ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.05
CC BY 4.0
DOI: 10.21822/2073-6185-2024-51-3-163-171 Оригинальная статья /Original article

Методический подход к количественной оценке защищенности открытых операционных систем АС ОВД

А.И. Янгиров[1], И.М. Янгиров[2], Е.А. Рогозин[3], С.Б. Ахлюстин[4]
[1,2] ФКУ «НИЦ «Охрана» Росгвардии,
[1,2] 111539, г. Москва, Реутовская, 12Б, Россия,
[3,4] Воронежский институт МВД России,
[3,4] 394065, г. Воронеж, проспект Патриотов, 53, Россия

Резюме. Цель. В статье рассмотрены положения подхода нечеткой логики применительно к методу количественной оценки защищенности открытых операционных систем (далее – ОС) автоматизированных систем органов внутренних дел Российской Федерации (далее – АС ОВД РФ) с учетом вероятных угроз безопасности и требований стандарта ГОСТ Р ИСО/МЭК 15408 для нивелирования возможных последствий. Информационным сообщением от 18 октября 2016 г., № 240/24/4893 «Об утверждении Требований безопасности информации к операционным системам» ФСТЭК России определено 6 классов защищенности ОС. ОС, соответствующие 1, 2 и 3 классам защиты, применяются в информационных (автоматизированных) системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, ОС, соответствующие 4, 5 и 6 классам защиты, не предназначены для обработки таких сведений. В представленном исследовании под открытыми ОС АС ОВД РФ понимаются ОС АС ОВД, в которых не обрабатывается информация, содержащая сведения, составляющие государственную тайну. **Метод.** Исследование проведено на основе метода анализа возможных угроз безопасности открытых ОС, а также требований стандарта ГОСТ Р ИСО/МЭК 15408, с применением положений нечеткой логики. **Результат.** Результатом работы автоматизированной системы расчета показателя защищенности анализируемой открытой ОС является один из заданных критериев показателей степени защищенности ОС, основанный на положениях нечеткой логики. **Вывод.** Авторами предложен метод оценки защищенности открытых ОС АС ОВД РФ, основанный на положениях нечеткой логики.

Ключевые слова: оценка защищенности, требования безопасности, банк данных угроз безопасности информации, показатель защищенности, критерии защищенности, операционная система, автоматизированная система расчета

Для цитирования: А.И. Янгиров, И.М. Янгиров, Е.А. Рогозин, С.Б. Ахлюстин. Методический подход к количественной оценке защищенности открытых операционных систем АС ОВД. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(3):163-171. DOI:10.21822/2073-6185-2024-51-3-163-171

Methodological approach to quantitative assessment of the security of open operating systems AS of the Internal Affairs Bodies

A.I. Yangirov[1], I.M. Yangirov[2], E.A. Rogozin[3], S.B. Akhlyustin [4]
[1,2] FSI «SRC «OKHRANA» of the Federal service of National Guard of Russia,
[1,2] 12B Reutovskaya St., Moscow 111539, Russia,
[3,4] Voronezh Institute of the Ministry of Internal Affairs of Russia,
[3,4] 53 Patriots Ave., Voronezh 394065, Russia

Abstract. Objective. The article considers the provisions of the fuzzy logic approach in relation to the method of quantifying the security of open operating systems (OS) of automated systems of the internal affairs bodies of the Russian Federation (AS of the Russian Federation), taking into account possible security threats and the requirements of the standard GOST

R ISO/IEC 15408 for leveling possible consequences. Information Message № 240/24/4893 dated October 18, 2016 «On Approval of Information Security Requirements for Operating Systems» of the FSTEC of Russia defines 6 OS security classes. Operating systems corresponding to protection classes 1, 2 and 3 are used in information (automated) systems in which information containing information constituting a state secret is processed, operating systems corresponding to protection classes 4, 5 and 6 are not intended for processing such information. In the presented study, the open operating systems of the AS of the Russian Federation are understood as OS AS, in which information containing information constituting a state secret is not processed. **Method.** The study was conducted based on the method of analyzing possible security threats to open operating systems, as well as the requirements of GOST R ISO/IEC 15408 standard, using the provisions of fuzzy logic. **Result.** The result of the automated system for calculating the security index of the analyzed open OS is one of the specified criteria for the degree of security of the OS, based on the provisions of fuzzy logic. **Conclusion.** The authors propose a method for assessing the security of open OS of the AS of the Russian Federation, based on the provisions of fuzzy logic.

Keywords: security assessment, security requirements, data bank of information security threats, security indicator, security criteria, operating system, automated calculation system

For citation: A.I. Yangirov, I.M. Yangirov, E.A. Rogozin, S.B. Akhlyustin. Methodological approach to quantitative assessment of the security of open operating systems AS of the Internal Affairs Bodies. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(3):163-171. DOI:10.21822/2073-6185-2024-51-3-163-171.

Введение. Значительная часть задач, с которыми мы сталкиваемся в различных сферах знаний, периодически становятся слишком сложными и многоаспектными из-за большого количества факторов, которые должны быть учтены при достижении определенной научной цели. Для решения подобных задач не всегда применимы исключительно точные и строго определенные модели и алгоритмы. Многие определения и понятия по своей сути обладают нечетким характером из-за индивидуальности человеческих суждений, приближенности мнений и их дальнейшего лексического описания.

Традиционные методы решения научных задач в условиях размытости факторов обычно ограничиваются учетом только незначительных изменений, что не предоставляет возможности для учета различных вариаций в структуре модели.

Для получения оценочных критериев необходимо обладать достаточным количеством информации. Однако в задачах обеспечения безопасности такая информация редко доступна, и поэтому использование только теоретико-вероятностного подхода оказывается затруднительным. Решение таких задач требует гибкого подхода, так как использование моделей и алгоритмов, основанных на бинарной логике (истина или ложь) и точных параметрах, ограничивает возможности получения результатов, которые должны отражать показатели максимально приближенные к реальным.

Для решения подобных задач также зачастую применяются экспертные оценки и другая информация, которая характеризуется субъективной неопределенностью. Наличие многокритериальности в определенных научных задачах также является своего рода элементом субъективной неопределенности, свойственным оценке информационной безопасности. В таких условиях требуется использование соответствующего математического инструментария при решении вопросов оценки информационной защищенности.

На сегодняшний день нечеткая логика, разработанная и представленная в работах Лотфи Аскера Заде, является одним из перспективных направлений научных исследований при анализе, долгосрочном прогнозировании и создании рабочих моделей явлений и процессов, которые сложно формализуемы и трудно поддаются структуризации.

Данный подход отличается от традиционной математической логики тем, что не требует точно сформированных закономерных действий на каждом шаге модели-

рования. Возможности нечеткой логики позволяют перевести процесс моделирования на более высокий уровень, базируясь на минимальном наборе закономерностей.

Постановка задачи. Целью исследования является применение положений подхода нечеткой логики относительно метода количественной оценки защищенности открытых ОС АС ОВД РФ с учетом вероятных угроз безопасности и требований стандарта ГОСТ Р ИСО/МЭК 15408 для нивелирования возможных последствий. Подробное описание рассматриваемой методики расчета оценки защищенности открытых ОС ОВД РФ ранее было представлено в статьях, посвященных разработке автоматизированной системы расчета оценки защищенности ОС на основе анализа требований безопасности.

Методы исследования. Исследования основаны на методах анализа возможных угроз безопасности ОС и требований стандарта ГОСТ Р ИСО/МЭК 15408, количественной оценки требований безопасности ОС АС ОВД РФ с применением положений нечеткой логики.

Основополагающий принцип нечеткой логики заключается в принятии неопределенности как неотъемлемого элемента реального мира. Что отличает нечеткую логику от традиционного бинарного подхода, это - способность работать с понятиями, которые не могут быть определены однозначно как полностью истиные или ложные, а имеют определенную степень вероятности или принадлежности. Применение нечеткой логики находит востребование в различных областях, включая управление процессами, принятие решений и распознавание образов.

Гибкость и способность адаптироваться к неопределенным данным делают нечеткую логику ценным инструментом для решения различных задач. Вместо жесткого деления между истинностью и ложностью, нечеткая логика оперирует понятиями принадлежности и степенями истинности, что позволяет учесть различную степень неопределенности и более точно описать нечеткие понятия, такие как «небольшой» или «быстрый».

В контексте информационной безопасности, данная проблема обладает значительной актуальностью. Оптимальность при принятии решений составляют целостность и безопасность системы, гарантируя достижение максимальной эффективности в обеспечении безопасности, с одной стороны.

С другой же стороны, важно отметить, что оценка и управление информационной безопасностью связаны с наличием случайных факторов и неточностей. В связи с этим математическая модель должна быть построена таким образом, чтобы не только адекватно отражать сущность моделируемых процессов и явлений, но и учитывать условия неопределенности.

В традиционных подходах, случайности в естественных процессах в основном рассматриваются с точки зрения вероятностного значения. Однако такой подход не всегда корректен, на практике неопределенность часто зависит от субъективных оценок. Кроме того, в области обеспечения безопасности, обычно невозможно однозначно определить частоту проявлений отдельных событий.

Применение математического подхода, основанного на нечеткой логике, имеет свои преимущества. Прежде всего, данный подход позволяет описывать условия и решать задачи на достаточно понятном языке. Более того, отмечается его универсальность, и как следствие, высокая эффективность.

Однако необходимо отметить и некоторые недостатки. В базовом наборе правил, составляемых экспертом, могут быть пропущены необходимые элементы или возникнуть противоречия. Кроме того, выбор вида и параметров функций принадлежности, описывающих входные и выходные переменные системы, является субъективным и могут недостаточно точно отражать реальность.

Примечательно, что термин «нечеткий» вызывает некоторое беспокойство у лиц, принимающих решения о выборе методов для осуществления проектов. «Нечеткость» ассоциируется с неуверенностью и возможным недостатком надежности будущей системы.

Следует отметить, что компьютерные модели, основанные на нечеткой логике, достаточно точны и конкретизированы в отношении определенной ситуации, поступающей на вход модели. Такие модели обладают преимуществом в обработке входной информации, имеющей разнородную качественность, при этом обеспечивается более достоверное описание поведения объекта. То есть нечеткие системы позволяют получить единственное решение для определенной ситуации, учитывая общую степень погрешности, приблизительности и неполноты входных данных.

Так как математический аппарат нечеткой логики является важным инструментом для анализа слабоструктурированных и сложно формализуемых процессов, к которым, в том числе, возможно отнести задачи обеспечения информационной безопасности, рассмотрим основные принципы и идеи, лежащие в основе теории.

Подход нечеткой логики определяется правилами выполнения операций и преобразований с нечеткими множествами с последующим принятий нечетких решений. Основные правила, используемые в нечеткой логике, включают следующие:

1. Принцип нечеткой импликации: определяет, каким образом нечеткое правило влияет на выводы. Формула импликации используется для определения степени принадлежности выводу на основе степени принадлежности входным переменным.

2. Принцип нечеткого объединения: определяет, как объединить два или более нечетких множества в одно. Это может быть выполнено, например, через операцию объединения (логическое «или») или через алгоритмы агрегации, такие как максимум или среднее значение.

3. Принцип нечеткого пересечения: определяет, как выполнить операцию пересечения двух или более нечетких множеств. Это может быть выполнено, например, через операцию пересечения (логическое «и») или через алгоритмы, такие как минимум или произведение.

4. Принцип нечеткого вычисления: определяет, как вычислить степень принадлежности результату на основе степени принадлежности входных переменных и правил нечеткой логики.

5. Принцип агрегации выводов: определяет, как объединить несколько выводов для получения окончательного решения. Это может быть выполнено, например, через операцию объединения (логическое «и») или через алгоритмы агрегации, такие как максимум или среднее значение.

6. Принцип дефаззификации: определяет, как преобразовать нечеткое множество в определенное значение. Различные методы могут использоваться для получения точечного значения, такие как центр тяжести, средневзвешенное значение или другие алгоритмы.

Все эти правила и принципы помогают в исполнении операций и принятии нечетких решений на основе нечетких данных для достижения более гибкого и адаптивного подхода в логических вычислениях.

Правила нечеткой логики позволяют работать с размытыми и неопределенными понятиями и данными. В этой теории также могут использоваться нечеткие множества, которые содержат элементы, принадлежность которых является частичной. Для описания нечетких множеств используются функции принадлежности, которые определяют, насколько элементы относятся к этим множествам. Значения функции принадлежности варьируются от 0 до 1, где 0 – означает полное отсутствие принадлежности, а 1 – полную принадлежность.

На практике, функции принадлежности обычно представляются графически с помощью кривых или графиков. Используются различные формы функций, такие как треугольные, гауссовы или трапециевидные, возможно комбинирование нескольких типов на одном графике. Основной принцип заключается в том, что, чем выше значение функции принадлежности, тем больше элемент относится к определенному множеству. При построении нечетких множеств выбирают форму функции принадлежности (исходя из

исходных данных), определяют ее параметры, после чего отмечают значения, чтобы они наилучшим образом отражали интересующие нас характеристики.

Для более ясного понимания принципов работы нечеткой логики можно рассмотреть простейший пример. Рассмотрим такое нечеткое понятие как «температура чая». Чай может быть различной температуры, следовательно, возможно введение нечеткого терм-множества, состоящего из следующих основных переменных: «холодный», «теплый», «горячий». Определим, что температура рассматривается от 0 до 100 °С, так как при 0 °С вода становится льдом, а при 100 °С начинается процесс испарения. Таким образом, получим область рассуждений в виде T = [0; 100]. Восприятие температуры у людей может разниться. Например, один человек может охарактеризовать температуру чая термином «холодный», если она ниже комнатной температуры, в то время как другие люди будут считать такую температуру «теплой» или даже «горячей». Допустим, что для всех чай является «холодным», если его температура находится в пределах от 0°С до 20°С. Более высокие температуры люди из выборки определяют по-разному, в зависимости от своих предпочтений, однако для всех людей чай считается «теплым» при T = [40; 60] °С. Горячим обычно признается чай от 80 °С и выше.

Функция принадлежности для понятия «холодный чай» может быть построена таким образом, чтобы отражать различные предпочтения или базироваться на статистических данных о температурных предпочтениях широкой аудитории.

Так, при температурах от 0 до 20 °С возможно однозначно интерпретировать чай «холодным» и принадлежность его к данному множеству будет равна 1. По мере удаления от этой точки значение функции будет уменьшаться, указывая на уменьшение принадлежности к понятию. Функция принадлежности – Q(T) принимает значения от 0 до 1, где 0 – означает полное отсутствие принадлежности, а 1 – полную принадлежность.

Обобщив вышесказанное, можем представить функцию принадлежности температуры чая к множеству «холодный» в трапецеидальном виде. Аналогичным образом можно построить функции принадлежности к нечетким переменным «теплый», «горячий» (рис. 1).

$$\mathrm{Q_{хол}}(T°\mathrm{C}) = \begin{cases} 1, & T \in [0;20]; \\ 1 - \dfrac{T-20}{20}, & T \in (20;40); \\ 0, \text{ в остальных случаях} \end{cases}$$

$$\mathrm{Q_{теп}}(T°\mathrm{C}) = \begin{cases} 1 - \dfrac{40-T}{20}, & T \in (20;40); \\ 1, & T \in [40;60]; \\ 1 - \dfrac{T-60}{20}, & T \in (60;80); \\ 0, \text{ в остальных случаях} \end{cases}$$

$$\mathrm{Q_{гор}}(T°\mathrm{C}) = \begin{cases} 1 - \dfrac{80-T}{20}, & T \in (60;80); \\ 1, & T \in [80;100]; \\ 0, \text{ в остальных случаях} \end{cases}$$

Рис. 1. Функции принадлежности к нечетким переменным «холодный», «теплый», «горячий»
Fig. 1. Membership functions for fuzzy variables “cold”, “warm”, “hot”

На рис. 1 $Q_{хол}(T^{\circ}C)$ – принадлежность к множеству «холодный», $Q_{теп}(T^{\circ}C)$ – принадлежность к множеству «теплый», $Q_{гор}(T^{\circ}C)$ – принадлежность к множеству «горячий», T – температура.

Отобразим полученные значения на графике функции соответствия диапазонов принадлежности температуры (рис. 2). Множество «холодный» (от 0 до 40) обозначено синим цветом, множество «теплый» (от 20 до 80) обозначено желтым цветом, множество «горячий» (от 60 до 100) обозначено красным цветом.

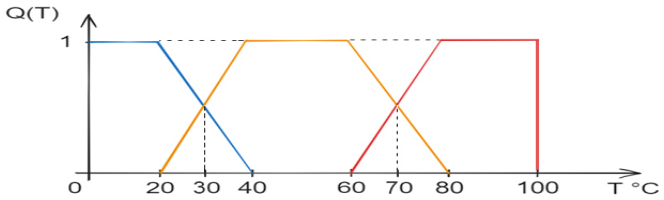

Рис. 2. График функции соответствия диапазонов принадлежности температуры
Fig. 2. Graph of the correspondence function of temperature membership ranges

Учитывая пересечения областей получаем, что к множеству «холодный» температура относится от 0 °С (включительно) до 30 °С (включительно), к множеству «теплый» температура относится от 30 до 70 °С (включительно), к множеству горячий температура относится от 70 до 100 °С (включительно).

Обсуждение результатов. В сфере информационной безопасности данный подход также может обеспечить возможность оценки различных критериев. Оптимальность при принятии решений является одним из ключевых аспектов обеспечения целостности и безопасности ОС, позволяя достигать максимальной эффективности в обеспечении защищенности. Вместе с тем, при обеспечении защиты ОС также необходимо учитывать наличие возможных случайных факторов и неточностей. Поэтому математическая модель должна быть построена таким образом, чтобы достаточно точно отражать сущность моделируемых процессов и явлений, учитывая при этом условия неопределенности.

В ранее опубликованных исследованиях, посвященных разработке автоматизированной системы для оценки степени защищенности открытых ОС ОВД РФ, представлена взаимозависимая связь между определенными критериями, которые определяют уровень защищенности ОС [1-4]. Исследования основывались на анализе требований безопасности в соответствии с ГОСТ Р ИСО/МЭК 15408 и потенциальных угроз.

В результате работы программы выводится лингвистический показатель защищенности, который зависит от количественной оценки требований безопасности и определяет уровень защищенности: «низкий», «средний» или «высокий». Для представленного программного обеспечения и реализованного в нем подхода возможно применение положений нечеткой логики, которые могли бы позволить учесть неопределенность и субъективность предложенных лингвистических показателей, а также другие обстоятельства, возникающие при эксплуатации ОС, оценке ОС, некорректной настройке ОС и тому подобном.

На данный момент в банке данных угроз безопасности информации, разработанном ФАУ «ГНИИИ ПТЗИ ФСТЭК России», имеется 222 угрозы, каждая из которых имеет определенное количество последствий [6]. При реализации какой-либо угрозы выделены следующие типы последствий: «нарушение конфиденциальности», «нарушение целостности» и «нарушение доступности». Представленные последствия проявляются в зависимости от типа реализованной угрозы. В зависимости от потенциала угрозы ОС может проявиться от 1 до 3 последствий, что позволяет распределить угрозы с учетом количества этих последствий. При анализе угроз безопасности можно выделить следующие категории, основанные на количестве последствий:

1) угрозы, имеющие 1 последствие (88 шт.);
2) угрозы, имеющие 2 последствия (52 шт.);
3) угрозы, имеющие 3 последствия (82 шт.).

Для обеспечения функционирования нечеткой логики вводятся определенные правила, которые позволяют классифицировать угрозы в соответствии с их потенциалом. Применительно к разработанному программному обеспечению введем следующие правила:

1) Если будут нивелированы угрозы, которые имеют наибольшее количество последствий, систему можно считать однозначно минимально защищенной (246 шт);

2) Если будут нивелированы угрозы, которые имеют 2 и 3 последствия, систему можно считать средней по уровню защищенности (350 шт);

3) Если будут нивелированы угрозы, имеющие 1, 2 и 3 последствия, систему можно считать максимально защищенной (438 шт).

4) Поскольку семейства функциональных требований, требований доверия и других критериев сложно классифицировать по уровню защиты от конкретных последствий, предполагается, что они нивелируются равномерно (отсутствие определенного требования не позволяет однозначно сказать, в каком виде выразится уязвимость ОС, так как зависимости требований могут быть многогранны);

5) В методе оценки защищенности открытых ОС АС ОВД применяется эталонный профиль защиты (наиболее защищенный профиль защиты, предназначенный для применения на автоматизированных рабочих местах систем, находящийся в открытом доступе на сайте ФАУ «ГНИИИ ПТЗИ ФСТЭК России», разработанный в соответствии с ГОСТ Р ИСО/МЭК 15408), при реализации всех требований защиты указанного профиля система будет иметь максимальную защищенность.

В соответствии с установленными правилами, определим следующие степени защищенности ОС: «уязвимая система», «минимально защищенная система», «средне защищенная система», «максимально защищенная система». Исходя из изложенных выше данных, приходим к выводу, что наиболее подходящим вариантом функции принадлежности будет треугольная форма. Учитывая рассмотренные ранее данные и введенные правила сформируем функции принадлежности защищенности открытых ОС (рис. 3).

$$Q_{у}(N_{п}) = \begin{cases} 1 - \frac{N_{п}}{246}, N_{п} \in [0; 246); \\ 0, \text{в остальных случаях.} \end{cases}$$

$$Q_{мин}(N_{п}) = \begin{cases} 1 - \frac{246 - N_{п}}{246}, N_{п} \in [0; 246); \\ 1 - \frac{N_{п} - 246}{104}, N_{п} \in [246; 350); \\ 0, \text{в остальных случаях.} \end{cases}$$

$$Q_{ср}(N_{п}) = \begin{cases} 1 - \frac{350 - N_{п}}{104}, N_{п} \in [246; 350); \\ 1 - \frac{N_{п} - 350}{88}, N_{п} \in [350; 438); \\ 0, \text{в остальных случаях.} \end{cases}$$

$$Q_{макс}(N_{п}) = \begin{cases} 1 - \frac{438 - N_{п}}{88}, N_{п} \in (350; 438]; \\ 0, \text{в остальных случаях.} \end{cases}$$

Рис. 3. Функции принадлежности показателей защищенности открытых ОС
Fig. 3. Membership functions of security indicators of open OS

На рис. 3 $Q_{у}(N_{п})$ – принадлежность к множеству «уязвимая система», $Q_{мин}(N_{п})$ – принадлежность к множеству «минимально защищенная система», $Q_{ср}(N_{п})$ – принадлежность к множеству «средне защищенная система», $Q_{макс}(N_{п})$ – принадлежность к множеству «максимально защищенная система», $N_{п}$ – количество последствий.

На основании функций принадлежности сформируем график функции соответствия диапазонов принадлежности степени защищенности открытых ОС (рис. 4).

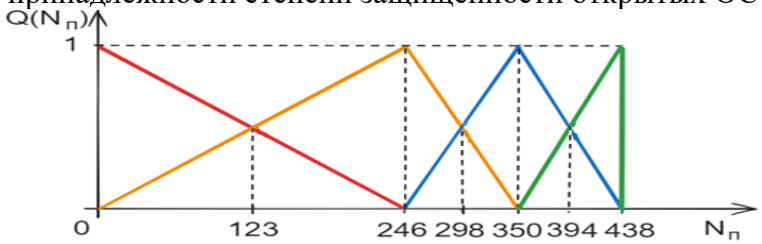

Рис. 4. График функции соответствия диапазонов принадлежности степени защищенности открытых ОС
Fig. 4. Graph of the correspondence function of the ranges of belonging to the degree of protection of open OS

На рис. 4 область принадлежности к множеству «уязвимая система» обозначена красным цветом (от 0 до 246), область принадлежности к множеству «минимально защищенная система» обозначена оранжевым цветом (от 0 до 350), область принадлежности

к множеству «средне защищенная система» обозначена синим цветом (от 246 до 438), область принадлежности к множеству «максимально защищенная система» обозначена зеленым цветом (от 350 до 438). Учитывая пересечения областей принадлежности, степени защищенности открытых ОС предполагают следующие диапазоны: «уязвимая система» – от 0 до 123 (включительно), «минимально защищенная система» – от 123 до 298 (включительно), «средне защищенная система» – от 298 до 394 (включительно), «максимально защищенная система» – от 394 до 438 (включительно).

При рассмотрении данного подхода в контексте разработанного программного обеспечения, стоит отметить, что при использовании эталонного профиля защиты предполагается, что реализация всех его требований (полная реализация на 100%) нивелирует все возможные последствия угроз (в данном случае их число составляет 438). Исходя из этого, выборка угроз напрямую влияет на процент защищенности системы.

Проведем аналогию с другими показателями: если нивелировано до 123 последствий угроз (задействовано примерно до 28% требований) – система может считаться уязвимой, при нивелировании от 123 до 298 последствий угроз (задействовании примерно от 28 до 69% требований) – система может считаться минимально защищенной, при нивелировании от 298 до 394 последствий угроз (задействовании примерно от 69 до 90 % требований) – система может считаться средней защищенности, при нивелировании от 394 до 438 последствий угроз (задействовании примерно от 90 до 100 % требований) – система может считаться максимально защищенной.

Вместе с тем эти данные касаются исключительно случая, когда задействованы одновременно все угрозы и реализуется максимальное количество требований. В случае противодействия меньшему количеству угроз график будет сужаться в левую сторону и значения соответствия параметров защищенности будут изменяться в меньшую сторону.

Вывод. Таким образом, нечеткая логика позволяет учесть неопределенности при оценке степени защищенности открытых ОС. Это важное преимущество, которое делает нечеткую логику востребованной в различных сферах, включая управление, прогнозирование, искусственный интеллект и многие другие. Каждая отдельная система имеет свои особенности, и использование представленного подхода позволяет точнее рассматривать необходимые аспекты, учитывая нюансы и потенциальные риски.

Библиографический список:

1. Алгоритмизация расчета оценки защищенности операционных систем АИС ОВД, разработанного на основе анализа требований безопасности ГОСТ Р ИСО/МЭК 15408 и возможных угроз / А.И. Янгиров, Е.А. Рогозин, О.И. Бокова, С.Б. Ахлюстин // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 3. – С. 167-171. – DOI 10.21822/2073-6185-2023-50-3-167-171. – EDN QIOPOE.
2. К вопросу оценки защищенности операционных систем, использующихся в автоматизированных информационных системах органов внутренних дел / А.И. Янгиров // Охрана, безопасность, связь. – 2023. – № 8-3. – С. 83-90. – EDN SLCGLG.
3. Расчет оценки защищенности открытых операционных систем на основе анализа требований безопасности по ГОСТ р ИСО/МЭК 15408 / А.И. Янгиров, Е.А. Рогозин // Вопросы обеспечения безопасности в киберпространстве: Материалы Всероссийской научно-технической конференции, Махачкала, 16.12.2022. – Махачкала: Дагестанский государственный технический университет, 2022. – С. 243-248. – EDN EDHHEY.
4. Разработка автоматизированной системы расчета оценки защищенности операционных систем информационных систем на основе анализа требований безопасности / А.И. Янгиров, Е.А. Рогозин, Е.Ю. Никулина, А.В. Калач // Вестник Воронежского института ФСИН России. – 2022. – № 4. – С. 182-188. – EDN BNBXNZ.
5. Информационное сообщение от 18 октября 2016 г. № 240/24/4893 «Об утверждении Требований безопасности информации к операционным системам» ФСТЭК России – [Электронный ресурс] – Режим доступа. – URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-18-oktyabrya-2016-g-n-240-24-4893 (Дата обращения: 01.02.2024).
6. Банк данных угроз безопасности информации – [Электронный ресурс] – Режим доступа. – URL: https://bdu.fstec.ru/ (Дата обращения: 01.02.2024).

7. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности [Электронный ресурс] – Режим доступа. – URL: https://docs.cntd.ru/document/1200105710 (Дата обращения: 27.12.2023).
8. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности [Электронный ресурс] – Режим доступа. – URL: https://docs.cntd.ru/document/1200105711 (Дата обращения: 27.12.2023).

References:

1. Algorithm for calculating the security assessment of operating systems of the AIS OVD, developed on the basis of the analysis of the security requirements of GOST R ISO / IEC 15408 and possible threats / A.I. Yangirov, E.A. Rogozin, O.I. Bokova, S.B. Akhlyustin. Herald of the Daghestan State Technical University. Technical Sciences. 2023;50(3):167-171. - DOI 10.21822/2073-6185-2023-50-3-167-171. - EDN QIOPOE. (In Russ)
2. On the issue of assessing the security of operating systems used in automated information systems of internal affairs bodies. A.I. Yangirov. *Security, safety, communication*. 2023; 8-3:83-90. – EDN SLCGLG. (In Russ)
3. Calculation of the security assessment of open operating systems based on the analysis of security requirements according to GOST r ISO/IEC 15408 / A.I. Yangirov, E.A. Rogozin // Issues of ensuring security in cyberspace: Proceedings of the All-Russian scientific and technical conference, Makhachkala, 12/16/2022. – Makhachkala: Dagestan State Technical University, 2022;243-248. – EDN EDHHEY. (In Russ)
4. Development of an automated system for calculating the security assessment of operating systems of information systems based on the analysis of security requirements. A.I. Yangirov, E.A. Rogozin, E.Yu. Nikulina, A.V. Kalach . *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2022; 4:182-188. – EDN BNBXNZ. (In Russ)
5. Information message of October 18, 2016 No. 240/24/4893 "On approval of the Information Security Requirements for Operating Systems" of the FSTEC of Russia - [Electronic resource] - Access mode. - URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii- ot-18-oktyabrya-2016-g-n-240-24-4893 (Accessed: 01.02.2024). (In Russ)
6. Information Security Threat Database - [Electronic resource] - Access mode. - URL: https://bdu.fstec.ru/ (Accessed: 01.02.2024). (In Russ)
7. GOST R ISO/IEC 15408-2-2013. Information technology. Security methods and tools. Information technology security evaluation criteria. Part 2. Security functional components [Electronic resource] – Access mode. – URL: https://docs.cntd.ru/document/1200105710 (Accessed: 27.12.2023). (In Russ)
8. GOST R ISO/IEC 15408-3-2013. Information technology. Security methods and tools. Information technology security evaluation criteria. Part 3. Security assurance requirements [Electronic resource] – Access mode. – URL: https://docs.cntd.ru/document/1200105711 (Accessed: 27.12.2023). (In Russ)

Сведения об авторах:

Янгиров Адиль Илдарович, начальник отделения лабораторных исследований и испытаний; adil-yan@yandex.ru

Янгиров Илдар Мухаматович, научный сотрудник отдела развития средств обнаружений; YIMufa@yandex.ru

Рогозин Евгений Алексеевич, доктор технических наук, профессор; профессор кафедры автоматизированных информационных систем ОВД; evgenirogozin@yandex.ru

Ахлюстин Сергей Борисович, кандидат технических наук, начальник кафедры тактико-специальной подготовки; cerg7676@yandex.ru

Information about authors:

Adil I. Yangirov, Head of the Laboratory Research and Testing Department; adil-yan@yandex.ru

Ildar M. Yangirov, Researcher at the Department of Development of Detection Tools; YIMufa@yandex.ru

Evgeny A. Rogozin, Dr. Sci. (Eng), Prof.; Prof., Department of Automated Information Systems of the Department of Internal Affairs; evgenirogozin@yandex.ru

Sergey B. Akhlyustin, Cand. Sci. (Eng), Head of the Department of Tactical and Special Training; cerg7676@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 15.06.2024.

Одобрена после рецензирования/ Reviced 10.07.2024.

Принята в печать/Accepted for publication 10.07.2024.