Новые проблемы, методология и возможности сэйфеометрики

Безопасность является многопараметрическим свойством систем. С математической точки зрения безопасность может представлять функциональную зависимость от времени, характеристик системы, например количества систем безопасности, надежности, количества степеней опасности системы, степени автономности работы, в том числе от участия в ней человека.

Проводимая человеком качественная оценка ситуаций в сфере безопасности основана на интерпретации эмпирических, практических данных, извлечении из них полезной информации. Полученный на практике результат имеет неопределенность, может зависеть от квалификации интерпретатора, т.е. изначально зависит от наблюдателя, человеческого фактора. Несмотря на кажущуюся необъективность оценки уровня безопасности, можно выделить статистические закономерности, определить и исключить систематические закономерности и т.п. Неопределенность может объясняться разными причинами, а учесть и зафиксировать все факторы при оценке безопасности практически невозможно. Для получения достоверного результата надо принять вероятностную природу используемых для оценок в сфере безопасности величин.

Практические вопросы безопасности оперируют с эмпирическими данными, результатами наблюдений. Как и в хемометрике, в сэйфеометрике аналитические закономерности получаются с применением методов индукции и дедукции. При индукции от наблюдения переходят к идее, и от более конкретного — к более общему. Знания, полученные таким способом, будут носить вероятностный характер. При дедукции ситуация обратная. В сэйфеометрике большую роль играет наблюдение, которое обеспечивает нас информацией для постановки проблемы, задачи или гипотезы. При рассмотрении безопасности систем с различающимися параметрами может быть применен метод абдукции (делается редуктивный вывод, проводится извлечение вероятности из частных случаев).

Для начала оценки безопасности объекта надо определиться с набором измеряемых свойств или признаков. Многообразие этого набора будет формировать как возможности анализа, так и уровень его сложности.

Большинство величин в механике, термодинамике, электричестве, оптике могут быть измерены и оценены с помощью шкал физических величин, где имеются принятые эталоны и масштабы. В сэйфеометрике применение различных шкал и масштабов зависит от имеющейся в распоряжении совокупности данных и их статистики. Чем меньше в нашем распоряжении информации, тем шкала является более классификационной, ранговой (например, ключевые показатели эффективности — KPI от англ. Key Performance Indicators), интервальной и относительной. С увеличением количества данных шкала может приближаться с долей условности к абсолютной (для широкого диапазона комбинаций зависимостей для конкретной промышленной установки, когда можно говорить, что достигаемые разными путями уровни безопасности могут считаться квазиэквивалентными).

Измерения бывают прямые и косвенные. Прямые измерения в сфере безопасности используются для определения количественных значений физических величин параметрического поля данных на стыке с механикой, термодинамикой, электричеством, оптикой. В отличие от них количественные оценки в сфере безопасности, например вероятность, риск, надежность, основаны на косвенных измерениях. Используемые здесь в практике величины не имеют эталонов.

В основе использования конкретных методологических подходов лежат принятые для оценки гипотезы или предположения. Если результат последующего приближения выявленной закономерности является сомнительным, то это говорит о неадекватности принятой гипотезы.

Работа устройств и систем, рассматриваемых в целях определения их уровня безопасности, не является случайной. Время следует рассматривать, как величину из параметрического поля данных, которая является фактором или трендом процесса старения устройств и систем или их разрушения. Рассматриваемые вне параметрического поля данных величины в сэйфеометрике являются дискретными и обладают свойством эргодичности, а процессы их изменения в основном следует считать стационарными, эргодическими.

Распределения для дискретных событий, например совокупности систем, инспекций, нарушений и т.п., можно экстраполировать на непрерывное пространство событий для их лучшей интерпретации и понимания.

Увеличение потенциала безопасности и возможностей систем безопасности, будучи

непрерывным процессом, определяется экономическими затратами и рациональностью используемых подходов. В связи с этим предлагается постулировать концепцию достижения обоснованного *уровня приемлемой безопасности* $Q_{пр}$. Он находится вблизи *предельного достижимого уровня безопасности* Q_{MAX}, требующего существенных экономических затрат при достижении.

Изменение уровня безопасности объекта с течением времени зависит от его надежности. Уровень безопасности будет более стабильным для надежных объектов, чьи параметры, характеризующие функциональную работоспособность, будут находиться в проектных пределах более длительное время. Поэтому при анализе устаревания объекта усиливается роль исследования математических функций показателей надежности (безотказности и ремонтопригодности) на наличие экстремума, когда уровень безопасности будет изменяться. В информационном потоке отдельных данных для принятия решений важно не только проводить анализ неблагоприятных событий, но и иметь представление о фактическом уровне достигнутой безопасности и живучести системы.

При рассмотрении уровней безопасности оборудования связь функции риска неблагоприятных эффектов $p(t)$ с функцией состояния безопасности $q(t)$ можно получить с использованием теории вероятностей: $q(t) = 1 - p(t)$. Аналогичная связь используется в целях рассмотрения киберзащиты системы, где вводится понятие *индекс киберзащищенности* (Е.С. Альбицкая. Методы количественной оценки кибербезопасности на АЭС. Ч. 2. — Атомная техника за рубежом. — 2019. — № 3. — С. 14—24). При рассмотрении состояния оборудования в начальный момент времени значение $p(0)$ минимально, а величина $q(0)$ — максимальна. В ходе старения оборудования в момент времени t_c функция состояния безопасности достигает критического значения $q_{кр}$, что схематично показано на *рисунке 1*. На практике могут иметь место и другие закономерности, например, если есть притирка или приработка деталей, то в начальный период времени риск неблагоприятных эффектов $p(t)$ велик.

Как будет зависеть уровень безопасности $Q(N)$ от количества используемых систем безопасности (далее — СБ) N?

Для проведения оценки уровня безопасности всегда требуется тщательная постановка задачи и грамотная сортировка исходных данных, соответствующая алгоритму анализа данных. Среди СБ следует выделить простые и комплексные, пассивные и активные. Для рассмотрения надо построить последовательность систем от простых к комплексным, от пассивных к активным. Самой первичной и основной СБ является устройство отключения, которое может быть реализовано как выключатель, рубильник, блокировка, стопор и т.п. или может запускать обратный процесс. Это устройство является наиболее простым и эффективным. Его работа обеспечивает нейтральную или нулевую безопасность. Нередко неисправность такого конструктивно незначительного элемента может быть причиной серии отказов в оборудовании и системах, вызывать нестандартные ситуации в управлении.

Работа используемого по назначению устройства начинается после его включения. С этого момента эксплуатация устройства считается небезопасной. Устройство характеризуется опасностью для людей и окружающей среды. Аспекты опасности должны быть определены в зависимости от конкретной ситуации, и при рассмотрении они принимаются как *степени опасности*. Конкретное устройство будет характеризоваться определенной степенью опасности. Первая СБ — это элемент включения-выключения (кнопка выключения устройства), который определяет его нейтральную безопасность. Безопасность устройства увеличивается с увеличением количества применяемых СБ. Консервативно считаем, что одна СБ нейтрализует одну степень опасности, а СБ — черный ящик.

Принимая за основу концепцию достижения приемлемого уровня безопасности, функцию уровня безопасности определяем из уравнения $dQ = (\alpha \cdot dN)/N$, его решением будет функция типа $Q(N) = a + \alpha \cdot lnN$, где a и α — коэффициенты.

Анализ графиков на *рисунке 2* при $\alpha_1 > \alpha_2$, $a = 0$ и эквивалентными СБ позволяет сделать следующие выводы:

1. Все устройства имеют элемент безопасности или СБ для перехода устройства в состояние нейтральной безопасности, когда $N = 1 \rightarrow Q = 0$.

2. Уровень безопасности более простых устройств с α_1 при увеличении количества используемых СБ повышается быстрее, чем уровень безопасности для более сложных с α_2.

3. Простое устройство, работающее только в зоне I (зона небезопасной эксплуатации) можно считать примитивным, например, имеет только состояния «вкл/выкл». Такое устройство имеет два состояния безопасности и является не интеллектуальным, т.к. для него не устанавливается $Q_{пр}$.

4. Более сложное устройство в зоне II (зона безопасной эксплуатации) может иметь более двух состояний безопасности из-за наличия $Q_{пр}$ и является интеллектуальным, т.к. требуется сравнение текущего уровня Q с $Q_{пр}$. В зоне I уровень безопасности более интеллектуального устройства выше, чем у менее интеллектуального, на основании проектных решений ему присуще свойство внутренней безопасности или самозащищенности.

5. Более простое устройство достигает $Q_{пр}$ раньше, чем более сложное, т.е. ему не требуется большое количество СБ. Высокотехнологическое

устройство является более опасным и требует большего количества СБ.

В целом рисунок 2 показывает то, что более простым устройствам при эксплуатации обоснованно требуется уделять меньше внимания со стороны оператора или автоматики, чем комплексным. Сделанные выводы не противоречат данным наблюдений.

На рисунке 2 показаны элементы логики работы примитивного и интеллектуального устройств. Анализ элементарного логического устройства базируется на работе электронного триггера с состояниями логическая единица «1» и логический нуль «0». Логика простого устройства — бинарная, тут имеется два состояния объекта (зона I), что структурно соответствует элементу включения-выключения. Однако в сложных системах требуется и такая оценка ситуаций, как ни «1» — ни «0». Логика интеллектуального устройства не бинарная, количество состояний объекта больше двух (зона II), например три, для описания состояния которой удобно использование троичной симметричной системы счисления. В свою очередь, уже известно преимущество троичной системы перед двоичной (D.E. Knuth, The Art of Computer Programming. — Vol. 2: Seminumerical Algorithms. — Pp. 190—192. Addison-Wesley. — 2nd ed. — 1980).

Подходы сэйфеометрики интеллектуализируют работу человека с большими массивами и наборами данных, позволяют открывать скрытые и неочевидные закономерности, предлагают дополнительные варианты рассмотрения вопросов, облегчают работу, могут использоваться при управлении автономными системами.

Применение методологии и алгоритмов количественной оценки безопасности в сфере искусственного интеллекта основано на уже выявленных закономерностях. Некоторые из них могут носить абдукционный характер, когда проявляются эмпирические законы и связи при наблюдении свойств и отношений. «Творческие» возможности робота базируются на переборе комбинаций случаев и вариантов с учетом критериев приемлемости, заложенных человеком или алгоритмически определенных в ходе работы. Быстродействие электроники определяет его «творческий», аналитический потенциал.

Очевидно, что сам робот способен только увеличить или уменьшить количество поступающих от физических датчиков к нему сигналов или событий для последующего рассмотрения. Этот массив данных определяется возможностями входного канала оборудования. Однако робот не может определить критерии приемлемости при анализе данных. Это делает человек, закладывая алгоритмы обработки информации в управление оборудованием для работы автоматики.

В ряде случаев требуется постоянная оценка приемлемости ситуации. Необходимые условия часто определяются рамочными или пороговыми значениями параметров системы. Анализ достаточных условий безопасной эксплуатации является более сложным и требует оценки комбинаций факторов. Тут и следует применять подходы сэйфеометрики как инструмента для селекции информации.

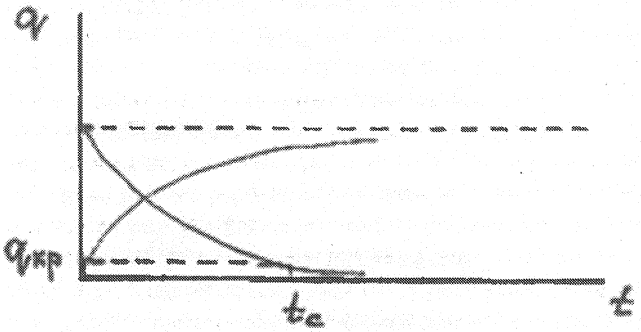

Рис. 1

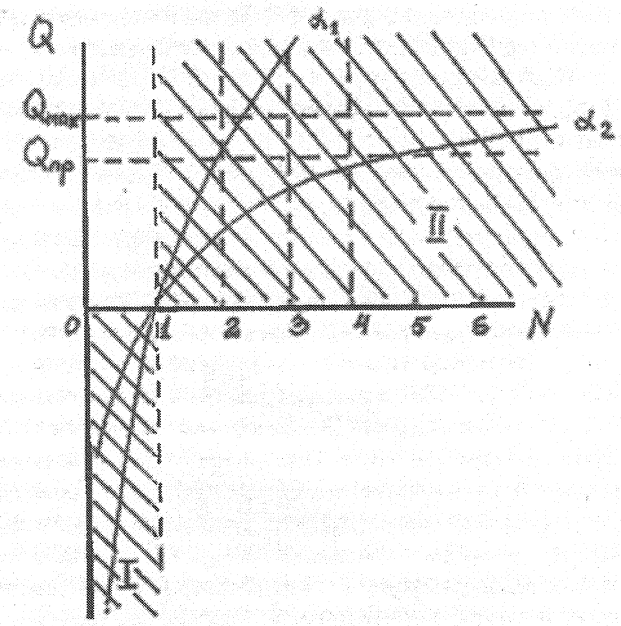

Рис. 2

Дмитрий ЛОБАЧ,
кандидат технических наук, главный специалист отдела науки и информации Госатомнадзора