8. Федеральный закон от 29 ноября 2018 года № 459-ФЗ «О федеральном бюджете на 2019 год и на плановый период 2020 и 2021 годов»//СПС КонсультантПлюс.

Вересников Г.С., Огородников О.В.

Оценка информационной безопасности в условиях смешанной неопределенности

Аннотация: Оценка информационной безопасности является актуальной задачей на всех этапах работы комплекса защиты информации и в настоящее время становится одним из важнейших аспектов общей экономической безопасности деятельности организации, характеризуя состояние защищённости ее бизнес-среды. Защита информации представляет собой особую деятельность по предотвращению утечки информации, несанкционированных изменений ее потоков и других воздействий, негативно влияющих на стабильную работу организации и связанных с ней экономических агентов. В статье представлена методика оценки информационной безопасности в случае смешанной алеаторной (статистической) и эпистемической (экспертной) неопределенности входных данных. Представленная методика рассмотрена на примере расчета уровня риска информационной безопасности.

Ключевые слова: информационная безопасность, оценка рисков, алеаторная неопределенность, эпистемическая неопределенность, теория неопределенности

Алеаторная неопределенность возникает, когда параметры характеризуются вариабельностью, зафиксированной в статистических данных, достаточных для принятия статистических гипотез о неопределенных параметрах. В этом случае параметру соответствует функция распределения вероятности. Эпистемическая неопределенность возникает из-за недостатка знаний, результатов наблюдений. В этом случае информацию получают от экспертов. Для работы с экспертной неопределенностью существует много математических теорий.

Наиболее популярные из них это интервальная математика, теория нечетких множеств Л. Заде и теория возможностей Л. Заде. В данной работе для описания неопределенных параметров предлагается теория неопределенности Б. Лю, так как в ней существуют простые аналитические выражения для вычисления детерминированных дубликатов целевых параметров для достаточно широкого класса функций.

Из-за наличия недетерминированных параметров аналитические выражения для оценки безопасности информационных систем не могут применяться исходном виде. Это объясняется тем, что результатом вычисления аналитических выражений, которые зависят от недетерминированных параметров, всегда является недетерминированная величина, распределение которой зависит от распределений этих параметров. В связи с этим в качестве замены аналитических выражений необходимо использовать числовые характеристики недетерминированных величин, являющихся результатом вычисления этих выражений.

Пусть оценка безопасности информационной (ИБ) системы задается функцией (аналитическим выражением) $f(\bar{\xi},\bar{\omega})$, зависящей от параметров $\bar{\xi}$ и $\bar{\omega}$, соответственно, с эпистемической и алеаторной неопределенностью, т.е. величиной со смешанной неопределенностью. Известны два подхода к моделированию величин со смешанной неопределенностью, основанные на разных интерпретациях этих величин [1, 2, 3].

В первом подходе $f(\bar{\xi},\bar{\omega})$ рассматривается как случайная величина, параметризованная эпистемическими величинами. Характеристика функции $f(\bar{\xi},\bar{\omega})$ со смешанной неопределенностью определяется в два этапа. Сначала определяется стохастическая характеристика $S'(\bar{\xi}) = S_{\bar{\omega}}(f(\bar{\xi},\bar{\omega}))$ функции $f(\bar{\xi},\bar{\omega})$. Полученная характеристика $S'(\bar{\xi})$ не зависит от случайных величин и как функция от эпистемических величин является эпистемической величиной. Затем определяется эпистемическая характеристика величины $S'' = S_{\bar{\xi}}(S'(\bar{\xi}))$, которая

является характеристикой функции $f(\bar{\xi},\bar{\omega})$ со смешанной неопределенностью.

Во втором подходе $f(\bar{\xi},\bar{\omega})$ рассматривается как эпистемическая величина, параметризованная случайными величинами. Сначала определяется эпистемическая характеристика $S^{'}(\bar{\omega}) = S_{\bar{\xi}}(f(\bar{\xi},\bar{\omega}))$ функции $f(\bar{\xi},\bar{\omega})$. Здесь $S^{'}(\bar{\omega})$ рассматривается, как функция от случайных величин и поэтому является случайной величиной. Затем определяется стохастическая характеристика эпистемической характеристики $S^{''} = S_{\bar{\omega}}(S^{'}(\bar{\omega}))$, которая и является характеристикой функции $f(\bar{\xi},\bar{\omega})$ со смешанной неопределенностью.

Предлагаются функции для оценки безопасности информационных систем, включающие в себя параметры с эпистемической неопределенностью, интерпретировать в рамках теории неопределенности [4] как неопределенные величины с функциями распределения неопределенности. Используем второй подход к моделированию величин со смешанной неопределенностью. Тогда функция $f(\bar{\xi},\bar{\omega})$ рассматривается как неопределенная величина, параметризованная случайными величинами.

Выведем числовые характеристики, усредняющие функцию $f(\bar{\xi},\bar{\omega})$ по неопределённым и случайным параметрам, – ожидаемое значение и математическое ожидание. Пусть $f(\bar{\xi},\bar{\omega})$ – непрерывная строго возрастающая по $\xi_1, \ldots, \xi_q$ и строго убывающая по $\xi_{q+1}, \ldots, \xi_n$, тогда числовая характеристика функции $f(\bar{\xi},\bar{\omega})$ как неопределенной величины согласно [4] имеет вид:

$$E^M(f(\bar{\xi},\ \bar{\omega}) = \int_0^1 f\ (\Phi_{\xi_1}^{-1}(\alpha), \Phi_{\xi_2}^{-1}(\alpha), \ldots$$
$$\ldots, \Phi_{\xi_q}^{-1}(\alpha), \Phi_{\xi_{q+1}}^{-1}(1-\alpha), \ldots, \Phi_{\xi_n}^{-1}(1-\alpha),\ \bar{\omega})d\alpha.$$

Числовая характеристика математического ожидания случайной величины $E^M(f_i(\bar{\xi},\bar{\omega})$ имеет вид:

$$E^P(E^M(f\ (\bar{\xi},\bar{\omega}))=\int\limits_{R^h}\int\limits_{0}^{1}\Phi_{\xi_1}^{-1}(\alpha),\Phi_{\xi_2}^{-1}(\alpha),...$$

$$...,\Phi_{\xi_q}^{-1}(\alpha),\Phi_{\xi_{q+1}}^{-1}(1-\alpha),...,\Phi_{\xi_n}^{-1}(1-\alpha),\bar{\omega})d\alpha d\Psi_{\omega_1}...d\Psi_{\omega_h},$$

где ξ_1, ξ_2, ..., ξ_n − входные неопределенные параметры с функциями распределения Φ_{ξ_1}, Φ_{ξ_2},..., Φ_{ξ_n}, имеющими обратные функции распределения; ω_1, ..., ω_h − входные случайные параметры с функциями распределения Ψ_{ω_1}, Ψ_{ω_2}, ..., Ψ_{ω_h};

Использование числовых характеристик, усредняющих функцию $f(\bar{\xi},\bar{\omega})$ по случайным и неопределённым параметрам, не всегда подходит для оценки информационной безопасности. Требования к надежности этих оценок приводят к необходимости использования квантилей неопределенных и случайных величин. В этом случае определяется уровень функции, непревышение которого гарантируется с заданной надежностью (степенью уверенности α_f и вероятностью β_f):

$$r_f,\ P(inf_{\alpha_f}\ (f\ (\bar{\xi},\bar{\omega}))\le r_f\ )\ge\beta_f\ ,$$

где в соответствии с [4]:

$$inf_{\alpha_f}(f(\bar{\xi},\bar{\omega}))=f(\Phi_{\xi_1}^{-1}(\alpha_f),\Phi_{\xi_2}^{-1}(\alpha_f),...$$

$$...,\Phi_{\xi_q}^{-1}(\alpha_f\ ),\Phi_{\xi_{q+1}}^{-1}(1-\alpha_f),...,\Phi_{\xi_n}^{-1}(1-\alpha_f),\ \ \bar{\omega}).$$

Аналогичным образом определяется уровень функции, который будет больше всех возможных значений $f(\bar{\xi},\bar{\omega})$ с заданной надежностью (степенью уверенности α_f и вероятностью β_f):

$$r_f,\ P(sup_{\alpha_f}\ (f\ (\bar{\xi},\bar{\omega}))\ge r_f\ )\ge\beta_f\ ,$$

где в соответствии с [4]:

$$sup_{\alpha_f}\ (f\ (\bar{\xi},\bar{\omega}))=f\ (\Phi_{\xi_1}^{-1}(1-\alpha_f),\Phi_{\xi_2}^{-1}(1-\alpha_f),...$$

$$...,\Phi_{\xi_q}^{-1}(1-\alpha_f\ ),\Phi_{\xi_{q+1}}^{-1}(\alpha_f),...,\Phi_{\xi_n}^{-1}(\alpha_f\ ),\ \bar{\omega}).$$

Если аналитическое выражение $f(\overline{\xi}, \overline{\omega})$ не является монотонным по неопределенным параметром, то для вычисления числовых характеристик эпистемических величин используются алгоритмы [5].

Ниже приведен пример применения описанного подхода к выражению для расчета риска из Практического руководства по управлению ИБ (BS 7799). Схожее выражение содержит в ГОСТ Р ИСО/МЭК ТО 7. Значение риска R рассчитывается как:

$$R = L(t) \cdot L(v) \cdot S,$$

где $L(t)$ – уровень угрозы ИБ, $L(v)$ – уровень/степень уязвимости, S – ценность актива.

Пусть параметры $L(v)$ и S являются неопределенными величинами, а параметр $L(t)$ вероятностной величиной. Определим уровень риска r, который не будет превышен с заданной степенью уверенности α_R и вероятностью β_R. Тогда выражение для r будет выглядеть так:

$$P(inf_{\alpha_R}(R(L(t),\ L(v), S)) \leq r) \geq \beta_R,$$

где $inf_{\alpha_R}\big(R(L(t),\ L(v), S)\big) = L(t) \cdot \Phi_{L(v)}^{-1}(\alpha_R) \cdot \Phi_S^{-1}(\alpha_R)$, $\Phi_{L(v)}^{-1}$ и Φ_S^{-1} – обратные функции распределения неопределенности для $L(v)$ и S соответственно.

Применение данного подхода позволит произвести более корректную оценку показателей информационной безопасности в условиях смешанной неопределенности входных данных.

Заключение

В статье предложен подход к решению задачи оценки информационной безопасности в условиях смешанной неопределенности, базирующийся на теории неопределенности Б. Лю [4]. Эта теория для достаточно широкого класса функций позволяет получить аналитические выражения числовых характеристик функций, зависящих от неопределенных параметров. Для моделирования функции оценки информационной безопасности, зависящей от неопределенных и случайных величин, предложено интерпретировать ее как неопределенную величину, параметризованную случайными величинами. Выведены формулы для расчета числовых характеристик аналитических выражений, зависящих от случайных и неопределенных величин.

Литература:

1. *Eldred S., Swiler T., Tang G.* Mixed aleatory-epistemic uncertainty quantification with stochastic expansions and optimization-based interval estimation//Reliability Engineering and System Safety. – 2011. – Vol. 96. № 9. – P. 1092-1113.

2. *Lockwood B., Anitescu M., Mavripilis D.* Mixed aleatory/epistemic uncertainty quantification for hypersonic flows via gradient-based optimization and surrogate models// 50th AIAA Aerospace Sciences Meeting including the New Horizons Forum and Aerospace Exposition. – 2012 [Электронный ресурс]. – URL: https://www.researchgate.net/publication/268471807_Mixed_AleatoryEpistemic_Uncertainty_Quantification_for_Hypersonic_Flows_via_Gradient-Based_Optimization_and_Surrogate_Models (дата обращения 20.10.2020).

3. *Язенин А.В.* Основные понятия теории возможностей. – М.: Физматлит, 2016. – 144 с.

4. *Liu B.* Uncertainty Theory. 4-nd edition. – Berlin: Springer-Verlag, 2015. – 487 p.

5. *Zhu Y.* Functions of uncertain variables and uncertain programming//Journal of Uncertain Systems. – 2012. – Vol. 6(4). – P. 278-288.

Кереселидзе Н.Г.

Модели распространения вируса SARS-CoV-2 и проблемы управления безопасностью

Аннотация: Предложены математические и компьютерные модели распространения вируса SARS-CoV-2 с учетом протокола борьбы с эпидемией принятой властями Грузии. Ставится задача управления борьбы с эпидемией.

Ключевые слова: математическая, компьютерная модель, SARS-Cov-2, управление, эпидемия

1. Введение. Пандемия COVID19, вызванная вирусом SARS-CoV-2, не обошла стороной и Грузию. Реакция властей Грузии на эпидемию SARS-Cov-2 была разной весной и осенью 2020 года. Так например, весной 2020, власти прислушались к советам экспертов из системы здравоохранения, и фактически ввели локдаун в стране.