УПРАВЛЕНИЕ, МОДЕЛИРОВАНИЕ, АВТОМАТИЗАЦИЯ

DOI: 10.24143/2072-9502-2021-3-7-15
УДК 004.942

НЕЧЕТКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ: ОСОБЕННОСТИ ПОСТРОЕНИЯ ФУНКЦИЙ ПРИНАДЛЕЖНОСТИ[1]

И. В. Котенко, И. Б. Паращук

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Российская Федерация

Объектом исследования являются методологические подходы к решению задач построения функций принадлежности в приложении к процедурам принятия решений (поддержки принятия решений) для нечеткого управления информацией и событиями безопасности современных киберфизических систем. Данные методологические подходы (методы) позволяют учесть нечеткость наблюдаемых и управляемых параметров защищенности сложных управляемых технических систем. При этом сравнительный анализ рассматриваемых подходов ориентирован на наиболее применимые для конкретных задач методы – метод построения функций принадлежности на основе анализа функций плотности вероятности и метод, использующий простую вероятностную схему. На базе метода, использующего анализ функций плотности вероятности, предложен механизм определения значений функций принадлежности для задачи принятия решений о принадлежности конкретной компьютерной атаки к нечеткому множеству опасных атак (множеству атак большого уровня опасности). Этот механизм не обладает большой математической и вычислительной сложностью, но позволяет учесть нечеткость наблюдаемых и управляемых параметров безопасности, что обеспечит повышение достоверности контроля информации и событий безопасности в рамках нечеткого управления защищенностью систем такого класса.

Ключевые слова: управление информацией и событиями безопасности, нечеткое управление, принятие решений, функция принадлежности, метод, нечеткое множество, вероятность.

Для цитирования: *Котенко И. В., Паращук И. Б.* Нечеткое управление информацией и событиями безопасности: особенности построения функций принадлежности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2021. № 3. С. 7–15. DOI: 10.24143/2072-9502-2021-3-7-15.

Введение

В отличие от классических управляемых инженерных систем, например традиционных систем машиностроения, энергетики и промышленного производства, современные киберфизические системы (КФС) представляют собой большие и многокомпонентные инженерные объекты, реализованные на основе бесшовной интеграции вычислительных алгоритмов и встроенных физических компонентов. Применение КФС позволяет повысить адаптивность, масштабируемость, отказоустойчивость и безопасность инженерных систем, а также эргономичность их использования. Принято считать, что в системах такого класса кибернетическая и физическая составляющие тесно интегрированы во всех масштабах и на всех уровнях в рамках единого информационного пространства с помощью датчиков и сенсоров [1].

Киберфизические системы позволяют организационно и технически скоординировать разнородные дискретные и непрерывные подсистемы, объекты и процессы, интегрируют в себе кибернетическую составляющую, компьютерные аппаратные и программные технологии. В рамках КФС объединены силы, средства и процессы, эти системы основаны на интеграции кибернетического, технологического, физического (ресурсного) и информационного пространств.

[1]Работа выполнена при частичной финансовой поддержке РФФИ (проект 18-29-22034) и бюджетной темы 0073-2019-0002.

В основе процесса функционирования КФС лежит обмен информацией, поэтому защита этой информации, обеспечение ее доступности, целостности и конфиденциальности является приоритетной проблемой в мировой теории и практике [2]. В этой связи также продолжает оставаться актуальным важное направление исследований в рамках защиты информации – управление событиями и инцидентами информационной безопасности систем такого класса [3]. Для этого создаются специальные SIEM (Security Information and Event Management) подсистемы. Они берут на себя функции управления информацией, инцидентами и событиями безопасности. Помимо того, что такие подсистемы осуществляют мониторинг защищенности – анализируют в реальном времени события (угрозы) безопасности, исходящие от устройств сети и приложений, – они, по сути, являются подсистемами поддержки принятия решений (ППР) по выбору и применению мер противодействия, по реагированию на эти угрозы. Их цель – не допустить или предельно минимизировать возможный ущерб, который может быть нанесен данным, циркулирующим в сложных управляемых информационно-технических системах, например таких, как КФС [4].

Анализ релевантных работ

Реализуемые в современных системах защиты информации процессы контроля и управления информацией, событиями и инцидентами безопасности имеют сложную иерархию, но в основе их традиционно лежат процедуры принятия решений (ПР) и ППР. Процедуры и алгоритмы ПР и ППР по управлению информацией и событиями безопасности имеют свои особенности и нацелены на реализацию на всех этапах сбора и анализа данных от систем контроля цифрового сетевого контента с целью обнаружения и противодействия угрозам безопасности КФС. При этом решаются задачи сбора и обработки данных о событиях безопасности от распределенных сенсоров, задачи обработки больших данных для предварительного анализа событий безопасности, задачи оценки защищенности и многие другие.

Необходимость учета этих особенностей и анализ физической сущности перечисленных решаемых задач приводят к необходимости поиска новых современных и перспективных подходов к процедурам управления событиями и инцидентами информационной безопасности. На наш взгляд, наиболее адекватные подходы к процедурам управления событиями и инцидентами информационной безопасности в рамках обеспечения защиты информации, циркулирующей в сложных управляемых технических системах и компьютерных сетях, рассмотрены в ряде современных работ [3–11].

Работа [3] рассматривает алгоритмы ситуационного управления информацией и событиями безопасности для защиты данных в критически важных инфраструктурах. Здесь предложена модель управления, основанная на готовых пакетах (наборах) управленческих решений, что, имея ввиду разнообразие угроз, неприемлемо для полноценной защиты реальных сложных управляемых технических систем и компьютерных сетей.

В работах [4, 5] утверждается, что управление информацией и событиями безопасности сложных управляемых технических систем (таких, как КФС) и компьютерных сетей может быть практически воплощено на базе замкнутых контуров управления с обратной связью. Но подобные алгоритмы управления требуют существенных вычислительных и временных затрат на сбор и обработку статистических данных наблюдения, получаемых по каналам обратной связи. Эти алгоритмы управления сложны с точки зрения программно-аппаратной реализации каналов наблюдения.

Подходы к формализации и построению алгоритмов управления информацией и событиями безопасности технических систем и компьютерных сетей, подходы к ПР по управлению, рассмотренные в работах [6] и [7], ориентированы в основном на традиционные методы определения (идентификации) параметров информационной безопасности и управления (манипулирования) значениями этих параметров, но, в силу необходимости учета многообразия угроз и иных негативных влияющих факторов, могут быть малоэффективны для полноценного многокритериального управления, для описания всех возможных управляющих воздействий, направленных на обеспечение доступности, целостности и конфиденциальности данных.

Работа [8] посвящена важным вопросам классификации современных подсистем управления инцидентами безопасности, интересна для общего понимания современных подходов к данной проблеме, но почти не содержит практических рекомендаций по формированию алгоритмов управления информацией, событиями и инцидентами безопасности, например в условиях неопределенности (нечеткости, неполноты, противоречивости) данных наблюдения.

Существует ряд работ [9–11], в которых рассмотрены алгоритмы управления безопасностью информации, основанные на визуализации данных наблюдения, на поиске закономерностей и аномалий в данных наблюдения за параметрами информационной безопасности, а также на управлении рисками. Эти подходы частично затрагивают вопросы управления в условиях неопределенности, но требуют предварительной идентификации нечетких или неполных данных наблюдения, например в рамках SIEM-подсистем, а эти процедуры не всегда можно реализовать практически в динамике функционирования КФС (фактор инерционности, «запаздывания» данных наблюдения).

Технологические и методологические подходы, применяемые в рамках решения традиционных задач управления и принятия любых иных решений по управлению информацией и событиями безопасности, рассматриваются в работе [12]. Здесь предложены некоторые подходы к разработке процедур принятия таких решений, причем рассмотренные в статье алгоритмы ПР по контролю и управлению информационной безопасностью отличаются глубиной анализа и набором управляемых (контролируемых) параметров. Однако рассмотренные в этой работе методологические подходы и алгоритмы ПР являются сложными с точки зрения математической реализации и не унифицированы для различных конкретных процессов ПР, также не способны учитывать неопределенность (нечеткость) наблюдаемых и управляемых параметров при ПР, не приспособлены к задачам так называемого нечеткого управления.

Таким образом, из анализа релевантных работ следует, что традиционные подходы к построению алгоритмов управления информацией и событиями безопасности не позволяют в полной мере учесть неопределенность (нечеткость) наблюдаемых и управляемых параметров защищенности сложных управляемых технических систем, таких как КФС. Поэтому представляется актуальной задача формулировки подходов к ПР по нечеткому управлению информацией и событиями безопасности, опирающихся на алгоритмы построения функций принадлежности (ФП) нечетких множеств [13].

Теоретические подходы к построению функций принадлежности в задачах нечеткого управления информацией и событиями безопасности

Рассмотрим различные теоретические аспекты построения ФП нечетких множеств в приложении к задачам ПР по управлению информацией и событиями безопасности.

Допустим, введены термы нечеткой лингвистической переменной, т. е. введены качественные (не количественные) значения логико-лингвистической переменной x, характеризующей нечеткие суждения (мнения) экспертов и лиц, принимающих решения, например, о текущем уровне (степени) опасности конкретного типа компьютерных атак для информационной безопасности КФС: «уровень опасности конкретного типа компьютерных атак x мал» и «уровень опасности конкретного типа компьютерных атак x большой».

Очевидно, что любой ФП $\mu(x)$, характеризующей, в рамках ПР, текущий уровень опасности конкретного типа компьютерных атак для информационной безопасности КФС, присущ несколько субъективистский уклон вне зависимости от того факта, что ФП может отражать мнение не одного субъекта-специалиста, а целого коллектива, группы экспертов.

Для принятия обоснованного решения по управлению информацией и событиями безопасности необходимо определить значение ФП, характеризующих уровень (степень) опасности конкретного типа компьютерных атак.

Одним из простейших нечетких алгоритмов решения данной задачи является вариант построения ФП по так называемой простой вероятностной схеме [13].

Аналитическая (в терминах математики теории нечетких множеств) сущность такого варианта построения ФП заключается в следующем. Для любого из n экспертов формулируется запрос его экспертного мнения – «является ли переменная x элементом множества A», где множество A определяет терм«большой уровень опасности конкретного типа компьютерных атак для информационной безопасности КФС».

В случае, когда n_1 специалистов-экспертов отвечают на запрос их экспертного мнения положительно, а n_2 экспертов отвечают отрицательно, принято определять ФП $\mu(x)$, характеризующую, в нашем случае, текущий уровень опасности конкретного типа компьютерных атак для информационной безопасности КФС, в виде

$$\mu(x) = n_1 / (n_1 + n_2),$$

причем $n_1 + n_2 = n$ [13].

Известны четыре базовых классификационных признака алгоритмов (методов) построения ФП нечетких множеств [13]: основанный на предположении (гипотетический) вид области определения нечеткого множества: числовая – дискретная (*a*) или непрерывная (*b*) и нечисловая (*c*); используемый в рамках построения ФП метод экспертного опроса: индивидуальный (d_1) или групповой (d_2); вид применяемой экспертной информации: порядковая (e_1) или кардинальная (e_2); трактовка получаемых данных – итогов экспертного опроса: вероятностная (*D*) или детерминированная (*N*).

В работах [13, 14] рассмотрены теоретические аспекты построения алгоритма поиска значений ФП типа $< a, d_1, e_2, N >$. Сущность данного алгоритма заключается в использовании итоговых (результирующих) мнений, по сути, вердикта, выносимого так называемым лицом, принимающим решения (ЛПР), на основе количественного сравнения им степеней принадлежности.

Итог формулировки результирующих мнений ЛПР – матрица отношений $B = \| b_{ij} \|$ размером $n \times n$. Здесь n – количество точек u_i, в которых необходимо сравнить значения ФП. При этом каждый элемент b_{ij} матрицы отношений B – субъективное мнение ЛПР об отношении $\mu_{\tilde{A}}(u_i)/\mu_{\tilde{A}}(u_j)$, где *i* и *j* – *i*-я строка и *j*-й столбец матрицы отношений. Данное мнение, эта субъективистская оценка, призвана отразить мнение конкретного ЛПР о том, во сколько раз ФП $\mu_{\tilde{A}}(u_i)$ больше ФП $\mu_{\tilde{A}}(u_j)$.

Вводится балльная шкала, значения которой соответствуют шкале интенсивности в рамках терма «уровень опасности конкретного типа компьютерных атак для информационной безопасности КФС». В соответствии с этой балльной шкалой назначаются значения элемента b_{ij} матрицы отношений B, поскольку однозначно определено, что $b_{ij} = 1,$ и с целью согласования оценок ЛПР установлено, что $b_{ij} = 1/b_{ji}$, причем символом b_{ji} обозначен любой иной элемент в *i*-й строке матрицы отношений, кроме однозначно определенного элемента $b_{ij} = 1$. Важно отметить, что количество вопросов к ЛПР для формулировки его результирующих мнений будет не n^2, а $(n^2 - n)/2$.

Значения ФП $\mu_{\tilde{A}}(u_1)$, ..., $\mu_{\tilde{A}}(u_n)$ в точках сравнения u_1, ..., u_n определяются путем решения задачи о вычислении собственного вектора матрицы отношений *B*:

$$B W^{\mathrm{T}} = v_{\max} W,$$

где $W = (w_1, \ldots, w_n)$ – соответствующий собственный вектор; $v_{\max}$ – максимальное собственное число матрицы отношений *B*; $^{\mathrm{T}}$ – знак транспонирования матрицы.

Решение этой задачи является единственным и всегда существует, т. к. матрица отношений *B* является положительно определенной матрицей. Тогда можно показать, что ФП равна

$$\mu_{\tilde{A}}(u_i) = w_i / \sum_{i=1}^{n} w_i .$$

В итоге значения ФП $\mu_{\tilde{A}}(u_i)$, характеризующей, в рамках ПР по управлению информацией и событиями безопасности, текущий уровень опасности конкретного типа компьютерных атак для информационной безопасности КФС, оказываются измеренными в шкале отношений.

Помимо того, что рассмотренный подход (благодаря вычислению собственного вектора матрицы отношений *B*) позволяет измерять ФП в балльной шкале отношений, он обладает и другими неоспоримыми достоинствами. В частности, простая вероятностная схема позволяет учесть несогласованность мнений (оценок) специалистов-экспертов путем использования коэффициента несогласованности λ:

$$\lambda = (\nu_{\max} - n) / n \ , \ \lambda \geq 0 \ ,$$

где значение $\lambda = 0$ соответствует полной согласованности их мнений (суждений, оценок), например, об уровне опасности конкретного типа компьютерных атак для информационной безопасности. Кроме того, практикуемая при данном подходе процедура парных сравнений является достаточно удобной и несложной для ЛПР, ибо она не навязывает ему априорных ограничений (например, не требует транзитивности суждений).

В работах [13, 15] также предложен подход к построению ФП типа $< b, d_1, e_2, N >$. Сущность данного подхода заключается в параметрическом определении ФП с участием одиночного, обособленного индивидуума – ЛПР, – который должен напрямую оценить параметры ФП с учетом того факта, что вид самой функции задается явно (постулативно, аксиоматически). Примером может служить ситуация, когда ФП имеет треугольную форму, в этом случае ЛПР отмечает (определяет) такие параметры ФП u_1, u_2, u_3, при которых эта функция имеет все нулевые и одно единичное значения. Например, если $\mu_{\tilde{A}}(u_2) = 1$, то для всех $u \le u_1, \ u \ge u_3$ получается $\mu_{\tilde{A}}(u) = 0$.

Тривиальность данного подхода с точки зрения практического построения ФП, а также компактность параметрического представления ФП являются достоинствами метода, но эти достоинства обусловлены априорным исследованием адекватности используемых форм (треугольной, трапецеидальной, в виде колокола и др.) и соответствующих этим формам аналитических описаний ФП, характеризующих, например, текущий уровень (степень) опасности конкретного типа компьютерных атак для информационной безопасности КФС.

В работе [16] рассмотрены теоретические аспекты построения ФП на основе алгоритма, использующего типовой комплект форм (графиков) ФП. В рамках этого алгоритма ЛПР останавливает свой выбор на наиболее подходящей ему форме (графике) ФП из типового комплекта, а затем, в диалоге с ЭВМ, устанавливает его параметры и, в случае необходимости, корректирует эти параметры.

Научный теоретический и практический интерес, с точки зрения построения ФП, характеризующих текущий уровень (степень) опасности конкретного типа компьютерных атак для информационной безопасности КФС, на наш взгляд, может представлять метод равноделения (метод психологического шкалирования). Известен алгоритм, базирующийся на процедуре $< b, d_1, e_2, N >$ построения ФП для термов лингвистической переменной с числовой областью определения на основе метода равноделения. Здесь лицу, принимающему решения, одна за другой предъявляется несколько пар точек интервала с возможными значениями ФП. При каждом предъявлении ЛПР должно назвать среднюю по принадлежности точку интервала, а по набору этих точек с помощью метода интерполяции определяется искомая ФП.

Построение функции принадлежности на основе анализа функций плотности вероятности

Для практических задач нечеткого управления информацией и событиями безопасности наиболее приемлем, на наш взгляд, алгоритм построения ФП на базе анализа функций плотности вероятности.

Этот подход присущ классу алгоритмов $< b, d_1, e_2, N >$. Он основан на отображении ФП через функции от плотности вероятности четких случайных границ между термами лингвистической переменной.

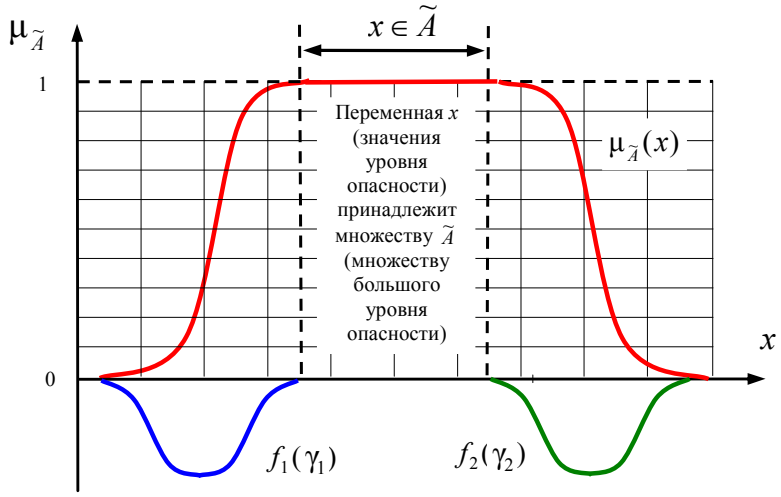
Рассмотрим этот алгоритм построения ФП подробнее в приложении к задачам ПР по управлению информацией и событиями безопасности, например, к задаче ПР о принадлежности конкретной компьютерной атаки к нечеткому множеству опасных атак (множеству атак большого уровня опасности).

Пусть некоторое множество A имеет физический смысл терма-множества значений лингвистической переменной «большой уровень опасности конкретного типа компьютерных атак для информационной безопасности» и описывается интервалом (γ_1, γ_2). В этом случае если параметр (объект) x – уровень опасности конкретного типа компьютерных атак $x > \gamma_1$ и $x < \gamma_2$, то $x \in A$, иначе $x \notin A$.

Множество A считается нечетким множеством $\tilde{A}$, поскольку γ_1 и γ_2 – случайные величины. Этот факт обусловлен тем, что имеются параметры (значения уровня опасности конкретно-

го типа компьютерных атак) x, относительно которых нельзя определенно утверждать, принадлежат ли они множеству A (множеству большого уровня опасности конкретного типа компьютерных атак) или не принадлежат.

Пусть $f_1(\gamma_1)$ и $f_2(\gamma_2)$ – функции плотности вероятности нижней и верхней границ уровня принадлежности переменной x (значения уровня опасности) к множеству A (множеству большого уровня опасности) соответственно (рис.).



Графическая интерпретация построения функции принадлежности в задаче принятия решения о принадлежности конкретной атаки к нечеткому множеству опасных атак на основе анализа функций плотности вероятности

Если ФП имеет вероятностный вид, ее значение $\mu_{\tilde{A}}(x)$, характеризующее, в нашем случае, текущий уровень опасности конкретного типа компьютерных атак для информационной безопасности КФС, определяется в соответствии с выражением

$$\mu_{\tilde{A}}(x) = P(x \in A).$$

С учетом случайного характера величин γ_1 и γ_2, характеризуемых функциями плотности вероятности нижней и верхней границ уровня принадлежности переменной x (значения уровня опасности) множеству A (множеству большого уровня опасности), получаем

$$\mu_{\tilde{A}}(x) = P(\gamma_1 < x < \gamma_2).$$

Значение ФП для нашей задачи ПР о принадлежности конкретной компьютерной атаки нечеткому множеству опасных атак (множеству атак большого уровня опасности) может быть определено (с учетом независимости случайных величин γ_1 и γ_2) как

$$\mu_{\tilde{A}}(x) = P(x > \gamma_1)\, P(x < \gamma_2).$$

Обозначим вероятностную меру $\int_{-\infty}^{x} f_1(\gamma_1)\, d\gamma$ (см. рис.) через $F_1(x)$, а $\int_{-\infty}^{x} f_2(\gamma_2)\, d\gamma$ – через $F_2(x)$. Исходя из того, что $F_1(x) = P(\gamma_1 < x)$, получаем окончательное значение ФП для задачи ПР (ППР) в рамках нечеткого управления информацией и событиями безопасности: принадлежит ли конкретная компьютерная атака уровня x нечеткому множеству $\tilde{A}$ опасных атак (множеству атак большого уровня опасности)

$$\mu_{\tilde{A}}(x) = F_1(x)\,[1 - F_2(x)].$$

Таким образом, предложенный методологический подход предоставляет возможность определять значения ФП в задачах нечеткого управления информацией и событиями безопасности, причем значения $\mu_{\tilde{A}}(x)$, найденные на основе анализа функций плотности вероятности по отношению к значениям, получаемым на основе других методов, не требуют дополнительного анализа вида графиков функций активации нечетких множеств, не нуждаются в согласовании оценок экспертов.

Заключение

В ходе исследования установлено, что определять функции принадлежности $\mu_{\tilde{A}}(x)$ в задачах принятия решений (поддержки принятия решений) в рамках нечеткого управления информацией и событиями безопасности можно не только с помощью процедур непосредственного опроса специалистов-экспертов, но и на основе корректных математических процедур преобразования функций плотности распределения вероятности ($F_1(x)$ и $F_1(x)$) случайных границ между термами лингвистической переменной, характеризующей уровень опасности конкретного типа компьютерных атак для информационной безопасности КФС. При этом сами функции $F_1(x)$ и $F_2(x)$ для задач такого класса могут быть построены как на основе сбора и анализа статистики, так и с помощью экспертного опроса.

Таким образом, обсуждены и проанализированы несколько методов построения ФП в приложении к задачам принятия решений (поддержки принятия решений) в рамках нечеткого управления информацией и событиями безопасности КФС. Эти методы не обладают большой математической и вычислительной сложностью, но позволяют учесть неопределенность (нечеткость) наблюдаемых и управляемых параметров защищенности, что дает возможность повысить достоверность контроля информации и событий безопасности современных КФС.

СПИСОК ЛИТЕРАТУРЫ

1. *Kotenko I. V., Parashchuk I. B.* Synthesis of controlled parameters of cyber-physical-social systems for monitoring of security incidents in conditions of uncertainty // Journal of Physics: Conference Series, IOP Publishing. 2018. N. 1069 (1): 012153. P. 1–6.

2. *Sun Y.* Research on Security Issues and Protection Strategy of Computer Network // The Open Automation and Control Systems Journal. 2015. N. 7. P. 2097–2101.

3. *Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Тр. СПИИРАН. 2012. Вып. 1 (20). С. 27–56.

4. *Miller D. R., Harris S., Vandyke S.* Security Information and Event Management (SIEM) implementation. New York: Mc Graw Hill, 2011. 430 p.

5. *Kizza J. M.* Guide to Computer Network Security: 3rd ed. New York: Springer, 2015. 545 p.

6. *Pfleeger C. P., Pfleeger S. L.* Security in Computing. New Jersey: Prentice Hall, 2015. 944 p.

7. *Dordal P. L.* An Introduction to Computer Networks. Release 1.9.0. URL: https://archive.org/details/academictorrents_958e2487d2db5f41f9c056bb35cf547edf38528f (дата обращения: 03.04.2021).

8. *Рыболовлев Д. А., Карасев С. В., Поляков С. А.* Классификация современных систем управления инцидентами безопасности // Вопр. кибербезопасности. 2018. № 3 (27). С. 47–53.

9. *Jacobs J., Rudis B.* Data-Driven Security: Analysis, Visualization and Dashboards: 1st ed. New York: John Wiley & Sons, Inc., 2014. 352 p.

10. *Talabis M., McPherson R., Miyamoto I., Martin J.* Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data: 1st ed. New York: Syngress Media, 2014. 182 p.

11. *Wheeler E.* Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. New York: Syngress Media, 2011. 424 p.

12. *Zubarev I. V., Zhidkov I. V., Kadushkin A. V., Medovshchikova S. A.* Vulnerabilities in information systems // Information and mathematical technologies in science and management. 2016. N. 3. P. 174–185.

13. *Паращук И. Б., Бобрик И. П.* Нечеткие множества в задачах анализа сетей связи. СПб.: ВУС, 2001. 80 с.

14. *Усков А. А.* Системы с нечеткими моделями объектов управления. Смоленск: СФРУК, 2013. 153 с.

15. *Назаров Д. М., Конышева Л. К.* Интеллектуальные системы: основы теории нечетких множеств: учеб. пособие для академического бакалавриата. М.: Юрайт, 2019. 186 с.

16. *Алексеев А. В.* Интерпретация и определение функций принадлежности нечетких множеств // Методы и системы принятия решений. Рига: РПИ, 1979. С. 42–50.

Статья поступила в редакцию 15.04.2021

ИНФОРМАЦИЯ ОБ АВТОРАХ

Игорь Витальевич Котенко – д-р техн. наук, профессор; зав. лабораторией проблем компьютерной безопасности; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; Россия, 199178, Санкт-Петербург; ivkote@comsec.spb.ru.

Игорь Борисович Паращук – д-р техн. наук, профессор; ведущий научный сотрудник лаборатории проблем компьютерной безопасности; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; Россия, 199178, Санкт-Петербург; shchuk@rambler.ru.

FUZZY MANAGEMENT OF INFORMATION AND SECURITY EVENTS: FEATURES OF CONSTRUCTING MEMBERSHIP FUNCTIONS

I. V. Kotenko, I. B. Parashchuk

St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg, Russian Federation

Abstract. The object of the study is methodological approaches to solving the problems of constructing membership functions in the application to decision-making procedures (decision support) for the fuzzy management of information and security events of modern cyber-physical systems. These methodological approaches (methods) allow taking into account the vagueness of the observed and controlled parameters of the protection of complex controlled technical systems. At the same time, the comparative analysis of the approaches under consideration is focused on the most applicable methods for specific tasks - the method of constructing membership functions based on the analysis of probability density functions and the method using a simple probabilistic scheme. Based on the method that uses the analysis of probability density functions, a mechanism for determining the values of membership functions for the problem of making decisions about the relevance of a particular computer attack to a fuzzy set of dangerous attacks (a set of attacks of a high level of danger) is proposed. This mechanism does not have a great mathematical and computational complexity, but it allows us to take into account the fuzziness of the observed and controlled security parameters, which will increase the reliability of monitoring information and security events within the framework of fuzzy security management of systems of this class.

Key words: security information and event management, fuzzy management, decision making, membership function, method, fuzzy set, probability.

For citation: Kotenko I. V., Parashchuk I. B. Fuzzy management of information and security events: features of constructing membership functions. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2021;3:7-15. (In Russ.) DOI: 10.24143/2072-9502-2021-3-7-15.

REFERENCES

1. Kotenko I. V., Parashchuk I. B. Synthesis of controlled parameters of cyber-physical-social systems for monitoring of security incidents in conditions of uncertainty. *Journal of Physics: Conference Series, IOP Publishing*, 2018, no. 1069 (1): 012153, pp. 1-6.
2. Sun Y. Research on Security Issues and Protection Strategy of Computer Network. *The Open Automation and Control Systems Journal*, 2015, no. 7, pp. 2097-2101.
3. Kotenko I. V., Saenko I. B., Polubelova O. V., Chechulin A. A. Primenenie tekhnologii upravleniia informatsiei i sobytiiami bezopasnosti dlia zashchity informatsii v kriticheski vazhnykh infrastrukturakh [Applying security information and event management technology to protect information in critical infrastructures]. *Trudy SPIIRAN*, 2012, iss. 1 (20), pp. 27-56.
4. Miller D. R., Harris S., Vandyke S. *Security Information and Event Management (SIEM) implementation*. New York, McGrawHill, 2011. 430 p.
5. Kizza J. M. *Guide to Computer Network Security*. New York, Springer, 2015. 545 p.

6. Pfleeger C. P., Pfleeger S. L. *Security in Computing*. New Jersey, Prentice Hall, 2015. 944 p.

7. Dordal P. L. *An Introduction to Computer Networks. Release 1.9.0.* Available at: https: // archive.org/details/academictorrents_958e2487d2db5f41f9c056bb35cf547edf38528f (accessed: 03.04.2021).

8. Rybolovlev D. A., Karasev S. V., Poliakov S. A. Klassifikatsiia sovremennykh sistem upravleniia intsidentami bezopasnosti [Classification of modern security incident management systems]. *Voprosy kiberbezopasnosti*, 2018, no. 3 (27), pp. 47-53.

9. Jacobs J., Rudis B. *Data-Driven Security: Analysis, Visualization and Dashboards*. New York, John Wiley & Sons, Inc., 2014. 352 p.

10. Talabis M., McPherson R., Miyamoto I., Martin J. *Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data*. New York, Syngress Media, 2014. 182 p.

11. Wheeler E. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. New York, Syngress Media, 2011. 424 p.

12. Zubarev I. V., Zhidkov I. V., Kadushkin A. V., Medovshchikova S. A. Vulnerabilities in information systems. *Information and mathematical technologies in science and mana*gement, 2016, no. 3, pp. 174-185.

13. Parashchuk I. B., Bobrik I. P. *Nechetkie mnozhestva v zadachakh analiza setei sviazi* [Fuzzy sets in analysis of communication networks]. Saint-Petersburg, VUS Publ., 2001. 80 p.

14. Uskov A. A. *Sistemy s nechetkimi modeliami ob"ektov upravleniia* [Systems with fuzzy models of control objects]. Smolensk, SFRUK Publ., 2013. 153 p.

15. Nazarov D. M., Konysheva L. K. *Intellektual'nye sistemy: osnovy teorii nechetkikh mnozhestv: uchebnoe posobie dlia akademicheskogo bakalavriata* [Intelligent systems: fundamentals of fuzzy set theory: teaching aids for academic bachelor's degree]. Moscow, Iurait Publ., 2019. 186 p.

16. Alekseev A. V. Interpretatsiia i opredelenie funktsii prinadlezhnosti nechetkikh mnozhestv [Interpretation and definition of membership functions of fuzzy sets]. *Metody i sistemy priniatiia reshenii*. Riga, RPI Publ., 1979. Pp. 42-50.

The article submitted to the editors 15.04.2021

INFORMATION ABOUT AUTHORS

Igor V. Kotenko – Doctor of Technical Sciences, Professor, Head of the Laboratory of Computer Security Problems; St. Petersburg Federal Research Center of the Russian Academy of Sciences; Russia, 199178, Saint-Petersburg; ivkote@comsec.spb.ru.

Igor B. Parashchuk – Doctor of Technical Sciences, Professor; Leading Researcher of the Laboratory of Computer Security Problems; St. Petersburg Federal Research Center of the Russian Academy of Sciences; Russia, 199178, Saint-Petersburg; shchuk@rambler.ru.