Методы анализа рисков информационной безопасности: нечеткая логика

А.С. Любухин

***Аннотация*—В данной статье представлено теоретическое исследование вопроса применимости теории нечетких множеств для анализа и оценки информационных рисков при проведении аудита защищенности объектов критической информационной инфраструктуры. Рассмотрены особенности данной теории на примерах из предметной области информационных рисков с построением диаграммы, иллюстрированием этапов реализации нечеткого вывода. Детализирован каждый из этапов нечеткого вывода с транспонированием на процесс анализа и оценки информационных рисков на примере анализа информации о DDOS-атаках на информационную систему. В ходе исследования доказана применимость теории нечетких множеств для решения задачи по анализу и оценке информационных рисков объектов критической информационной инфраструктуры.**

***Ключевые слова*—информационный риск, анализ рисков, количественные методы, качественные методы, теория нечетких множеств, лингвистическая переменная, фаззификация, дефаззификация, продукционное правило.**

I. Введение

Одной из ключевых областей исследования в сфере информационной безопасности является анализ рисков. Процесс анализа информационных рисков является неотъемлемой частью процесса риск-менеджмента. В условиях внешнеполитического давления на все системы общества нашей страны необходимо уделять достаточное внимание защите информационных систем – как государственных, так и частных. Анализ рисков в мероприятиях по защите информации занимает ключевое место.

Инструментарий и методы, с помощью которых осуществляется не только управление рисками (риск-менеджмент), но и оценка информационных рисков с разных позиций, весьма разнообразны ввиду широты рассматриваемой проблемы и самого объекта (информационных рисков). Наиболее известным методом является метод экспертных оценок, который в современном мире постепенно становится вспомогательным этапом реализации новых методов на этапе сбора входных данных. Кроме того известны и другие методы анализа рисков, в частности использование алгоритма k-means кластеризации и взаимной информации для вычисления величины риска информационной безопасности[1]. Необходимость в поиске и дополнении новых методов обусловлена сверхдинамичностью сферы IT-технологий и ростом масштаба их использования и применения на практике. Методы, с помощью которых осуществляется анализ, в том числе и информационных рисков, направлены на разностороннюю оценку характеристик информационных рисков.

Статья получена 7 ноября 2022.

А.С. Любухин Ростовский государственный экономический университет (РИНХ) Ростов-на-Дону, Россия (e-mail: r.vv2020@mail.ru).

II. Место теории нечетких множеств в риск-менеджменте

A. Количественные и качественные методы

Наиболее часто используемыми такими методами являются методы количественного и качественного анализа, имитационное моделирование и нечеткая логика.

К качественным методам анализа рисков относят методы экспертных оценок и аналогий, которые представляют наглядные результаты без числовой оценки рисков. Преимуществом является то, что результаты анализа рисков этими методами могут использоваться в качестве входных данных в процессе минимизации этих рисков. Однако, часто к недостаткам метода экспертных оценок и аналогий относят достаточно высокую степень субъективности мнения эксперта, а также зависимость от квалификации и уровня знаний каждого из экспертов. Вероятность наступления так называемого «человеческого фактора» в данных методах выше относительно методов количественного анализа.

Количественные методы, напротив, направлены на представление результата в виде конкретной количественной характеристики для возможности численного определения финансовых и иных потерь от реализации каждого из рисков. Для представления конкретного числового результата используются параметры и инструменты теории вероятности и математической статистики: дисперсия, коэффициент вариации, среднее отклонение.

B. Возникновение и характеристика теории нечеткой логики

Что касается непосредственно теории нечеткой логики (теории нечетких множеств), то это принципиально новый подход к анализу различных процессов: экономики, бизнеса, информационной безопасности, информационных проектов. Процессы в данных предметных областях характеризуются относительно высокой степенью неопределенности, которая существенно затрудняет возможность применения точных методов, в частности количественных. Порой такая неопределенность вообще исключает возможность применения любых других

подходов к анализу.

Сама по себе теория нечетких множеств сформировалась в 60-х годах прошлого века в трудах профессора из университета Беркли Л. Заде. На следующих этапах развития данной теории стараниями таких ученых как Б. Коско, Дж. Бакли, Г. Прейда были исследованы вопросы операций над нечеткими числами, проецирования теории нечетких множеств на различные предметные области: экономику, финансы.

В дальнейшем с развитием экономики, расширением бизнес-индустрии, а также с развитием рыночных отношений данная теория стала применяться также и для представления и анализа бизнес-процессов [2].

Нечеткая логика представляет собой достаточно гибкий и эффективный инструмент анализа большого объема информации, которую относительно трудно упорядочить и проанализировать традиционными методами и способами. Именно этим и обусловлено использование этого метода во многих предметных областях.

Не стали исключением и информационно-телекоммуникационные технологии, развитие которых идет огромными темпами и обусловливает необходимость появления новых методов и подходов к анализу информации в информационных системах.

Основной измерительной единицей теории нечетких множеств является лингвистическая переменная, характеризующаяся относительной размытостью по отношению к математическим численным параметрам. Лингвистическая переменная отличается высокой степенью субъективности, но именно этим и объясняется массовость ее применения в информационных системах, т.к. многие параметры там часто трудно описать с помощью математического языка и объективно оценить тоже не представляется возможным.

III. Применение теории нечетких множеств для анализа рисков информационной безопасности

Лингвистические переменные в теории информационных рисков характеризуют такие параметры грамотность персонала, уровень квалификации злоумышленников и т.д. Так, например, уровень квалификации злоумышленников можно представить в виде шкалы от 0 до 10, где 0 – отсутствие квалификации, технического образования и навыков, а 10 – высокая квалификация теоретической и практической подготовки, индивидуальные особенности и талант взломщика. Соответственно, внутри данной шкалы кроме отдельных баллов существуют определенные промежутки – интервалы. Каждый из интервалов (их как минимум 3 – низкий уровень, средний, высокий) характеризует ряд объектов, которые обладают сходными параметрами, которые отличаются друг от друга не столь существенно, чтобы влияние данных отличий могло изменить значения других взаимосвязанных параметров до предельных значений.

В теории управления информационными рисками, описанный выше пример будет представлять такую же шкалу, значения параметров которой, однако, будет зависеть от объекта защиты – объекта предполагаемой гипотетической атаки со стороны абстрактного злоумышленника, либо группы злоумышленников.

Например, применительно к сфере объектов критической информационной инфраструктуры уровень квалификации атакующих будет, безусловно, высоким, поскольку атакующая сторона в таком случае представляет собой иностранные спецслужбы, зарубежные правительства, криминальные группировки и т.п. Исходя из того, что в таких структурах высок уровень политического и финансового давления и контроля, количество ресурсов, которые могут быть задействованы для атаки, априори считается высоким. Следовательно, и затраты на подготовку, повышение квалификации и оплату труда взломщиков тоже могут быть высокими и не ограничиваться.

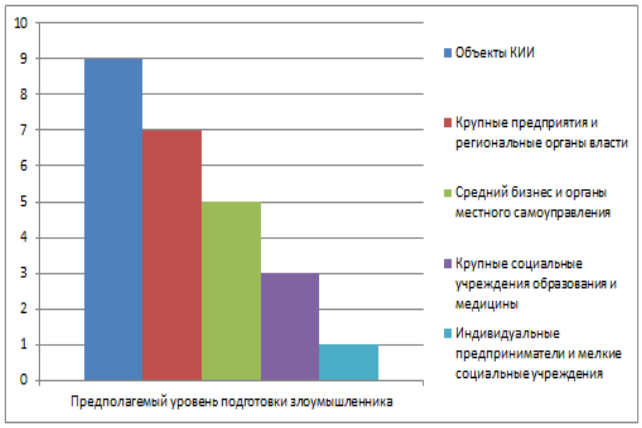

Рисунок 1 – Пример шкалы нечетких переменных «Предполагаемый уровень подготовки злоумышленника»

На приведенной выше диаграмме показан пример шкалы нечетких множеств для параметра рисков, описанного ранее. Т.е. уровень подготовки злоумышленника зависит от объекта атаки, т.к. объекту атаки всегда соответствует атакующий объект, и уровень значимости информации каждой из систем может заинтересовать конкретную группу взломщиков.

Несмотря на все преимущества теории нечетких множеств, одним из недостатков является субъективный подход, который можно прямо проследить на данной диаграмме: уровень подготовки злоумышленника для каждой группы атакуемых объектов может быть и другим, да и группы можно формировать совершенно иным образом, например в соответствии с принципами категорирования объектов защиты согласно нормативным правовым документам (например, в случае со сферой критической информационной инфраструктуры это Приказ ФСТЭК № 239 от 25.12.2017 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации) [3].

Кроме входных данных влияние может оказать и квалификация (подготовка) экспертов, которые осуществляют формирование шкалы нечеткой логики и распределение объектов и значений шкалы по этим объектам. Кроме того, возможно введение дополнительных уровней – не только «низкий», «средний» и «высокий», но и «выше среднего», «ниже среднего».

Анализируя данный пример, можно также, опираясь на способы задания шкалы нечетких множеств определить следующие утверждения: «уровень подготовки злоумышленников, атакующих объекты КИИ (критической информационной инфраструктуры) – высокий; уровень злоумышленников, атакующих крупные предприятия и органы региональной власти – выше среднего и т.д.

Отнесение параметра к определенному интервалу осуществляется посредством экспертных оценок, с помощью которых происходит построение функции принадлежности. С помощью данного математического инструмента лингвистическая переменная переводится на математический язык. Если продолжать анализировать приведенную выше диаграмму, то можно утверждать, что функция принадлежности представляет собой математическую функцию, которая определяет степень уверенности, с которой элементы множества X принадлежат нечеткому множеству Y. Функция будет выглядеть следующим образом:

$$F_Y(X).$$

График, характеризующий зависимость уровня риска от сопутствующих факторов может быть сформирован в зависимости от статистических данных различными математическими функциями. Необходимо определить закон распределения (Пуассона, Вейбулла, нормальное распределение, экспоненциальный закон и т.д.), которому подчиняется данная последовательность статистических данных и в зависимости от закона распределения определить функцию распределения.

Например, для простого определения уровня информационного риска – высокий или низкий, можно применить функцию, график которой изображен на следующем рисунке.

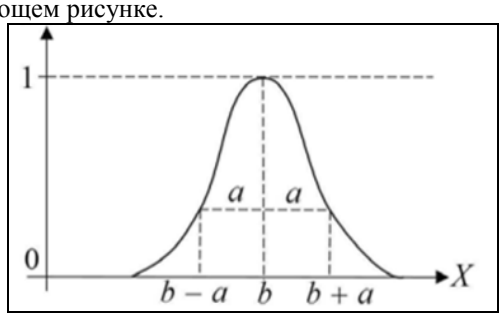

Рисунок 2 – Пример функции принадлежности значения параметра нечеткому множеству на основе статистических данных

На примере представлена Гауссова функция принадлежности, которая характеризует степень принадлежности значений параметров информационных рисков нечеткому множеству $F_Y(X)$. Вершина графика со значением 1 определяет максимальный уровень принадлежности. Наряду с функцией Гаусса выделяют треугольные, кусочно-линейные, сигмоидные и трапециевидные функции принадлежности [4].

Построение же самих функций осуществляется как прямыми, так и косвенными методами. Прямые непосредственно задают правила определения значений функций, однако с большой долей субъективизма.

В косвенных методах условия формируются заранее, а значения функции подбираются экспертами таким образом, чтобы согласовываться с условиями, сформулированными заранее. Приведенный пример на рисунке 2 строится в большинстве случаев с помощью статистических данных, полученных с помощью журнала регистрации событий, различных реестров, а также информации графиков (например, скорость соединения, скорость передачи данных, количество обращений к системе в определенный момент времени).

Кроме того используют и методы парного сравнения, ранговых оценок и т.д., где экспертные мнения выступают в качестве заранее подготовленной и независимой входной информации для последующего анализа и обработки.

IV. Основные этапы реализации теории нечетких множеств на практике при анализе информационных рисков

Реализуется на практике теория нечетких множеств, как правило, в виде систем нечеткого вывода, которые являются основой для многих экспертных и управляющих процессов. Теперь необходимо подвергнуть анализу непосредственно сам процесс нечеткого вывода с детализацией шагов каждого этапа вывода. На следующем рисунке представлены основные этапы нечеткого вывода.

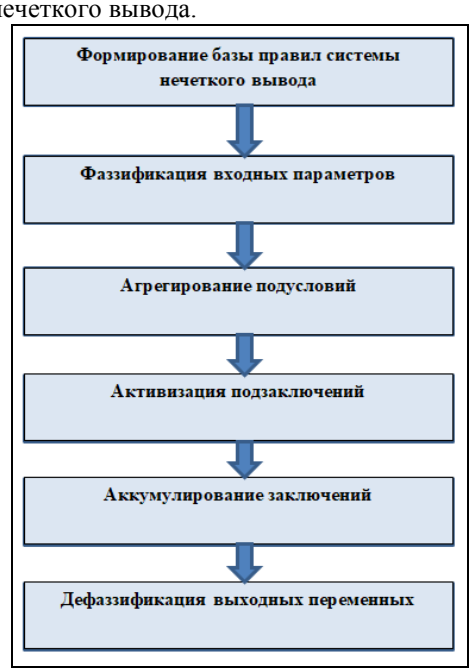

Рисунок 3 – Основные этапы нечеткого вывода

Пусть X и Y – входные переменные, представляющие собой параметры анализируемого объекта, данные о состоянии объекта управления, данные о внешних воздействиях, Z – выходная переменная. Конкретно применительно к менеджменту рисков входными переменными становятся параметры информационной системы, которые могут быть нарушены в ходе реализации мероприятий деструктивного воздействия на данные.

Каждая переменная X, Y, Z может принять различные значения, следовательно, существуют следующие лингвистические множества:

$$X=(X_1, X_2),$$
$$Y=(Y_1, Y_2, Y_3),$$
$$Z=(Z_1, Z_2, Z_3).$$

Количество элементов множества может варьироваться и быть различным для каждой системы [5]. Первый этап – формирование базы правил – представляет собой формулировку зависимости переменных множества Z от элементов множеств X и Y, которые являются следствием и условиями соответственно. Из множеств X и Y формируются входные параметры, а из Z – выходные параметры.

На этом этапе теория нечетких множеств коррелирует с методом экспертных оценок, поскольку база правил систем нечеткого вывода необходима для того, чтобы формальным языком представить знания экспертов, полученные эмпирическим путем. Такую форму представления информации называют нечеткими продукционными правилами. Система таких нечетких продукционных правил отражает знания экспертов о параметрах системы, характеристиках информационных рисков, характере функционирования системы в нормальном и аномальном состояниях, т.е. содержит формализованные человеческие знания.

Нечеткое продукционное правило представляет собой выражение вида:

$$(i):Q;P;A{=}{=}{>}B;S,F,N,$$

где (i) – имя нечеткой продукции, Q – сфера применения нечеткой продукции, P – условие применимости ядра нечеткой продукции, $A{=}{=}{>}B$ – ядро нечеткой продукции, в котором A – условие ядра (или антецедент), B – заключение ядра (консеквент), $=>$ - знак следования в логике, S – метод определения количественного значения степени истинности заключения ядра, F – коэффициент определенности или уверенности нечеткой продукции, N – постусловия.

Центральным компонентом является здесь ядро $A{=}{=}{>}B$. Представляется оно в виде выражения *«ЕСЛИ A, ТО B»*. Применительно к сфере информационных рисков в качестве параметров A и B могут выступить «реализация DDOS-атаки» и «нарушение доступности системы». Таким образом условие будет выглядеть следующим образом:

ЕСЛИ реализуется DDOS-атака,

ТО нарушится доступность системы

Данный пример демонстрирует простейшее продукционное правило. На практике данные правила могут быть составными и довольно сложными, дополненными связками «И», «ИЛИ», «НЕ».

Совокупность таких правил, относящихся к определенной предметной области (в нашем случае это сфера оценки информационных рисков) образует нечеткую продукционную систему.

На этапе фаззификации входных параметров происходит поиск функции принадлежности множеств, исходя из исходных данных. Т.е. осуществляется сопоставление численных значений входной переменной системы со значением функции принадлежности и соответствующей лингвистической переменной. Под численными значениями входной переменной понимается информация, полученная эмпирическим путем – с помощью счетчиков, датчиков и т.д. Данный процесс необходим для представления входных данных в антецендентах ядер нечетких продукционных правил и последующей правильной реализации непосредственно самих правил.

Рассматривая пример с анализом информационных рисков, реализацию процесса фаззификации можно определить следующим образом: датчиком зафиксировано количество DDOS-атак 12 атак/мес. В системе закреплены 4 лингвистических переменных: низкое количество атак, среднее, высокое, критическое. Для каждой лингвистической переменной определен численный промежуток, который помогает отнести входное конкретное численное значение с конкретной переменной системы. Если низкому уровню соответствует количество до 10, средний – от 10 до 60, высокий – от 60 до 100, критический – свыше 100 атак в месяц. При такой базе соответствия входное значение «12» будет соответствовать лингвистической переменной «средний уровень».

На этапе агрегирования определяется степень истинности каждого из подзаключений по каждому правилу, сформированному на первом этапе. Полученные на этапе фаззификации значения функций принадлежности термов лингвистических переменных используются в процедуре по определению степени истинности условий по каждому из правил системы нечеткого вывода. Относительно просто осуществляется определение истинности простого нечеткого высказывания – степень истинности соответствует значению функции принадлежности соответствующей лингвистической переменной. Более сложным процессом является определение истинности составного высказывания, состоящего из нескольких простых высказываний. В этом случае степень истинности определяется степенью истинности каждого из выражений, входящих в состав составного высказывания при помощи нечетких логических операций над этими результатами определения степени истинности.

На этапе активизации подусловий происходит формирование одного нечеткого подмножества для каждой переменной путем объединения нечетких подмножеств для каждой переменной. На данном этапе осуществляется нахождение степени истинности каждого из элементарных логических высказываний, которые составляют консеквенты ядер всех нечетких продукционных правил. Ситуация в данном случае аналогична этапу агрегирования – различается процесс определения степени истинности для консеквента, представляющего собой простое нечеткое высказывание и для составного высказывания. В первом случае определятся с помощью алгебраического произведения весового коэффициента и степени истинности антецедента нечеткого продукционного правила, а во втором – определяется на основе степени истинности каждого из элементарных высказываний, входящих в составное высказывание.

Подзаключения и аккумулирование заключений является обобщающим этапом систем нечеткого вывода. При аккумулировании осуществляется нахождение соответствия между выходными лингвистическими переменными и функций принадлежности. Для этого объединяются все степени истинности подзаключений. Результат представляет собой объединение нечетких множеств всех подзаключений нечеткой базы правил относительно соответствующей лингвистической

переменной. Объединение функций осуществляется по правилам классического объединения, либо алгебраического объединения. Также может применяться граничное объединение, драстическое объединение или λ-сумма.

Далее следует обратный фаззификации процесс дефаззификации – преобразование выходных переменных в количественные значения. Проводится дефаззификация одним из следующих методов[6]:

- метод центра тяжести;
- метод центра площади;
- метод левого модального значения;
- метод правого модального значения.

Анализируя процесс нечеткого вывода и детализируя каждый этап, можно прийти к следующему выводу: каждый из этапов может реализовываться различным образом. Например, этап активизации может проводиться различными методами нечеткой композиции, а объединение на этапе аккумуляции проводится не только максимальным объединением, но и другими способами. Этим и обусловлено разнообразие алгоритмов реализации нечеткого вывода:

- алгоритм Мамдани;
- алгоритм Цукамото;
- алгоритм Ларсена;
- алгоритм Сугено;
- упрощенный алгоритм нечеткого вывода.

Каждый из вышеперечисленных алгоритмов [7] имеет свою специфику и особенности реализации. Применимость алгоритмов к предметной области анализа информационных рисков является вопросом отдельного теоретико-практического исследования, выходящего за рамки анализа вопроса применения теории нечетких множеств при осуществлении анализа информационных рисков.

V. Заключение

Таким образом, в ходе теоретического анализа вопроса использования теории нечетких множеств, были исследованы базовые аспекты теории нечетких множеств. Также были представлены практические примеры, иллюстрирующие реализацию теории в эмпирических исследованиях вопроса анализа и оценки информационных рисков при проведении аудита защищенности объектов критической информационной инфраструктуры, как одного из аспектов предметной области информационной безопасности. Алгоритм систем нечеткого вывода, как способ применения на практике теории нечеткой логики, был рассмотрен с детальным выделением основных этапов. На примере информационных рисков объектов КИИ были прослежены основные особенности, достоинства и недостатки применения и реализации метода нечетких множеств. Данное теоретическое исследование продемонстрировало применимость теории нечетких множеств к анализу и оценке информационных рисков.

Благодарности

Автор выражает благодарность научному руководителю – к.т.н., доценту ф-та Компьютерных технологий и информационной безопасности Ростовского государственного экономического университета (РИНХ) Серпенинову О.В. за методическую поддержку исследования проблемы.

Библиография

[1] Любухин А.С. Алгоритм K-means кластеризации и взаимная информация – оптимальный инструмент для вычисления величины риска информационной безопасности // Сборник статей по итогам «XXI Международной научно-практической конференции «Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики» Изд-во: РГЭУ (РИНХ) 2021 г. с. 61-68

[2] Лотфи Задэ – отец нечеткой логики. Режим доступа: https://infopedia.su/27x7693.html.

[3] Приказ ФСТЭК от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ.

[4] Основные типы функций принадлежности Режим доступа: https://infopedia.su/19x9e74.html

[5] Чесалин А.Н., Гродзенский С.Я., Ван Ты Ф., Нилов М.Ю., Агафонов А.Н. Технология оценки рисков на этапах жизненного цикла продукции с использованием нечеткой логики - Russian Technological Journal 2020;8(6): 167-183 Режим доступа https://www.rtj-mirea.ru/jour/article/view/267.

[6] Методы дефаззификации Режим доступа https://docs.exponenta.ru/fuzzy/defuzzification-methods.html

[7] Хижняков Ю.Н. Алгоритмы нечеткого, нейронного и нейро-нечеткого управления в системах реального времени: учебное пособие г. Пермь Изд-во: ПНИПУ 2013 г. с. 127-145

А. С. Любухин. Аспирант Ростовского государственного экономического университета (РИНХ). Имеет квалификацию Бакалавр по специальности «Информационная безопасность», Магистр по специальности «Программная инженерия». Основной областью исследования автора являются методики анализа информационных рисков при проведении аудита защищенности объектов критической информационной инфраструктуры.

Научные публикации автора:

А.С. Любухин Алгоритм k-means кластеризации и взаимная информация – оптимальный инструмент для вычисления величины риска информационной безопасности // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики (Россия, г. Ростов-на-Дону, Ростовский государственный экономический университет (РИНХ), 2021 г.)

А.С. Любухин Цикл PDCA в риск-менеджменте // Информационные системы, экономика и управление Том 23 (Россия, г. Ростов-на-Дону, Ростовский государственный экономический университет (РИНХ), 2021 г.)

А.С. Любухин Применение теории массового обслуживания и математической статистики для анализа компьютерных атак на объекты критической информационной инфраструктуры // Научно-технический STARTUP 2021 (Россия, г. Петрозаводск, МЦНП «Новая наука», 2022 г.)

Предыдущие исследовательские интересы автора: нормативно-правовое регулирование информационной безопасности, языки программирования, моделирование средствами языка UML, теория графовых грамматик. Текущие исследовательские интересы: категорирование объектов критической информационной инфраструктуры, риск-менеджмент, нормативно-правовое регулирование сферы КИИ, теория массового обслуживания, аудит защищенности.

Information security risk analysis methods: fuzzy logic

A.S. Lyubukhin

***Abstract* – This article presents a theoretical study of the applicability of fuzzy set theory for the analysis and assessment of information risks in the course of auditing the security of critical information infrastructure objects. The features of this theory are considered on examples from the subject area of information risks with the construction of a diagram, illustrating the stages of implementation of fuzzy inference. Each of the stages of fuzzy inference is detailed with a transposition to the process of analyzing and evaluating information risks using the example of analyzing information about DDOS attacks on an information system. In the course of the study, the applicability of the fuzzy set theory for solving the problem of analyzing and assessing information risks of critical information infrastructure objects was proved.**

***Keywords* – information risk, risk analysis, quantitative methods, qualitative methods, fuzzy set theory, linguistic variable, fuzzification, defuzzification, production rule.**

References

[1] Lyubukhin A.S. *Algorithm K-means clustering and mutual information – the best tool for calculating the magnitude of information security risk* // Collection of articles on the results of the XXI International Scientific and Practical Conference "Problems of design, application and security of information systems in a digital economy" Publishing house: RSUE (RINH) 2021 p.61-68

[2] *Lotfi Zadeh is the father of fuzzy logic*. Access mode: https://infopedia.su/27x7693.html.

[3] FSTEC Order No. 239 dated December 25, 2017 "*On Approval of the Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation"*

[4] *Main types of membership functions* Access mode: https://infopedia.su/19x9e74.html

[5] Chesalin A.N., Grodzensky S.Ya., Van Ty F., Nilov M.Yu., Agafonov A.N. *Technology for risk assessment at product life cycle stages using fuzzy logic* – Russian Technological Journal 2020;8(6): 167-183 Access mode https://www.rtj-mirea.ru/jour/article/view/267

[6] *Defuzzification methods* Access mode https://docs.exponenta.ru/fuzzy/defuzzification-methods.html

[7] Khizhnyakov Yu.N. *Algorithms for fuzzy, neural and neuro-fuzzy control in real-time systems*: textbook Perm Publishing house: PNIPU 2013 p. 127-145

A.S. Lyubukhin. Postgraduate student of the Rostov State University of Economics (RINH). He has a Bachelor's degree in Information Security, a Master's degree in Software Engineering. The main area of the author's research is the methods of analyzing information risks when conducting an audit of the security of critical information infrastructure objects.

Scientific publications of the author:

A.S. Lyubukhin *Algorithm k-means clustering and mutual information – the optimal tool for calculating the magnitude of information security risk* // Problems of design, application and security of information systems in a digital economy (Russia, Rostov-on-Don, Rostov State University of Economics (RINH), 2021)

A.S. Lyubukhin *PDCA Cycle in Risk Management* // Information Systems. Economics and Management Volume 23 (Russia, Rostov-on-Don, Rostov State University of Economics (RINH), 2021)

A.S. Lyubukhin *Application of queuing theory and mathematical statistics for the analysis of computer attacks on critical information infrastructure objects* // Scientific and technical STARTUP 2021 (Russia, Petrozavodsk, ICNP 'New Science", 2022)

Previous research interests of the author: legal regulation of information security, programming languages, modeling by means of the UML language, the theory of graph grammars.

Current research interests: categorization of critical information infrastructure objects, risk management, regulatory and legal regulation of the field of CII, queuing theory, security audit.