УДК 621.311:682.039

ОЦЕНКА БЕЗОПАСНОСТИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Н. К. Юрков

Введение

Во многих приложениях под термином системная безопасность понимается безопасность серверов, на которых хранится некая информация. Здесь под термином «системная безопасность» мы понимаем безопасность сложных систем произвольной сущности происхождения, в том числе и вычислительных, но далеко не только их.

Термин «теория катастроф», введенный Р. Томом для обозначения теории особенностей, теории бифуркаций и их приложений, связан с приложениями, в которых плавное изменение параметров способно привести к резкому, скачкообразному изменению состояния или режима движения системы.

Идентификация систем в теории управления – это определение структуры системы и ее параметров путем анализа входных и выходных данных системы. В то же время идентификация в промышленной безопасности – установление тождественности опасных производственных объектов.

В самом широком смысле под идентификацией предлагается понимать выработку точного языка описания реальности и соответствующих понятий и категорий, т.е. понятий крайне высокого, насколько это возможно, уровня. Сложность понятий – цена за простоту языка описания реальности, ее «законов» [1].

В каждый конкретный исторический период могут быть недостаточными ресурсы для получения с заданной точностью необходимого для решения практической проблемы описания реальности. Возникает необходимость использования присущих только человеку способностей в процессе управления. Более того, любая система либо непосредственно в явном виде содержит человеческий фактор, либо является элементом системы, которая содержит человеческий фактор. Так что любая эффективная методология идентификации должна включать процесс человеческого выбора, так как именно в результате него вырабатывается текущее управление процессом идентификации.

Системный анализ безопасности ограничивается выявлением факторов и обстоятельств, влияющих на появление аварий, катастроф, чрезвычайных ситуаций, других нештатных ситуаций, а также разработкой предупредительных мероприятий, снижающих вероятность их появления.

В задаче распознавания состояния безопасности сложных технических систем (СТС) наиболее точное решение может быть получено, если оно принимается на основе достаточного количества исходных данных. В большинстве практических задач все многообразие состояний СТС может быть сведено к нескольким классам, число которых невелико ввиду ограниченного набора действий, принимаемых в том или другом состоянии. В простейшем случае речь идет о двух состояниях СТС (опасное или не опасное, устойчивое или не устойчивое и т.д.). В подобных задачах проводится измерение каких-либо физических параметров, характеризующих состояние СТС, и классификация состояний СТС осуществляется по полученным значениям.

Рассмотрим информационные критерии эффективности и необходимости контроля для достижения требуемого уровня безопасности. До проведения операции контроля неопределенность состояния объекта контроля характеризуется априорной безусловной энтропией $H(\omega)$, где ω – состояние объекта контроля. После проведения операции контроля путем измерения значений одного или нескольких параметров x неопределенность состояния будет характеризоваться усредненной величиной – полной условной энтропией $\overline{H}(\omega|x)$. Разность этих величин

$$I = H(\omega) - \overline{H}(\omega|x) \qquad (1)$$

представляет собой количество информации, полученной в результате операции контроля, и может характеризовать качество метода или системы контроля. Здесь

$$H(\omega) = -\sum_{i=1}^{k} P(\omega_i) \log_n P(\omega_i), \tag{2}$$

где $P(\omega_i)$ – априорные вероятности состояний; k – число состояний; n – основание логарифма $(n = 2)$. Однако значение этой величины зависит от априорных вероятностей состояния объекта и основания логарифма при ее вычислении. Поэтому более предпочтительной является относительная величина – информационная эффективность

$$Э = \frac{H(\omega) - \overline{H}(\omega \mid x)}{H(\omega)}. \tag{3}$$

Она характеризует информационную эффективность параметров контроля и СТС в целом безотносительно к основанию логарифма. Значение величины Э изменяется в пределах от 0 до 1.

В случае двух состояний (устойчивое и неустойчивое) энтропия вычисляется по формуле

$$H(\omega_H) = -P(\omega_H) \log P(\omega_H) - P(\omega_y) \log P(\omega_y). \tag{4}$$

Полная условная энтропия $\overline{H(\omega \mid x)}$ определяется как

$$\overline{H(\omega \mid x) = \int_x p(x) H(\omega \mid x) =}$$

$$= -\int_x \{P(\omega_y) p(x \mid \omega_y) \log_2 \frac{P(\omega_y) p(x \mid \omega_y)}{p(x)} + P(\omega_H) p(x \mid \omega_H) \log_2 \frac{P(\omega_H) p(x \mid \omega_H)}{p(x)}\} dx. \tag{5}$$

Здесь $P(\omega_i)$ – априорные вероятности состояний ω_i; $P(x \mid \omega_i)$ – условные вероятности параметра контроля (одного или нескольких) в состоянии ω_i; $p(x)$ – плотность вероятности параметра (параметров) контроля x:

$$p(x) = \sum P(\omega_i) p(x \mid \omega_i); \tag{6}$$

$H(\omega \mid x)$ – частная условная энтропия:

$$H(\omega \mid x) = -\sum P(\omega_i \mid x) \log_2 P(\omega_i \mid x), \tag{7};$$

где апостериорные вероятности $P(x \mid \omega_i)$ вычисляются по формуле Байеса

$$P(\omega_i \mid x) = \frac{P(\omega_i) p(x \mid \omega_i)}{p(x)}. \tag{8}$$

Свойства СТС характеризуются необходимостью контроля, которая оценивается относительным недостатком информации, требуемой для надежного принятия решений. Показатель необходимости контроля

$$N = \frac{H(\omega)}{H(\omega)} - H_Д, \tag{9}$$

где $H_Д$ – допустимое значение энтропии, вычисляемое через допустимые вероятности состояний. Значения N изменяются в пределах от –∞ до 1. Положительные значения свидетельствуют о необходимости контроля, отрицательные – о его необязательности.

В случае двух состояний объекта (ω_y и ω_H) допустимая вероятность неустойчивого состояния может быть принята равной $P_Д(\omega_H)$ = 0,00135 из условия граничного значения, равного

трем среднеквадратическим отклонениям. В этом случае $H_{Д}$ = 0,0148 бит при измерении энтропии в двоичных единицах информации. Для соответствия выбранных параметров контроля требованиям, которые обусловлены объектом, следует выполнять условие

$$Э > N. \quad (10)$$

Расчет информационной эффективности, а также дальнейшие вычисления при определении состояния объекта с использованием критерия Байеса предусматривают использование условных плотностей вероятности параметров контроля, соответствующих различным состояниям объекта. Очень часто при построении условных плотностей вероятности используется нормальный закон распределения, что позволяет значительно упростить вычисления [2]. Параметр порядка называется информатором и после установления порядка информация сокращается, поэтому следует за признак безопасности принять минимум информации, циркулирующей в системе, так как по количеству информации можно судить о безопасности – даже информационный градиент позволяет судить о приближающейся катастрофе.

Согласно предложенному в [1] информационному критерию безопасности, безопасность достигает своего максимума только в том случае, когда все выполняемые элементарные операции (атомы), из которых состоит процесс как субъект безопасности, имеют минимальную вероятность сбоя, другими словами, находятся под постоянным контролем, что задается выбранной частотой контрольных операций.

Переход на катастрофический сценарий развития ситуации сродни бифуркациям (особенности или катастрофы), т.е. происходит переход количества в качество, переход в другой аттрактор, имеющий катастрофически низкий потенциальный (организационный, энергетический, информационный, затратный) уровень, в который скатывается высокоорганизованная система с поразительной скоростью. Идти вниз легче, чем подниматься в гору.

Таким образом, на концептуальном уровне необходимо предусмотреть меры, разрушающие рекуррентный алгоритм управления (построения) СТС (и не только технических, но и произвольных сложных систем).

На техническом уровне нельзя оценивать безопасность, как во многих современных приложениях, по временным характеристикам (например, по величине дисперсии промежутков между регламентными осмотрами и ремонтами), так как они (осмотры и ремонты) не обеспечивают отсутствие сбоев (в том числе и катастрофических) в работе системы. Так, в теории гарантированного управления эксплуатацией это положение вполне доказывается.

Если аттрактор рассматривать как устойчивое состояние системы, переход на которое сопровождается всплеском (резким увеличением) количества информации, а катастрофа – это самый нижний энергетический уровень (энтропийный) согласно законам термодинамики, при переходе на который не только не тратится, но даже выделяется большое количество энергии (той энергии, которая была затрачена на организацию среды существования СТС), то для обеспечения безопасности следует предотвратить бифуркацию как переход сложно организованной системы в новый аттрактор под воздействием случайного скачка. Для этого на концептуальном уровне следует установить буфер, способный вернуть систему в сбалансированное состояние, но этот буфер должен обладать другой (отличной) физической структурой, не должен описываться рекуррентной моделью, должен в момент времени появления внешнего толчка (внешней накачки, если сравнивать с лазерным излучением) поднять «энергетический» барьер, с тем, чтобы не допустить «туннельного перехода» системы из стабильного в катастрофическое состояние [3].

Только находясь под постоянным контролем, только погрузившись в облако электронных средств контроля, вездесущего и непобедимого, на подобии распространения на нашей планете плесени, которая за счет своего многообразия и всепроникновения непобедима, можно надеяться на обеспечение системной безопасности.

Современные электронные технологии позволяют приступить к осуществлению такой утопической мысли, каковой является мечта о безопасном мире. Используя «облачную терминологию», можно представить систему обеспечения глобальной безопасности так, как это сделано на рис. 1.

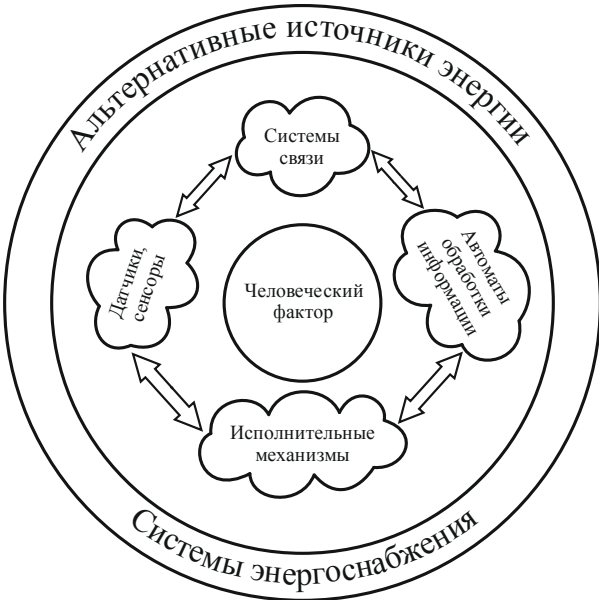

Рис. 1. Глобализация систем безопасности

Здесь всепроникающие источники энергии (в том числе и альтернативные) обеспечивают бесперебойное снабжение энергией. В центре системы (под неусыпной охраной) находится человеческий фактор как главный источник опасности, для защиты от которого подразумевается создание глобальных (мировых, всепроникающих) систем связи, сбора информации (содержат датчики, сенсоры), систем автоматической обработки информации, а также исполнительные механизмы.

Как нам видится ближайшее будущее, за счет глобализации развития электроники, в том числе и печатной, произойдет новый взрыв коммерческих применений электроники, расширяющий достигнутые границы контроля за ситуацией.

Автоматы обработки информации примут на себя основную нагрузку по выявлению потенциально опасных ситуаций и выработают управляющие воздействия на исполнительные механизмы.

Рассмотрим основные источники угроз. Как это не печально, но основным источником техногенных катастроф, по-прежнему, остается человеческий фактор. Конечно, непредсказуемый цунами может наделать великих бед, но, по сравнению с числовыми характеристиками катастроф, как это не кощунственно выглядит, природа занимает далеко не первое место в списке «организаторов» катастроф. По-прежнему, человек со своими слабостями порождает подавляющее большинство техногенных аварий, уносящих множество человеческих жизней и приносящих колоссальные убытки. В связи с этим позвольте сделать вывод о том, что главная цель глобальной безопасности – это устранение человеческого фактора из систем управления множественными катастрофосодержащими процессами.

Несмотря на это, не следует забывать, что основными процессами (элементами нештатных ситуаций, приводящих к катастрофам), контроль которых обеспечит системную безопасность, являются: болезнетворные микроорганизмы, химические вещества, газовые выделения, усталостные явления в материалах, алогичное поведение человека (психологические отклонения), климатические изменения, болезнь человека (физиологические изменения), симптомы старения, изменения в магнитных, гравитационных, электрических и других полях и т.д.

При решении задач обеспечения безопасности СТС риск от тяжелых аварий анализировался с нескольких точек зрения, таких как медико-биологические, экономико-экологические и глобально-социальные факторы с использованием понятия «приемлемый риск». Риск от тяжелых аварий определялся в виде [4] $R(P,C)=\sum_{i=1}^{k}P_iC_i$, где $A=(A_1,A_2,\ldots,A_k)$ – перечень событий, соответствующих тяжелым авариям; $P=(P_1,P_2,\ldots,P_k)$ и $C=(C_1,C_2,\ldots,C_k)$ – соответственно ве-

роятности и последствия указанных аварий; $R(P, C)$ должно стремиться к минимуму; естественно $R_{\min}(P, C) = R_0 \neq 0$ (R_0 – допустимый или приемлемый риск; $R > R_0$ определяет класс недопустимого риска).

Выбор приемлемого риска производился для общего случая, когда функции $P = P(q_1, q_2, \ldots, q_n, t)$, $C = C(c_1, c_2, \ldots, c_m, t)$ являлись неизвестными.

При составлении математической модели СТС, выборе и обосновании типа случайного процесса, адекватно описывающего его состояние, использовались марковские цепи, диффузионные процессы, ветвящиеся процессы, случайные процессы со стационарными приращениями и т.д. Для марковских процессов, задавая переходные вероятности с использованием уравнений Колмогорова–Смолуховского–Чепмена, получались нелинейные дифференциальные уравнения в частных производных относительно плотности распределения вероятностей для непрерывных случайных процессов или распределение для дискретных случайных величин. Последствие аварий отображает физико-химические изменения в окружающей среде и, как правило, находится из решений уравнений математической физики. На основе описания объекта и экологических последствий аварий получается операторное нелинейное уравнение

$$L(C, P) = R, \tag{12}$$

совпадающее по форме с уравнением теории упругости (R – внешняя нагрузка).

В рассматриваемом случае оно представимо в виде двух операторных уравнений

$$L_1(R, P, C) = P, \; L_2(R, P, C) = C. \tag{13}$$

При введении вектор-функции $X = (P, C)$ и нелинейного оператора A первое из них представится в виде операторного уравнения

$$A(R, X) = X. \tag{14}$$

Так как физико-химические изменения в окружающей среде должны соответствовать экологическим нормам, а вероятность возникновения аварий должна быть близка к нулю, то последнее уравнение имеет решение $X = 0$ при всех значениях риска R. При некоторых значениях R может иметь ненулевые решения, соответствующие скачкообразным изменениям (катастрофам) в экологической обстановке окружающей среды и изменению значений вероятностей аварий. Риск $R_{кр}$ назовем критическим, если при некоторых значениях R, близких к $R_{кр}$, это уравнение имеет малые ненулевые решения ($R_{кр}$ – точка бифуркации оператора $A(R, X)$). Таким образом, анализ безопасности СТС сводится к чисто математической задаче определения точек бифуркации $A(R, X)$, например, на основе линеаризации нелинейного оператора (отыскание точек бифуркации сводится к определению характеристических значений соответствующего линейного оператора). Каждое нечетно-кратное (в частности, простое характеристическое значение линейного оператора) является точкой бифуркации нелинейного оператора $A(R, X)$. Если характеристическое значение линейного оператора имеет четную кратность, то требуется дополнительный анализ, который сводится к конструированию так называемого поля вращения и доказательству его невырожденности. Определение точек бифуркации нелинейного оператора значительно сложнее. Упрощения возможны при известных функции последствиях аварий или вероятности распределения. Функция последствий аварий определяется в результате расчета технического состояния среды при чрезвычайной ситуации и необходимого времени ликвидации последствий аварий. При известном распределении вероятностей (или плотности распределения), построив случайный процесс, можно определить вероятности изменения состояния СТС во времени. Определяется значение критического риска $R_{кр}$, а далее – значение критического риска, для которого вероятность скачкообразного изменения технической обстановки (катастрофа) наибольшая. При этом наибольшая вероятность потери ее устойчивости (катастрофа) наступает при $R_{кр}$.

Отследить риски, контролировать изменения в вышеперечисленных процессах поистине невозможно на данном этапе развития техники. Но в настоящее время глобальный прорыв в решении этой проблемы видится в развитии так называемой органической и печатной электроники.

Прежде всего название «органическая и печатная электроника» вовсе не означает, что все используемые материалы являются органическими и наносятся они исключительно методами печати. На наш взгляд, достаточно удачны определения органической и печатной электроники, приведенные в википедии. Согласно им, печатная электроника – «совокупность печатных методов, используемых для создания электронных приборов». А органическая, или пластиковая, или полимерная электроника – «направление в электронике, основанное на применении проводящих полимеров, пластиков, органических соединений с низкой молекулярной массой (small molecular)» [5].

Таким образом, слова «органическая» и «печатная» характеризуют одно и то же направление в электронике, но по разным признакам: первое отражает преимущественный состав используемых материалов, а второе – преимущественную технологию нанесения материалов в процессе производства устройств. Основные преимущества органической электроники в сравнении с традиционной заключаются в меньшей стоимости изготовления устройств, их гибкости, применении более простых технологий изготовления, а также возможности изготовления изделий большой площади, что особенно актуально для экранов и систем освещения [2]. Вместе с тем на настоящем этапе развития органической электроники она не лишена ряда недостатков: низкого разрешения при печати (>5 мкм), низкой степени интеграции, низкой подвижности носителей заряда, ограничивающей диапазон рабочих частот. Так, при подвижности носителя заряда 0,5 $см^2/(В·с)$ максимальная рабочая частота составит 100 кГц.

Как правило, в органической электронике используются гибкие полимерные основания. Однако их использование создает ряд проблем. Гибкие основания обычно не полностью стабильны по размерам, что может существенно сказаться на разрешении и совмещении при печати рисунка. Кроме того, при воздействии высоких температур гибкие основания могут расплавиться, что ограничивает технологические возможности при производстве изделий органической электроники. В качестве гибких оснований в органической электронике наиболее широко применяются такие полиэфиры, как полиэтилентерефталат и полиэтиленнафталат; также могут использоваться полиимид, полипропилен, полилактид, циклоолефиновый сополимер, бумага и другие материалы.

Проводники необходимы практически во всех изделиях органической электроники. К проводникам предъявляется ряд требований, включающих низкое сопротивление, гладкость поверхности, химическую стойкость. Выделяют три группы материалов, используемых в органической электронике в качестве проводников: материалы на основе металлов; органические соединения; оксиды металлов.

Органические полупроводники используются в различных активных устройствах, причем многие из них могут быть нанесены из раствора, в том числе методами печати. В органической электронике в качестве полупроводников могут применяться следующие группы материалов: полимеры, например, политиофен; олигомеры, например, олиготиофены; органические соединения с низкой молекулярной массой, например, пентацен и его производные; углеродные нанотрубки; «гибридные» (органо-неорганические) материалы. Мобильность носителей заряда в органических полупроводниках сравнима с аморфным кремнием, но пока значительно ниже, чем в поликристаллическом кремнии. Ожидается, что в ближайшие несколько лет мобильность носителей заряда достигнет уровня поликристаллического кремния: сначала в лабораторных условиях, а потом и в серийно выпускаемых устройствах. Это станет возможным благодаря оптимизации органических соединений с низкой молекулярной массой и полимеров или использованию новых материалов, таких как углеродные нанотрубки или гибридные материалы. Большинство используемых сейчас органических полупроводников, в частности, пентацен и политиофен, относятся к полупроводникам *p*-типа, но полупроводники *n*-типа становятся более распространенными. Наличие полупроводников *p*- и *n*-типа позволяет реализовывать структуры типа КМОП, обладающие существенными преимуществами, в том числе меньшим энергопотреблением. Для производства изделий органической электроники может быть использована глубокая, флексографская, офсетная, трафаретная и струйная технологии печати, а также лазерная абляция.

На сегодняшний день очень успешно серийно выпускаются билеты, идентификационные карточки, солнечные батареи и другие изделия органической и печатной электроники. Конечно, по многим техническим характеристикам эти изделия уступают кремниевым аналогам: КПД солнечных батарей ниже, а объемы органической памяти и частота органического процессора несоизмеримо меньше. Тем не менее уникальные преимущества органической и печатной электрони-

ки, заключающиеся в низкой стоимости массового производства, гибкости и возможности изготовления изделий большой площади, а также высокие темпы совершенствования изделий открывают перед ней широкую область применения, ведь далеко не во всех устройствах нужны гигабайты памяти и гигагерцы частот. В самое последнее время появилась информация о создании в нашей стране дистанционных обнаружителей взрывчатых веществ, определении неадекватного поведения человека и др. Все это ведет к глобализации контроля, расширению его функций, добавляя в которые функции пресечения развития катастроф, мы получим «безопасное» существование человечества.

Таким образом, расширяя сферу применений электроники (в том числе и печатной) возможно достичь глобального контроля за ситуацией, ведь все катаклизмы предваряются какими-то ни было изменениями физических сред, зафиксировать, распознать и правильно интерпретировать которые и есть задача современной электроники.

Список литературы

1. Юрков, Н. К. Модели и алгоритмы управления интегрированными производственными комплексами : моногр. / Н. К. Юрков. – Пенза : Информационно-издательский центр ПГУ, 2003. – 198 с.
2. Юрков, Н. К. К проблеме обеспечения безопасности сложных систем / Н. К. Юрков // Надежность и качество – 2011 : тр. междунар. симп. : в 2 т. / под ред. Н. К. Юркова. – Пенза : Изд-во ПГУ, 2011. – Т. 1. – С. 104–106.
3. Тюрина, Л. А. Системная организация жизненного цикла промышленных изделий / Л. А. Тюрина, Н. К. Юрков // Тяжелое машиностроение. – 2006. – № 6. – С. 8–12.
4. Данилов, А. М. Системные методологии, идентификация систем и теория управления: промышленные и аэрокосмические приложения / А. М. Данилов, И. А. Гарькина, Э. В. Лапшин, Н. К. Юрков // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2009. – № 1. – С. 3–11.
5. Нисан, А. Органическая и печатная электроника – новая ветвь развития / А. Нисан // Поверхностный монтаж : инф. бюллетень ЗАО Предприятия ОСТЕК. – 2011. – № 4 (90). – С. 14–19.

УДК 621.311:682.039

Юрков, Н. К.

Оценка безопасности сложных технических систем / Н. К. Юрков // Надежность и качество сложных систем. – 2013. – № 2. – С. 15–21.

Юрков Николай Кондратьевич
доктор технических наук, профессор,
заведующий кафедрой,
кафедра конструирования
и производства радиоаппаратуры,
Пензенский государственный университет,
440026, г. Пенза, ул. Красная, 40.
(841-2) 56-43-46
E-mail: yurkov_NK@mail.ru

N. Yurkov
doctor of technical science, professor, the managing
of department construction and the production of radio equipment
Penza state university
440026, Penza, Red street, 40.
(841-2) 56-43-46
E-mail: yurkov_NK@mail.ru

Аннотация. Проводится анализ проблем обеспечения тотального контроля нештатных ситуаций, возникающий на начальных стадиях угроз безопасности. На базе информационного критерия безопасности предложено оценивать глобальный максимум по максимуму полезной информации. Показано, что приближение к локальному максимуму системной безопасности возможно лишь при глобализации систем контроля нештатных ситуаций, что может быть достигнуто даже при современном уровне развития электронной техники.

Ключевые слова: безопасность, сложная система, критерий безопасности, нештатные ситуации.

Abstract. Analyzes the problems of providing total control of emergency situations arising in the early stages of security threats. Based on the information criterion to assess the global security offered up to the maximum of useful information. It is shown that the approach to the local maximum system security is possible only if the globalization of control systems of emergency situations that can be achieved even at the present level of development of electronic technology.

Key words: security, complex system, the criterion of security, emergency situations.