УДК [002:004.056]:681.51/.54

Г. А. Попов, Е. А. Попова, А. В. Мельников

АНАЛИЗ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ УТОЧНЕННЫХ ЭКСПЕРТНЫХ ОЦЕНОК

Проведен анализ возможностей использования экспертных методов оценки параметров информационной безопасности сложных систем, к числу наиболее важных представителей которых относятся автоматизированные системы управления (АСУ). Показано, что применительно к оценке параметров информационной безопасности, и в частности рисков, наиболее приемлемыми методами оценки являются экспертные. При этом возможны два диаметрально противоположных подхода к оценке: при первом подходе оцениваются показатели безопасности глобальных компонентов автоматизированной системы, при втором – отдельные типовые элементы АСУ, а затем находятся интегрированные оценки на основе структурных взаимосвязей этих элементов. Обосновывается целесообразность использования второго подхода, поскольку он обеспечивает более высокую точность оценки. Однако этот подход существенно более трудоемок, опирается на большой набор оценочных данных, значительная часть которых получается экспертным путем. Ввиду обилия экспертных оценок, включающих субъективные искажения, предлагается процедура корректировки этих данных на основе функций преобразования. Предложены две подобные функции: одна сформирована на основе функции желательности Харрингтона, вторая – на основе полиномиальной экстраполяции по шкале Харрингтона. Показано, что последняя функция имеет ряд достоинств по сравнению с первой.

Ключевые слова: экспертные оценки, информационная безопасность, автоматизированные системы, шкала Харрингтона, функция корректировки оценок.

Введение

Проблема оценки безопасности автоматизированных систем, в силу принятых в настоящее время воззрений и подходов, заключается в оценке соответствующих рисков, что сводится к оценке параметров различных значимых угроз информационной безопасности этих систем, а также средних потерь при реализации этих угроз. В свою очередь, оценка параметров указанных характеристик безопасности является в общем случае крайне сложной. Применительно к автоматизированным системам данная проблема еще больше обостряется ввиду большой сложности и слабой структурированности этих систем. Нами анализируется возможность применения различных классов методов для решения проблемы оценки рисков информационной безопасности, исследуются некоторые недостатки использования экспертных методов для оценки параметров сложных систем, типичным представителем которых являются автоматизированные системы. Работ по использованию экспертных методов применительно к оценке параметров сложных систем достаточно много (см. например, [1, 2]). Публикаций по разработке методов и процедур «подправки» этих оценок с учетом искажений, присущих субъективной природе этих оценок, найти не удалось.

I. Общая процедура оценки параметров информационной безопасности автоматизированных систем на основе экспертных методов

Можно выделить два маргинальных подхода к экспертной оценке параметров сложных систем.

1. Непосредственная оценка параметров всего объекта (например, автоматизированной системы) целиком. Однако при таком подходе степень субъективизма экспертной оценки очень высока, что существенно снижает качество конечного результата. Кроме того, при данном подходе численное оценивание параметров (по абсолютной или относительной шкале) для эксперта крайне затруднительно, и поэтому используются методы, требующие от эксперта менее строгую информацию, в частности методы ранжирования, парных сравнений, методы, использующие лингвистические переменные или нечеткие категории. В результате получаются экспертные данные, которые часто принципиально не могут обеспечить высокого качества конечных оценок.

2. Вначале строится взвешенный граф, описывающий технологическую взаимосвязь всех автономных компонентов системы; применительно к автоматизированной системе, при относительно полной ее иерархизации, в качестве компонент могут рассматриваться отдельные автономные устройства (датчиковые устройства, связанные со сбором первичных данных об объек-

те управления, отдельные компьютеры, периферийные устройства, элементы системы передачи данных, программные системы и т. п.), а сам граф обычно имеет иерархическую структуру. Затем численно оцениваются параметры безопасности каждого из компонентов (на основе экспертных или любых других методов) и полученные оценки поэтапно интегрируются в соответствии с их иерархической структурой до самого верхнего уровня. Конечные оценки и могут рассматриваться в качестве конечного результата. Эти оценки имеют ряд преимуществ по сравнению с оценками, получаемыми на основе предыдущего подхода: они обычно являются числовыми оценками, более стабильны, обеспечивают большую достоверность конечного результата, поскольку при интегрировании большого числа численных оценок субъективные отклонения оценок отдельных экспертов от абсолютного значения оцениваемого параметра взаимно нивелируются, взаимно уничтожаются, что повышает качество оценок. Однако при данном подходе требуется большой объем подготовительных работ для организации и проведения экспертизы, что делает данный подход сложнореализуемым. Использование современных сетевых технологий позволяет организовать дистанционное проведение искомой экспертной процедуры в любом режиме, удобном индивидуально каждому из экспертов. Кроме того, показатели информационной безопасности большинства из компонентов типовые, мало изменяются с течением времени, могут копироваться и тиражироваться после однократного привлечения экспертов для начальной оценки их параметров, что также при масштабном использовании данного подхода существенно уменьшает издержки и затраты, связанные с его реализацией.

Исходя из всего вышесказанного, можно сделать заключение, что на основе второго подхода могут быть получены более качественные конечные результаты и что в настоящее время созданы необходимые условия и предпосылки для его практической реализации.

Отметим также, что могут быть использованы смешанные подходы, когда часть показателей получают на основе оценки параметров отдельных глобальных компонентов автоматизированных систем управления (АСУ), а часть – на основе оценки параметров отдельных элементов с их последующей интеграцией. В этом случае могут быть обеспечены практически более приемлемые характеристики процесса оценивания и оценки качества конечного результата. Однако анализ способов формирования наиболее приемлемых вариантов сочетания обоих подходов требует самостоятельных исследований.

II. Анализ возможностей использования различных классов методов оценки параметров безопасности автоматизированных систем

Использование различных классов методов для оценки параметров рисков имеет свои особенности и недостатки. *Аналитические* методы приемлемы только для оценки параметров угроз природного и, частично, техногенного характера. Для наиболее важных типов угроз, связанных со злоумышленными действиями, использование аналитических методов крайне ограничено ввиду непредсказуемости, в общем случае, потенциальных действий злоумышленника. *Эвристические* методы оценок применительно к сфере информационной безопасности пока не дают требуемой точности результатов. Использование *статистических* методов для оценки параметров угроз также проблематично, поскольку практически крайне мало статистических данных, связанных со злоумышленным нарушением, что вызвано следующими причинами:

1. Злоумышленные нарушения происходят достаточно редко, поэтому требуются достаточно большие промежутки времени для того, чтобы собрать объем статистических данных, достаточный для проведения статистического анализа. Отметим, что за большие промежутки могут произойти достаточно значимые изменения в самом процессе обеспечения информационной безопасности, и это в значительной степени может обесценить собранные статистические данные.

2. Все стороны, участвующие в процессе злоумышленного нарушения информационной безопасности, обычно скрывают сведения по этому нарушению по следующим причинам. Злоумышленник скрывает, поскольку не желает потенциально навлечь на себя опасность наказания за свой поступок, а также с целью в дальнейшем, возможно, повторить подобные нарушения. Потерпевшая сторона скрывает, поскольку, во-первых, не желает подрывать имидж надежного и стабильного партнера, полностью контролирующего ситуацию в «своих стенах», а во-вторых, с целью не выдавать информацию о возможной уязвимости своей системы обеспечения информационной безопасности, а также о масштабах понесенных потерь.

3. Статистические методы обработки информации эффективны, когда исходные случайные события подчиняются определенным (вообще говоря, неизвестным) закономерностям. В случае же злонамеренных нарушений в общем случае подобных закономерностей нет.

По причинам, перечисленным выше, в настоящее время наиболее приемлемыми методами оценки параметров угроз являются экспертные методы. Однако их применение для оценок параметров рисков связано с рядом проблем.

Основными обобщенными параметрами, характеризующими любую угрозу, являются вероятность нарушения информационной безопасности за заданный регламентный период и средняя величина ожидаемого ущерба в случае нарушения информационной безопасности угрозой заданного типа. Наиболее затруднительна оценка ожидаемого ущерба, поскольку конечная величина ущерба складывается из многих составляющих (непосредственные потери, связанные с нарушением, издержки, связанные с закрытием канала проникновения угрозы и ликвидации последствий происшедшей угрозы, включая подрыв престижа, использование похищенной информации в конкурентной борьбе и др.). Однако для одной из наиболее важных проблем обеспечения информационной безопасности – проблемы формирования политики безопасности – важны не абсолютные величины ущерба, а соотношения между ущербами для различных типов угроз и для разных элементов и объектов системы. Вследствие этого для выработки политики безопасности достаточно иметь относительные оценки величин ожидаемого ущерба, которые могут быть получены, в частности, на основе экспертных методов.

Как было показано в разделе I, процедура оценки рисков информационной безопасности в автоматизированных системах является, вообще говоря, иерархической, на самом нижнем уровне которой необходимо оценить параметры рисков простых типовых компонентов. Для оценки вероятности нарушения информационной безопасности в типовых компонентах наиболее удобны прямые экспертные методы. Применительно к рассматриваемой задаче можно задаться определенной шкалой оценок (например, от 0 до 100), описывающей относительные значения искомой вероятности либо предполагаемую частоту успешности нарушения безопасности данного объекта при заданном числе попыток. В качестве результирующей оценки вероятности берется среднее арифметическое значение оценок, которое усредняется по всем экспертам. Степень согласованности мнений экспертов оценивается на основе вычисления отклонения результатов экспертизы от идеального случая, когда мнения всех экспертов полностью совпадают. Для того чтобы величина отклонения находилась в пределах от 0 до 1, ее делят на максимальное значение этого отклонения. В результате получается число, называемой коэффициентом конкордации.

Для оценки средних потерь чаще всего используются лингвистические оценки с их последующим преобразованием в числовые оценки на основе определенной шкалы. Очень часто для этих целей используется шкала Харрингтона, в которой шкала возможных лингвистических оценок состоит из пяти значений: очень низкий (ОН) уровень, низкий (Н), средний (С), высокий (В), очень высокий (ОВ), которым сопоставляются интервальные оценки соответственно [0; 0,2), [0,2; 0,37), [0,37; 0,63), [0,63; 0,8) и [0,8; 1].

Шкала Харрингтона по существу отражает характер искажений экспертных оценок, порожденных их субъективным характером. Если бы экспертные оценки не страдали указанным недостатком, то следовало бы перечисленным выше лингвистическим оценкам сопоставить интервалы одинаковой длины, т. е. соответственно интервалы [0; 0,2), [0,2; 0,4), [0,4; 0,6), [0,6; 0,8), [0,8; 1]. Таким образом, шкала Харрингтона позволяет описать функцию, описывающую численно искажения оценок ввиду их субъективного характера. Мы выдвигаем предположение, что подобным искажениям должны подвергаться не только лингвистические оценки, но и все другие виды оценок, в том числе и **числовые**, и поэтому числовые оценки также нуждаются в уточнении, точнее, в корректировке, исключающей (точнее, минимизирующей) субъективные искажения этих оценок. Таким образом, для повышения качества экспертных оценок, особенно в иерархических схемах их интеграции, описанных в разделе I, целесообразно «подправить» каждую оценку, по возможности уменьшив субъективные искажения.

Подправку оценок предлагается осуществить путем преобразования исходных оценок на основе некоторой функции – функции корректировки оценок. Функцию корректировки можно построить прежде всего на основе функции желательности Харрингтона $H(x) = \exp(-\exp(-x))$, которая тесно связана с выбором приведенных выше концов интервалов в шкале Харрингтона [3]. Функция Харрингтона описывает, в какой мере результат эксперимента, наблюдения или оценки желателен для заинтересованного в этом результате субъекта при позитивном восприятии параметра оценки (т. е. чем больше значение параметра, тем он более желателен). Тогда искомая функция корректировки является функцией, обратной по отношению к функции Харрингтона. Однако предварительно необходимо процентрировать и промасштабировать функцию та-

ким образом, чтобы: а) она изменялась в интервале от 0 до 1 для аргументов, изменяющихся в интервале от 0 до 1; б) при $x = 0$ функция принимала нулевое значение. Вначале выберем наиболее характерный отрезок изменения функции $H(x)$. Анализ графика функции показывает, что в качестве такого отрезка может быть выбран отрезок [–2; 3]. Тогда преобразование аргумента, переводящее значение из промежутка [–2; 3] в промежуток [0; 1], задается функцией $5x + 2$.

Получаем функцию

$$h(x) = \frac{H(5x+2) - H(-2)}{H(3) - H(-2)} = \frac{\exp(-\exp(-5x-2)) - \exp(-e^2)}{\exp(-1/e^3) - \exp(-e^2)}.$$

Тогда искомое преобразование (т. е. функция, обратная по отношению к функции $h(x)$), задается соотношением

$$p_H(x) = 0,2(-\ln(-\ln[(e^{-e^{-3}} - e^{-e^2})x + e^{-e^2}]) + 2)$$

(как решение уравнения $x = h(y)$). График функции $p_H(x)$ приведен на рис. 1.

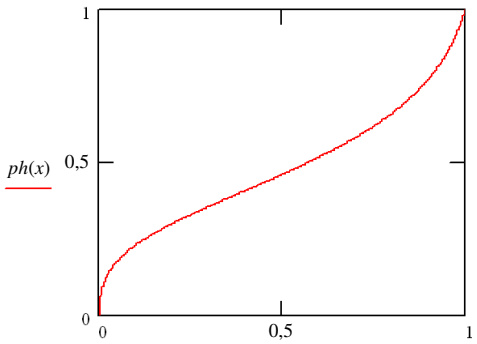

Рис. 1. Преобразование на основе функции Харрингтона

Поскольку $\exp(-e^2) \approx 0,006$ и $\exp(-e^{-3}) \approx 0,9514$, то последнюю формулу можно переписать в виде

$$p_H(x) = 0,2\left(-\ln(-\ln[0,9508x + 0,0006]) + 2\right).$$

Если бы оценки не содержали субъективных искажений, то функция корректировки была бы тождественной, т. е. $p(x) = x$. Тогда функция $i_H(x) = p_H(x) - x$ может рассматриваться как функция искажений, описывающая величину субъективных искажений при каждом конкретном значении оценки. График функции приведен на рис. 2. Как видно из рис. 2, функция корректировки $p_H(x)$ по существу опирается на предположение, что субъекты склонны значительно завышать малые значения оценок; например, значение $x = 0,1$ завышается приблизительно на 0,15 единицы, т. е. в 2,5 раза. Одновременно большие значения оценок субъекты склонны занижать; например, значение $x = 0,85$ занижается приблизительно на 0,15 единицы, т. е. в 1,21 раза. Данное предположение представляется слишком завышенным по своим числовым характеристикам, и поэтому ниже предлагается другой метод построения функции корректировки, опирающий на полиномы.

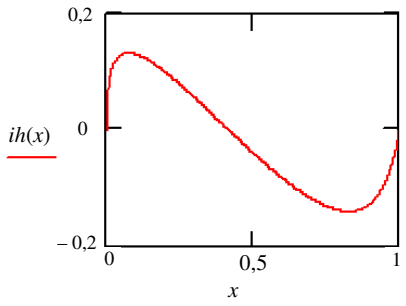

Рис. 2. Функция искажений при преобразовании на основе $p_H(x)$

В качестве функции корректировки, устраняющей субъективные искажения, предлагается выбрать функцию, которая в концевых точках интервалов в шкале Харрингтона, т. е. при $x = 0$; 0,2; 0,37, 0,63; 0,8 и 1, принимала бы значения концевых точек интервалов, соответствующих равномерной шкале оценок, т. е. 0; 0,2; 0,4; 0,6; 0,8 и 1 соответственно. Наиболее простой подобной функцией является многочлен 5-й степени, который может быть получен на основе интерполяционной формулы Лагранжа:

$$p(x) = 0\frac{(x-0,05)(x-0,25)(x-0,5)(x-0,7)(x-1)}{(0-0,05)(0-0,25)(0-0,5)(0-0,7)(0-1)} +$$

$$+0,2\frac{(x-0)(x-0,25)(x-0,5)(x-0,7)(x-1)}{(0,05-0)(0,05-0,25)(0,05-0,5)(0,05-0,7)(0,05-1)} +$$

$$+0,4\frac{(x-0)(x-0,05)(x-0,5)(x-0,7)(x-1)}{(0,25-0)(0,25-0,05)(0,25-0,5)(0,25-0,7)(0,25-1)} +$$

$$+0,6\frac{(x-0)(x-0,05)(x-0,25)(x-0,7)(x-1)}{(0,5-0)(0,5-0,05)(0,5-0,25)(0,5-0,7)(0,5-1)} +$$

$$+0,8\frac{(x-0)(x-0,05)(x-0,25)(x-0,5)(x-1)}{(0,7-0)(0,7-0,05)(0,7-0,25)(0,7-0,5)(0,7-1)} + 1\frac{(x-0)(x-0,05)(x-0,25)(x-0,5)(x-0,7)}{(1-0)(1-0,05)(1-0,25)(1-0,5)(1-0,7)}$$

или

$$p(x) = -0,083x + 10,022x^2 - 29,253x^3 + 33,858x^4 - 13,543x^5.$$

График функции $y = p(x)$ приведен на рис. 3, а соответствующей функции искажений – на рис. 4.

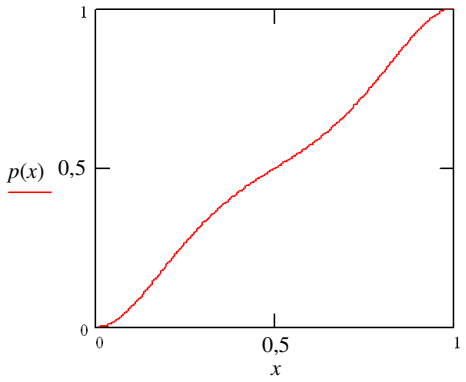

Рис. 3. График функции преобразований на основе полиномов

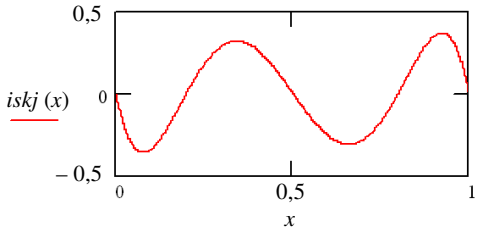

Рис. 4. График функции искажений при полиномиальном преобразовании оценок

Как видно из рис. 4, при полиномиальном преобразовании данных величина искажений носит колебательный характер, совершая два периода (четыре точки экстремума). При этом оказывается, что величина искажений (не более 0,04 единицы по всей шкале) существенно

меньше, чем при использовании функции Харрингтона. Например, при $x = 0{,}1$ оценка занижается приблизительно на 0,04 единицы – в 1,4 раза; при $x = 0{,}9$ оценка завышается на 0,04 единицы, т. е. в 1,04 раза. Однако характер искажений носит принципиально иной характер по сравнению с функцией $p_H(x)$: малые значения оценок занижаются, а большие завышаются, в то время как при использовании функции Харрингтона тенденции были противоположны. Данный вопрос требует дополнительных исследований.

Заключение

В работе получены следующие результаты:

1. Обоснована важность экспертных методов применительно к задаче оценки информационной безопасности сложных систем, и в частности АСУ.

2. Проведен анализ возможных подходов к использованию экспертных методов применительно к оценке параметров сложных систем, и в частности рисков информационной безопасности в АСУ.

3. Обоснована целесообразность корректировки экспертных оценок всех типов, включая числовые оценки, с целью минимизации влияния субъективной составляющей оценок. Предложены конкретные процедуры корректировки на основе введенных в ходе исследования функций преобразования данных.

СПИСОК ЛИТЕРАТУРЫ

1. *Охтилев М. Ю.* Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов / М. Ю. Охтилев, Б. В. Соколов, Р. М. Юсупов. М.: Наука, 2006. 410 с.

2. *Ястребенецкий М. А.* Надежность АСУТП: учеб. пособие / М. А. Ястребенецкий, Г. М. Иванова. М.: Энергоатомиздат, 1989. 264 с.

3. *Адлер Л. П.* Планирование эксперимента при поиске оптимальных условий / Л. П. Адлер, Е. В. Маркова, Ю. В. Грановский. М.: Наука, 1976. 297 с.

Статья поступила в редакцию 12.01.2015

ИНФОРМАЦИЯ ОБ АВТОРАХ

Попов Георгий Александрович – Россия, 414056, Астрахань; Астраханский государственный технический университет; д-р техн. наук; профессор; зав. кафедрой «Информационная безопасность»; popov@astu.org.

Попова Екатерина Александровна – Россия, 414056, Астрахань; Астраханский государственный технический университет; старший преподаватель кафедры «Информационная безопасность»; e.popova@astu.org.

Мельников Александр Викторович – Россия, 414056, Астрахань; Астраханский государственный технический университет; д-р техн. наук, профессор; профессор кафедры «Промышленное рыболовство»; alex_meln@list.ru.

G. A. Popov, E. A. Popova, A. V. Melnikov

ANALYSIS OF THE PARAMETERS OF INFORMATION SECURITY OF THE AUTOMATED SYSTEMS BASED ON THE SPECIFIED EXPERT ASSESSMENTS

Abstract. The paper analyzes the possibilities of using expert methods of assessment of the parameters of the information security of the complex systems, one of the most important representatives of which is an automated control system (ACS). It is shown that with respect to the assess-

ment of the information security parameters and, in particular, the risks, the most acceptable method of assessment is an expert one. In this case, there are two diametrically opposite approaches to assessment: the first approach is used to assess the safety performance of global automation components and the second – some typical elements of the ACS, and then integrated assessments are formed on the basis of the structural relationships of these elements. The paper substantiates the feasibility of using the second approach, because it provides a higher assessment precision. However, this approach is much more labor intensive, based on a large set of assessments, a significant portion of which is obtained by an expert. Due to the abundance of expert assessments, including subjective distortion, we propose a procedure to adjust these data based on the conversion functions. The paper proposes two such functions: one is formed on the basis of the Harrington's function of desirability and the second – on the basis of polynomial extrapolation by Harrington's scale. It is shown that the latter function has a number of the advantages compared with the first one.

Key words: expert assessment, information security, automated systems, Harrington's scale, function of assessment correction.

REFERENCES

1. Okhtilev M. Iu., Sokolov B. V., Iusupov R. M. *Intellektual'nye tekhnologii monitoringa i upravleniia strukturnoi dinamikoi slozhnykh tekhnicheskikh ob"ektov* [Intellectual technologies of monitoring and management of the structural dynamics of complex technical objects]. Moscow, Nauka Publ., 2006. 410 p.

2. Iastrebenetskii M. A., Ivanova G. M. *Nadezhnost' ASUTP* [Reliability of ACS]. Moscow, Energoatomizdat Publ., 1989. 264 p.

3. Adler L. P., Markova E. V., Granovskii Iu. V. *Planirovanie eksperimenta pri poiske optimal'nykh uslovii* [Planning of the experiment while optimization of the conditions]. Moscow, Nauka Publ., 1976.

The article submitted to the editors 12.01.2015

INFORMATION ABOUT THE AUTHORS

Popov Georgiy Aleksandrovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Head of the Department "Information Security"; popov@astu.org.

Popova Ekaterina Aleksandrovna – Russia, 414056, Astrakhan; Astrakhan State Technical University; Senior Lecturer of the Department "Information Security"; e.popova@astu.org.

Melnikov Alexander Victorovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Professor of the Department "Industrial Fishery"; alex_meln@list.ru.