, dangerous conditions, failure, accident, economic losses, safety level.

1. Введение. Проявление сложности современных систем (атомных электростанций, военных систем, отраслевых и региональных информационно-вычислительных систем, систем и средств автоматизации управления и др.) до конца не познано в научном плане и не решено удовлетворительно в прикладном смысле. Вероятность аварий на них меньше, чем у простых систем, но их последствия более масштабны и ликвидируются тяжелее[3]. В условиях дальнейшего развертывания научно-технического прогресса вопросы устойчивости функционирования сложных систем приобретают первостепенное и самостоятельное значение в отношении потенциально опасных объектов.

Крупнейшие аварии и катастрофы выявили существенную роль и значимость научных разработок проблемы аудита (анализа) безопасности сложных систем, необходимость применения системного подхода к исследованию этого свойства. Целью работы является исследование возможности и выявление особенностей применения структурно-логического метода к анализу безопасности потенциально опасных объектов.

2. Проблема безопасности потенциально опасного объекта. Усилия, направленные на повышение безотказности, живучести, отказоустойчивости системы, необходимы, но они не обеспечивают ее безопасности. Даже специально создаваемые системы контроля и защиты не могут гарантировать защиты от произвольных комбинаций событий (отказов), нарушений правил эксплуатации и иных неблагоприятных воздействий.

Интуитивное представление о сложности системы связывается с объемом оборудования (числом элементов, их массой, габаритными размерами и т. д.); разветвленностью связей между элементами и степенью их взаимодействия (многосвязностью, многорежимностью и т. д.); квалификацией персонала; стоимостью изготовления всей системы; трудностью оценки ее качества в целом, и отдельных ее свойств. В общем случае, понятие сложности учитывает как сложность структуры системы, так и сложность функций, реализуемых системой.

Потенциально опасные объекты (ПОО) относятся к классу структурно-сложных систем, которые при математическом описании не сводятся к последовательным, параллельным или древовидным структурам. Характерным примером ПОО являются современные компьютерные сети административного и ведомственного назначения, подверженные программно-информационным воздействиям (кибератакам) со стороны террористических организаций [1]. Поскольку единственным практически реальным и доступным путем проектирования и исследования структурно-сложных систем является моделирование, для оценки безопасности ПОО, в связи с невозможностью проведения полноценных экспериментов, единственным выходом является проигрывание всех возможных вариантов развития аварийной ситуации на математических моделях. Это, в свою очередь, предполагает необходимость разработки соответствующего математического обеспечения, базирующегося на современной теории и апробированных аналитических методах.

Кроме трудностей математического характера, следует выделить и трудности творческого характера, связанные с ПОО. Дело в том, что

лишь незначительная часть систем имеет явно выраженную структуру. Для подавляющего большинства ПОО возможные сценарии перехода любой системы в опасное состояние требуют умозрительного структурирования, что не всегда просто сделать.

Анализ причин и хода развития происшедших аварий показывает, что независимо от времени, типа производств и региона они подчиняются определенным закономерностям.

Как правило, аварии предшествует фаза накопления каких-либо дефектов в оборудовании или отклонений от номинальных процедур ведения процесса. Длительность этой фазы может измеряться минутами или годами. Сами по себе указанные дефекты и отклонения еще не представляют угрозы, но в критический момент, при наступлении инициирующего (неожиданного, редкого) события, в результате которого система попадает в опасное состояние, наносящее ущерб, они играют роковую роль.

При этом в проблеме безопасности на первый план выходят не учитываемые в теории надежности компоненты, а именно: среда, в которой функционирует система; защитные сооружения; неблагоприятные внешние воздействия; умышленные (или безответственные) действия людей.

В историческом плане под надежностью первоначально понимали только безотказность (*reliability*) — свойство системы сохранять работоспособность (т. е. не иметь отказов) в течение определенного времени при нормальных условиях эксплуатации. Под безопасностью (*safety*) в настоящее время понимается способность системы функционировать, не переходя в опасное состояние [3].

При проектировании и разработке методов аудита безопасности и алгоритмов управления состоянием ПОО необходимо тщательно и конкретно рассмотреть все множество опасных состояний и логику их возникновения. Иначе говоря, необходимо точно знать, как и при каких условиях могут возникнуть разрушительные последствия. Это позволит, с одной стороны, заблаговременно выработать и принять соответствующие меры защиты, а с другой — разработать безопасный алгоритм управления этой системой.

При анализе безопасности ПОО в случаях возникновения аварий и катастроф с серьезными последствиями целесообразно учитывать не только стандартные (проектные) условия их функционирования, но и возможность нестандартных (запроектных) разрушающих воздействий и грубых (непреднамеренных и сознательных) нарушений правил их эксплуатации.

3. Метод анализа безопасности. Основной целью анализа безопасности является уменьшение вероятности аварий и связанных с ними несчастных случаев, человеческих жертв, экономических потерь и нарушений в окружающей среде.

За последние десятилетия методы анализа безопасности, риска и надежности сложных систем получили широкое развитие. Одним из таких методов является структурно-логический метод, получивший название метода "дерева событий". Ценность данного метода определяется следующими факторами:

1) возможностью глубоко анализировать количественные и качественные аспекты безопасности и надёжности;

2) возможностью выбора правильных управленческих решений при оценке ситуаций с помощью модели “дерева решений”;

3) получением графически наглядного материала для практического руководства по обеспечению безопасности и т.д.

Применение данного метода предполагает, что система состоит из таких элементов, как единицы оборудования, материалы, персонал, которые находятся в определенной окружающей и социальной среде и подвержены старению. Опасные состояния вызываются одним или несколькими элементами и приводят к отказам в системе. Окружающая среда, персонал и старение могут влиять на систему только через ее элементы (рисунок 1).

Рис.1. Факторы и формы воздействия на систему

Каждый элемент может быть связан с другими элементами специфическим образом, поэтому надо уточнить взаимосвязи и топологию системы. Эти связи можно представить наилучшим образом в виде принципиальной схемы системы.

Отказы элементов являются основополагающими данными при анализе причинных связей. Они классифицируются на первичные отказы, вторичные и ошибочные команды.

Первичный отказ — это нерабочее состояние элемента, вызванное естественным старением.

Вторичный отказ определяется воздействием избыточных напряжений на элементы. Избыточные напряжения вызываются окружающей средой, людьми, различными источниками энергии. Примером вторичного отказа в компьютерной сети может служить реализация программной атаки класса *DoS*.

Ошибочные команды представляются в виде элемента, находящегося в нерабочем состоянии из-за неправильного сигнала управления или помехи. Примером ошибочной команды в компьютерной сети может служить неправильная настройка межсетевого экрана или антивирусной программы.

При анализе причинных связей с помощью «дерева событий» существует два подхода: прямой анализ и анализ с обратным порядком. Чтобы отыскать и наглядно представить причинную взаимосвязь, необходимы элементарные блоки, подразделяющие и связывающие большое число событий. С этой целью используются два типа блоков: символы событий и логические символы[2,4].

Процедура построения «дерева событий» сводится к следующему ряду последовательных действий:

1) анализ начинается с четкого определения конечного события;

2) конечное событие детализируется с точным определением причин и использованием логических знаков до событий, которые классифицируются как «состояния элементов», обеспечивающих реализацию предшествующих (последующих) событий;

3) разработка завершается, когда нет возможности отыскать новые «состояния элементов» (при этом не обеспечиваемые другими «состояниями элементов» события являются исходными или инициирующими).

Процедура построения «дерева событий» подразумевает, что процессы во времени не рассматриваются, и «дерево событий» является «мгновенным снимком» системы в момент *t*.

При анализе событий и построении "дерева событий" можно воспользоваться следующими понятиями формальной логики. Входные события логической операции “И” должны в совокупности обуславливать появление выходного события. Входные события для операции “ИЛИ” должны формулироваться так, чтобы они вместе исчерпывали все возможные пути появления выходного события.

Вначале исследуются причины, приводящие к появлению событий. Если имеется несколько причин, которые должны появиться одновременно, то используется операция “И”. С другой стороны, если любая из причин приводит к появлению выходного события, следует использовать операцию “ИЛИ”.

Вероятность появления независимых исходных событий можно рассчитать по формулам:

1) для логической связи "И"

$$P = \prod_{i=1}^{n} q_i \; ; \qquad (1)$$

2) для логической связи "ИЛИ"

$$P = 1 - \prod_{i=1}^{n} (1 - q_i) \, , \qquad (2)$$

где n — число событий; q_i — вероятность i–го события.

“Дерево событий” позволяет получить и интерпретировать качественные и количественные результаты в соответствии с целями анализа, например, осуществлять проверку достижения необходимого уровня безопасности всей системы.

В случае несоответствия системы заданному уровню безопасности определяют элемент системы, имеющий наибольшее влияние на вероятность наступления события.

Каждое головное событие анализируемого дерева представляет собой аварию или несчастный случай, серьезность которых определяется катастрофичностью последствий (величиной ущерба – потерь).

Ожидаемые потери при появлении головного события могут быть рассчитаны по формуле

$$E = \sum_{i=1}^{N} P_i U_i \, , \qquad (3)$$

где P_i — вероятность появления последствий i-го класса при проявлении головного события; N — число классов последствий

различной серьезности; U_i — потери, связанные с i–м классом последствий.

Приведенное выражение не определяет абсолютную меру потерь и справедливо только при проявлении головного события. Следовательно, величина E может рассматриваться как ожидаемые потери при аварии или несчастном случае. Значения U_i могут выражаться в деньгах, потерянных рабочих днях и т.д.

Другим способом определения величины E может быть учет реальных потерь в прошлом. Пусть, например, потери выражаются в потерянных рабочих днях. Предположим, что в n прошедших проявлениях головного события потери составляли U_1, U_2, …, U_n. Ожидаемые потери можно оценить по среднему арифметическому известных потерь:

$$E = \frac{\sum_{i=1}^{n} U_i}{n}. \qquad (4)$$

Можно показать, что фактически выражения (3) и (4) эквивалентны, если считать, что n равно числу классов последствий N, а вероятности проявления последствий различных классов равны между собой ($p_i = 1/n$). Это происходит, когда мы рассматриваем каждую аварию или несчастный случай как отдельную ситуацию.

Величина E, задаваемая формулами (3) и (4), показывает, каких потерь можно ожидать при аварии или несчастном случае, но она никак не связана с затратами на обеспечение безопасности. Чтобы их учесть, надо рассмотреть еще несколько важных факторов. Один из них — частота, с которой происходят аварии. При использовании дерева событий она выражается в терминах вероятностей (P).

Величины E и P являются абсолютными мерами «критичности» данного головного события, выражаемой в виде:

$$C = PE, \qquad (5)$$

где C — ожидаемые потери, связанные с проявлением головного события в течение данного интервала времени или с данной единицей трудоемкости.

Данный подход позволяет осуществлять:

проведение анализа для поиска нежелательного события дедуктивным методом;

поиск важнейших аспектов системы, влияющих на осуществление нежелательного события;

графическую интерпретацию, дающую наглядное представление об изменениях в системе;

выбор качественного или количественного метода анализа;

концентрацию усилий на анализе определенного вида событий (отказа);

проведение анализа в соответствии с реальными изменениями в системе.

Полученный при построении «дерева событий» графический материал может быть использован неоднократно, например, в качестве схемы для определения возможного нежелательного события.

«Дерево событий» позволяет получить и интерпретировать качественные результаты в зависимости от целей анализа, например, для проверки достижения необходимого уровня безопасности всей системы, определяемого вероятностью появления нежелательного события. В случае несоответствия системы данному уровню безопасности определяют элемент системы, имеющий наибольшее влияние на вероятность наступления нежелательного события. В «дерево событий» можно вводить ограничения, требования к конструкции, экономические параметры и т.п.

Построение «дерева событий» производят с учетом всех событий, его вызывающих, вниз от корневого события, представляющего собой нежелательное событие в системе. Построение заканчивается показом «первичных событий». Таким образом, наступление корневого события возможно при логическом взаимодействии «первичных событий», что устанавливается с помощью операций «И» и «ИЛИ».

Большой интерес представляют минимальные критические комбинации (пути) (МКК) базисных событий, набор которых не может быть сокращен без гарантии наступления корневого события. Выявление МКК является полезным при определении слабых мест в системе. Полный набор всех МКК является необходимым и достаточным условием наступления корневого события. Большой интерес представляет также нахождение минимальных, не совершающихся критических комбинаций событий (МНКК). Полный набор МНКК — это набор базисных элементов, не наступление которых гарантирует не наступление корневых событий.

Таким образом, качественный анализ системы представляет собой последовательность следующих операций:

1) определение корневого события;

2) изучение элементов системы и их взаимосвязи;

3) построение «дерева событий»;

4) запись соответствующей функции алгебры логики (ФАЛ) на основании построенного «дерева»;

5) преобразование ФАЛ к виду дизъюнктивной нормальной формы, т. е. к логической сумме логических произведений;

6) минимизация ФАЛ (т.е. ее упрощение с целью получения возможно меньшего числа членов возможно меньшей длины).

Конъюнкции минимизированной ФАЛ и являются МКК, т.е. наиболее простым вариантом реализации корневого события «дерева». Затем, при необходимости, определяют МНКК, последовательно исследуя влияние каждого из первичных событий и их конъюнкции на значения ФАЛ. В том случае, если при значении базисного события или его конъюнкции равном нулю, значение ФАЛ также равно нулю, то это событие (минимальная конъюнкция) является МНКК[2].

В настоящее время при анализе безопасности все большее внимание уделяется так называемой концепции «приемлемого риска». Под измерением риска принято понимать получение количественной оценки масштабов конкретной опасности, исходящей от системы. Эта количественная оценка риска представляет собой, как правило, определение математического ожидания случайной величины ущерба, возможных жертв, потерь, разрушений, вредных выбросов и т. п., связанных с нарушением функционирования, отказами или авариями систем. При этом предполагается, что заранее промоделированы и рассчитаны показатели E ущерба (объемы разрушений, радиоактивных выбросов, человеческих жертв, стоимость потерь и т.п.) для различных возможных уровней аварий (опасностей).

В данном случае вместо критерия работоспособности должен быть сформулирован логический критерий условий возникновения аварии любого из заданных уровней:

$$Y_c = \bigvee_{j=1}^{n} Y_{A_j}, \qquad (6)$$

где Y_{A_j} — логический критерий условия появления аварии j-го уровня.

Вероятность P_c реализации этого критерия определяет искомую вероятность аварии. Ущерб может быть определен по методике анализа эффективности качественно сложных систем. Однако критерием в данном случае является правило вычисления математического ожидания ущерба от аварий заданных уровней:

$$W_c = \sum_{j=1}^{n} E_j P(Y_{A_j}). \qquad (7)$$

Непосредственное управление безопасностью основывается на оперативном построении текущих вероятностных и детерминированных структурно-логических моделей нахождения системы в безопасных, предопасных (критичных) и опасных (аварийных) состояниях. На рис.2 представлен пример распределения (и количество $M_1 + M_2 + M_3 = V$) состояний системы из 9 элементов, вероятности пребывания системы в этих состояниях $P(Y_i)$ и число возможных путей перехода из начального состояния исправности (*nst*) в другие состояния различных областей[5].

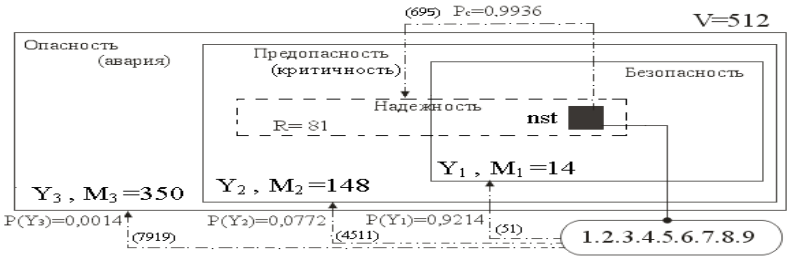

Рис.2. Факторы и формы воздействия на систему

Фактически это означает организацию в реальном масштабе времени формирования моделей текущих сценариев вариантов возможного возникновения и развития аварийных ситуаций, непосредственно определяемых в моменты изменения структуры системы и ее текущего состояния. Это позволяет повысить точность прогнозирования и оптимизации текущей безопасности системы по критериям минимизации возможности ее перехода из текущего в предопасные и аварийные состояния.

4. Заключение. Одновременно, основываясь на анализе выделенных логических функций переходов из текущего состояния, можно реализовать непосредственное детерминированное управление безопасностью. Оно выражается, например, в точном определении (на текущий момент времени) наиболее опасных элементов системы, отказы или поражения которых сразу приводят к аварии. Также могут прогнозироваться последствия планируемых решений или действий операторов и исключаться те из них, которые являются опасными или катастрофичными.

Это означает, что любое изменение состояния одного элемента x_i системы сразу проявляется в изменении ее текущего состояния. Оно, в свою очередь, сразу предполагает оперативное построение новых

моделей безопасных, предопасных и опасных (аварийных) переходов состояний системы. Данные модели теперь, уже с учетом нового (текущего) состояния, точно и однозначно указывают — в какое конкретное следующее состояние (безопасности, предопасности или опасности) может перейти система при изменении состояния ее элемента x_i. Это является детерминированной прогностической информацией для непосредственного управления безопасностью системы в процессе ее функционирования (например, запрещения действий, переводящих ее в опасные и аварийные состояния).

Одновременно эти данные могут служить основой более глубокого сценарного анализа безопасности сложившейся ситуации или текущей обстановки, включая прогнозирование развитие событий; определение пороговых значений критериальных (индикативных) показателей безопасности и эффективных мер по предотвращению угроз, организацию мониторинга за развитием ситуаций и создание информационной базы анализа устойчивости ПОО.

Литература

1. *Котенко И.В., Саенко И.Б., Юсупов Р.М.* Аналитический обзор докладов Международного семинара "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2010) // Труды СПИИРАН, Выпуск 13. СПб.: Наука, 2010. ISBN 978-5-02-025507-4.
2. *Белов П.Г.* Теоретические основы системной инженерии безопасности. — Киев: КМУГА, 1997. — 426 с.
3. *Рябинин И.А.* Надежность и безопасность сложных систем. — СПб.: Политехника, 2000. — 248 с.
4. *Э.Дж. Хенли, Х. Кумамото.* Надежность технических систем и оценка риска. — М.: Машиностроение, 1984. — 528 с.
5. *Можаев А.С., Синещук Ю.И.* Методологические основы информационной технологии моделирования систем и средств автоматизации управления ВМФ. — СПб. ВМИРЭ, 2009. — 222 с.

Синещук Юрий Иванович — д-р техн.наук, проф.; профессор Санкт-Петербургского университета Государственной противопожарной службы МЧС России. Область научных интересов: автоматизация процессов управления, качество и безопасность сложных организационно-технических систем, теория моделирования. Число научных публикаций — 111. sinegal@rambler.ru; СПбУГПС МЧС России, Московский проспект, 149. Санкт-Петербург, 196105, РФ; р.т. +7(812)388-99-63

Sineshchuk Yury Ivanovich — Ph.D., Doctor of Technical Sciences, professor; professor of Saint-Petersburg University of the State Fire Service Emergency of Russia. Research interests: automation of management processes, quality and safety of the complex organizational-technical systems, theory of modelling. The number of publications — 111. sinegal@rambler.ru; SPbU SFSER, Moskovsky prospect, 149, St. Petersburg, 196105, Russia; office phone. +7(812) 388-99-63.

Филиппов Александр Геннадьевич — преподаватель кафедры автоматики и сетевых технологий Санкт-Петербургского университета Государственной противопожарной службы МЧС России. Область научных интересов: автоматизация процессов управления, качество и безопасность сложных организационно-технических систем, теория моделирования. Число научных публикаций — 11. filippovag@inbox.ru; СПбУГПС МЧС России, Московский проспект, 149, Санкт-Петербург, 196105, РФ; р.т. +7(812) 388-99-63.

Philippov Alexandr Gennadyevich — lecturer of the department of automation and networking of Saint-Petersburg University of the State Fire Service Emergency of Russia. Research interests: automation of management processes, quality and safety of the complex organizational-technical systems, theory of modeling. The number of publications — 11. filippovag@inbox.ru; SPbU SFSER, Moskovsky prospect, 149, St. Petersburg, 196105, Russia; office phone. +7(812) 388-99-63.

Терехин Сергей Николаевич — канд.техн.наук, доцент; начальник кафедры автоматики и сетевых технологий Санкт-Петербургского университета Государственной противопожарной службы МЧС России. Область научных интересов: автоматизация процессов управления, качество и безопасность сложных организационно-технических систем. Число научных публикаций — 60. expert_terehin@inbox.ru; СПбУГПС МЧС России, Московский проспект, 149. Санкт-Петербург, 196105, РФ; р.т. +7(812) 388-99-63

Terehin Sergey Nikolaevich — PhD in Technical sciences, associate professor; chief of the department of automation and networking of Saint-Petersburg University of the State Fire Service Emergency of Russia. Research interests: automation of management processes, quality and safety of the complex organizational-technical systems. The number of publications — 60. expert_terehin@inbox.ru; SPbU SFSER, Moskovsky prospect, 149, St. Petersburg, 196105, Russia; office phone. +7(812) 388-99-63.

Николаев Денис Валерьевич — соискатель кафедры автоматики и сетевых технологий Санкт-Петербургского университета Государственной противопожарной службы МЧС России. Область научных интересов: автоматизация процессов управления, качество и безопасность сложных организационно-технических систем. Число научных публикаций — 6. nikolaev01@mail.ru; СПбУГПС МЧС России, Московский проспект, 149. Санкт-Петербург, 196105, РФ; р.т. +7(812) 388-99-63. Научный руководитель — Ю. И. Синещук.

Nikolaev Denis Valerjevich — competitor of the department of automation and networking of Saint-Petersburg University of the State Fire Service Emergency of Russia. Research interests: automation of management processes, quality and safety of the complex organizational-technical systems. The number of publications — 6. nikolaev01@mail.ru; SPbU SFSER, Moskovsky prospect, 149, St. Petersburg, 196105, Russia; office phone. +7(812) 388-99-63. Scientific adviser — Y.I. Sineshchuk.

Саенко Игорь Борисович — д-р техн.наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций — 220. ibsaen@mail.ru;

СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of laboratory of computer network security of Saint-Petersburg Institute for Information and Automation of RAS (SPIIRAS). Research interests: automated information systems, information security, processing and transfer of data on data links, theory of modeling and mathematical statistics, information theory. The number of publications — 220. ibsaen@mail.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн.наук, проф.
Статья поступила в редакцию 22.03.2011.

РЕФЕРАТ

Синещук Ю.И., Филиппов А.Г., Терехин С.Н., Николаев Д.В., Саенко И.Б. **Структурно-логический метод анализа безопасности потенциально опасных объектов.**

В статье авторами предлагается алгоритм проведения качественного анализа безопасности и надежности систем, технологических процессов, а также вероятного риска и возможных потерь, путем использования специального метода анализа, который направлен на уменьшение вероятности аварий и несчастных случаев, человеческих жертв и экономических потерь. Рассмотрены основные преимущества данного метода, его система и составные элементы, причины отказа составных элементов, предложена процедура построения данного метода, приведены формулы для расчетов.

Основной целью анализа безопасности является уменьшение вероятности аварий и связанных с ними несчастных случаев, человеческих жертв, экономических потерь и нарушений в окружающей среде.

Применение структурно-логического метода (метода "дерева событий") предполагает, что система состоит из таких элементов, как единицы оборудования, материалы, персонал, которые находятся в определенной окружающей и социальной среде и подвержены старению. Опасные состояния вызываются одним или несколькими элементами и приводят к отказам в системе. Окружающая среда, персонал и старение могут влиять на систему только через ее элементы.

Каждое головное событие анализируемого дерева представляет собой аварию или несчастный случай, серьезность которых определяется катастрофичностью последствий (величиной ущерба-потерь).

«Дерево событий» позволяет получить и интерпретировать качественные результаты в зависимости от целей анализа, направленного, например, на проверку достижения необходимого уровня безопасности всей системы, определяемого вероятностью появления нежелательного события. В случае несоответствия системы данному уровню безопасности определяют элемент системы, имеющий наибольшее влияние на вероятность наступления нежелательного события. В «дерево событий» можно вводить ограничения, требования к конструкции, экономические параметры и т.п.

Непосредственное управление безопасностью основывается на оперативном построении текущих вероятностных и детерминированных структурно-логических моделей нахождения системы в безопасных, предопасных (критичных) и опасных (аварийных) состояниях. Фактически это означает организацию в реальном масштабе времени формирования моделей текущих сценариев вариантов возможного возникновения и развития аварийных ситуаций, непосредственно определяемых в моменты изменения структуры системы и ее текущего состояния.

SUMMARY

Sineshchuk Y.I., Philippov A.G., Terehin S.N., Nikolaev D.V., Saenko I.B.
Structural-logical method of the safety analysis of the potentially dangerous objects.

In this paper authors propose the algorithm of carrying out of the qualitative analysis of safety and reliability of systems, technological processes, and also of probable risk and possible losses, by using of a special method of the analysis which is directed on reduction of probability of failures and accidents, human victims and economic losses. The basic advantages of the given method, its system and components, causes of failure of components are considered, procedure of construction of the given method is provided, formulas for calculations are presented.

The main purpose of safety analysis is to reduce the risk of accidents and related accidents, casualties, economic losses and disturbances in the environment.

The use of structural-logical method (the method of "event tree") suggests that the system consists of elements such as pieces of equipment, materials, personnel who are in a certain social environment are subjected to aging. Dangerous conditions caused by one or more elements lead to failures in the system. Environment, personnel and aging can affect the system only through its elements.

Each event in analyzed parent tree is an accident , the severity of which is determined by the catastrophic consequences (the damage-loss).

The "event tree" allow us to obtain and interpret high-quality results depending on the purpose of analysis, such as checking to achieve the necessary level of safety throughout the system and the probability of occurrence of undesirable events. In case of discrepancy of a given level of safety we define an element of the system which has the greatest influence on the likelihood of undesirable events. With the help of the "event tree" we can impose restrictions, construction requirements, economic parameters, etc.

Direct control of the safety is based on the current operational construction of probabilistic and deterministic structural and logical models aimed at estimation of system's safe, pre-hazardous (critical) and hazardous (emergency) conditions. Practically, this means the organization in real time the formation of models of current scenarios of possible options for the emergence and development of emergency situations, directly determined at the time of the restructuring of the system and its current state.