ПРИМЕНЕНИЕ МЕТОДОВ ТЕОРИИ ВОЗМОЖНОСТЕЙ ПРИ МОДЕЛИРОВАНИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Щербаков Е.С.¹, Корчагин П.В.²

Дается математическое представление модели функционирования системы защиты информации, базирующееся на применении методов теории возможностей, что позволяет компенсировать методологические трудности, сопряжённые с применением в тех же целях классической теории вероятностей. При исследовании статистических данных о информационных инцидентах специалисты сталкиваются с таким неприятным с методической точки зрения фактом, как статистическая неоднородность указанных данных. Источники этой неоднородности достаточно многочисленны и разнообразны по своей природе, но главной причиной служит всё-таки человеческий фактор. Плохое знание инструкций, невнимательность, степень утомления, торопливость пользователей – вот весьма неполный перечень источника неоднородности исходных данных. Провести факторизованный анализ причин, порождающих информационные инциденты, администратору безопасности не представляется никакой возможности. Однако обобщать факты, характеризующие информационные инциденты, проводить моделирование информационных инцидентов, и делать адекватные выводы всё-таки нужно. Статистическая неоднородность исходных данных делает невозможным применения для их обобщения и моделирования классических методов статистического моделирования. В статье предлагается решить задачу моделирования систем защиты информации на основе методов теории возможностей.

Ключевые слова: модель функционирования, вероятностные модели, моделирование систем защиты, статистическая неоднородность, интервальный анализ.

DOI: 10.21681/2311-3456-2017-1-2-5

Вероятностные модели широко используются для оценки эффективности функционирования систем защиты информации (СЗИ). Однако практика работы со случайными величинами убедительно доказывает, что вероятностные методы несостоятельны при моделировании сложных недетерминированных процессов, причём к этим процессам можно смело отнести действия по несанкционированному доступу к секретной информации. В работах [1, 2] показано, что теория вероятностей является частным случаем теории возможностей. В свою очередь математической основой последней является интервальный анализ и теория нечётких множеств.

В интервальном анализе предполагается, что имеется измеренное неточным прибором значение x неизвестной измеряемой величины x_0 , и известна абсолютная Δ (или относительная δ) ошибка измерения. Тогда границы интервала неопределённости измеряемой величины x_0 определяются из условия:

$$[x_0] = [x^-, x^+] = [x - \Delta; x + \Delta] = [x(1 - \delta); x(1 + \delta)]. \quad (1)$$

В «классической» интервальной арифметике операции с положительными (не включающими

нуля) интервалами определяются следующим образом:

$$\begin{aligned} [a] + [b] &= [a^- + b^-; a^+ + b^+]; \\ [a] - [b] &= [a^- - b^+; a^+ - b^-]; \\ [a] \times [b] &= [a^- \times b^-; a^+ \times b^+]; \\ [a] / [b] &= [a^- / b^+; a^+ / b^-]. \end{aligned} \quad (2)$$

В интервальной арифметике не выполняется дистрибутивный закон:

$$\begin{aligned} ([a] + [b]) [c] &\neq [a] [c] + [b] [c], \\ &\text{отсутствуют обратные элементы} \\ ([a] / [a]) &= 1, \\ [a] - [a] &= 0. \end{aligned}$$

Отечественные учёные развивали методы интервального анализа [3, 4]. Базовый принцип интервального анализа формулируется следующим образом: интервал неопределённости результата есть множество всех его возможных значений, получаемых при варьировании переменных и параметров задачи в границах известных интервалов. В частности, если дана функция (или функционал) $[y] = f([x])$, интервального векторного аргумента $[x] = ([x^1], \dots, [x^i], \dots, [x^k])$, то границы y^-, y^+ интервала неопределённо-

1 Щербаков Е.С., кандидат технических наук, профессор, Военная академия воздушно-космической обороны, г. Тверь, ses1828@rambler.ru

2 Корчагин П.В., кандидат технических наук, Военно-космическая академия имени А.Ф. Можайского, г. Санкт-Петербург, pavel.v.korchagin@gmail.com

сти значения функции определяются как решение двух задач на экстремум:

$$\begin{aligned} y^- &= \min_{x \in X} f(x), \\ y^+ &= \max_{x \in X} f(x). \end{aligned} \quad (3)$$

Применение интервального анализа позволяет снять многие проблемы и методические сложности, возникающие при решении прикладных задач статистическими методами.

В рамках интервального анализа неопределённость исходных данных может иметь разные источники и природу. Например, пусть в процессе экспериментального исследования в течении одного года эффективности функционирования одной и той же системы защиты информации (СЗИ), эксплуатируемой шестью различными пользователями, были получены статистические результаты, аппроксимируемые шестью разными законами распределения значения показателя эффективности СЗИ, перечисленными в таблице 1.

Таким образом, анализируются шесть законов распределения, указанных в таблице 1. Символом $\mathcal{E}_S$ будет обозначаться вариант закона распределения случайного значения при

$$S \in \{1, 2, 3, 4, 5, 6\}, \quad (4)$$

где S – индекс закона распределения (табл.).

Данные характеризуют эффективность функционирования СЗИ показателем, лежащим в замкнутом интервале $[0; 1]$, причём нуль соответствует абсолютно неэффективному функционированию СЗИ, а единица – абсолютно эффективному.

Таблица 1.

Варианты закона распределения, используемые для оценки показателя эффективности СЗИ

Индекс закона	Название закона
1	экспоненциальный
2	гиперпоказательный
3	Эрланга 2-го порядка
4	Эрланга 3-го порядка
5	Релея
6	Релея-Райса

Ставится задача: получить оценку показателя эффективности СЗИ на основе обобщения данных для всех пользователей. В силу статистической неоднородности результатов получение подобной оценки методами теории вероятностей и математической статистики невозможно. На основе методов теории возможностей задача решается следующим образом.

Для шести указанных в табл. законов распределения строятся доверительные интервалы, например, для доверительной вероятности $\beta = 0,95$ (рис. 1):

$$[\mathcal{E}_S^-; \mathcal{E}_S^+] \text{ для } S \in \{1, 2, 3, 4, 5, 6\}. \quad (5)$$

Объединение всех данных проводится с использованием разработанной авторами интервальной операции расслоения (рис. 2)

$$\begin{aligned} &DIL([\mathcal{E}_1^-; \mathcal{E}_1^+], [\mathcal{E}_2^-; \mathcal{E}_2^+], \dots, [\mathcal{E}_i^-; \mathcal{E}_i^+], \dots \\ &\dots, [\mathcal{E}_N^-; \mathcal{E}_N^+]). \end{aligned} \quad (6)$$

Рис. 1. Совмещённое рассмотрение доверительных интервалов оценок показателя эффективности СЗИ

Рис. 2. Группирование интервальных оценок

Операция $DIL(\dots)$ (от англ. divide into layers – разделить на слои) определяется следующим образом:

$$\begin{aligned} & DIL([\mathfrak{A}_1^-; \mathfrak{A}_1^+], [\mathfrak{A}_2^-; \mathfrak{A}_2^+], \dots, [\mathfrak{A}_j^-; \mathfrak{A}_j^+], \dots, \\ & \dots, [\mathfrak{A}_N^-; \mathfrak{A}_N^+]) = \{[\mathfrak{A}_B^-; \mathfrak{A}_B^+], [\mathfrak{A}_A^-; \mathfrak{A}_A^+], [\mathfrak{A}_C^-; \mathfrak{A}_C^+]\} \\ & \mathfrak{A}_B^- = \min\{\mathfrak{A}_1^-, \mathfrak{A}_2^-, \dots, \mathfrak{A}_j^-, \dots, \mathfrak{A}_N^-\}; \\ & \mathfrak{A}_B^+ = \max\{\mathfrak{A}_1^+, \mathfrak{A}_2^+, \dots, \mathfrak{A}_j^+, \dots, \mathfrak{A}_N^+\} + \\ & + \{[\mathfrak{A}_C^-; \mathfrak{A}_C^+], [\mathfrak{A}_A^-; \mathfrak{A}_A^+]\} \\ & \mathfrak{A}_C^- = \min\{\mathfrak{A}_1^-, \mathfrak{A}_2^-, \dots, \mathfrak{A}_j^-, \dots, \mathfrak{A}_N^-\}; \\ & \mathfrak{A}_C^+ = \max\{\mathfrak{A}_1^+, \mathfrak{A}_2^+, \dots, \mathfrak{A}_j^+, \dots, \mathfrak{A}_N^+\} + \\ & + \{[\mathfrak{A}_B^-; \mathfrak{A}_B^+], [\mathfrak{A}_A^-; \mathfrak{A}_A^+]\}. \end{aligned} \quad (7)$$

На основе анализа эмпирических данных определяются частоты попадания оценок эффективности СЗИ в интервалы B , A и C . Например, $P_B = 0,1$; $P_A = 0,5$; $P_C = 0,4$. В этом случае интервальные оценки представляются в форме гистограммы, представленной на рис. 3.

Далее определяется центр масс (ЦМ) фигуры, образованной огибающей всех компонент гистограммы B , A и C , построенной без пробелов. Проекция ЦМ на ось абсцисс и даст итоговый результат – наиболее точную аппроксимацию СЗИ (по Мамдани [5]).

Совокупность методических приёмов, правил и операций представляют суть усовершенство-

Рис. 3 – Обобщение статистически неоднородных результатов моделирования

ванного метода применения теории возможностей и теории интервалов для математического описания характера неопределённости и обобщения исходных данных, для моделирования функционирования СЗИ.

На основе предложенного методического подхода достаточно просто и эффективно решить задачи:

- моделирования процесса функционирования средств защиты информации на основе методов имитационного моделирования, например, с применением языка GPSS;

- классификации источников возникновения информационных инцидентов на основе анализа статистически неоднородных признаков;

- распознавания в реальном масштабе времени потенциально опасных ситуаций, характеризующие совокупностью статистически неоднородных признаков;

- разработки и уточнения рекомендации администраторам безопасности по профилактике информационных инцидентов и выявлению фактов нарушения.

Рецензент: Гамов Максим Викторович, доктор технических наук, профессор кафедры оценки эффективности боевых действий Военной академии воздушно-космической обороны г. Тверь, vavko@mil.ru

Литература:

1. Yager R. A foundation for a theory of possibility // J. of Cybernetics. – 1980. – Vol. 10, №. 1–3. – P. 177–209.
2. Пытьев Ю. П., «Возможность. Элементы теории и применения», Эдиториал УРСС, 2000. – 237 с.
3. Калмыков С. А., Шокин Ю.И., Юлдашев З.Х. Методы интервального анализа. – Новосибирск: Наука, 1986. – 354 с.
4. Орлов А. И. Асимптотический линейный регрессионный анализ для интервальных данных – М.: Издательство стандартов, 1986. – 279 с.
5. Прикладные нечёткие системы / Под. ред. Т. Тэрано, К. Асан, М. Сугэно. – М: Мир, 1993. – 368 с.

APPLICATION OF POSSIBILITY THEORY METHODS TO MODELLING INFORMATION SECURITY SYSTEMS

E. Sherbakov³, P. Korchagin⁴

Abstract. The article gives mathematical representation of the model of the information security system operation, which is based on the possibility theory methods, which allows compensating for methodological difficulties associated with the use of the classic probability theory for the same purpose. The specialists studying static data on information incidents face such unpleasant methodical problem as static heterogeneity of the specified data. The sources of this heterogeneity are multiple and have various nature, however, the main cause is still the human factor. Poor knowledge of manuals, lack of attention, fatigue, hastiness of the users is just a small list of causes for the source data heterogeneity. The security manager simply cannot carry out a fact-based analysis of causes that lead to information incidents. Nevertheless, it is necessary to consolidate facts that describe information incidents, model information incidents, and make adequate conclusions. Static heterogeneity of the source data makes it impossible to use classic methods of static modelling for their consolidation and modelling. The article suggests solving the problem of the information security modelling using the probability theory methods.

Keywords: operating model, probabilistic models, modeling systems of protection, statistical heterogeneity, interval analysis.

References

1. Yager R. A foundation for a theory of possibility, J. of Cybernetics. – 1980. – Vol. 10, №. 1–3. – P. 177–209.
2. Pyt'ev YU. P., *Vozmozhnost'. Elementy teorii i primeneniya*, Editorial URSS, 2000. – 237 s.
3. Kalmykov S. A., Shokin Y.I., Yuldashev Z.X. *Metody interval'nogo analiza*. – Novosibirsk: Nauka, 1986. – 354 s.
4. Orlov A. I. *Asimptoticheskiy lineyny regressionny analiz dlya interval'nykh dannykh* – M.: Izdatel'stvo standartov, 1986. – 279 s.
5. *Prikladnye nechyotkie sistemy* / Pod. red. T. Tehrano, K. Asan, M. Sughehno. – M: Mir, 1993. – 368 p.

3 Evgeniy Sherbakov, Ph.D., professor, Military Academy of Aerospace Defense, Tver, Russia, ses1828@rambler.ru

4 Pavel Korchagin, Ph.D., Military Space Academy named A.F.Mozhayskogo, St. Petersburg, Russia pavel.v.korchagin@gmail.com