**Модели и методы управления информационной безопасностью в условиях неопределенности.**

**Введение.**

Управление информационной безопасностью, как циклический процесс, требующий постоянного проведения анализа состояний информационной системы, зачастую осложнен неполнотой и неточностью данных, получаемых в процессе сбора. При этом, процесс принятия управленческих решений на основе экспертных оценок зачастую малоэффективен ввиду своего субъективного характера. В данной статье рассматривается вопрос создания системы поддержки принятия решений по управлению информационной безопасностью. Одним из возможных методов является компиляция теории нечетких множеств и многослойных нейронных сетей — нейро-нечеткие продукционные сети ANFIS.

**1. Понятие системы управления информационной безопасностью.**

Согласно ГОСТ Р ИСО/МЭК 17779-2005 «Информационная технология. Практические правила управления информационной безопасностью», система управления информационной безопасностью (СУИБ) — комплекс мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения [1].

Организация или предприятие формируют СУИБ исходя из определенных ей требований информационной безопасности с учетом трех факторов:

— **Оценка рисков организации**. Основанная на экспертном мнении или рассчитанная с помощью того или иного математического аппарата, оценка рисков позволяет обнаружить наиболее уязвимые информационные активы организации, а также спрогнозировать последствия реализации угроз в отношении этих информационных активов.

— **Нормативно-правовые и прочие юридические, законодательные, регулирующие или договорные требования**, которым должны следовать организация, а также её клиенты, партнеры и иные лица, так или иначе связанные с защищаемой информацией.

— **Особенности и принципы**, сформулированные в отношении действий относительно обрабатываемой информации.

После определения требований ИБ, как правило, следует этап выработки и внедрения мероприятий по управлению информационной безопасностью, которые обеспечат снижение рисков до приемлемого уровня.

Этап разработки мероприятий по УИБ в основном представляет собой творческий процесс, требующий детального планирования, всестороннего анализа специфических потребностей организации, а также оценки мероприятий по УИБ с точки зрения их экономической выгоды (например, оценка, основанная на критерии "стоимости-риска"). От выбранных на этом этапе мер зависит действенность и качество дальнейшего функционирования информационной системы.

При этом, эффективность УИБ зачастую зависит от правильности, обоснованности и своевременности решений, принятых в зависимости от результата работы мероприятий по УИБ, введенных в организации. Правильность, обоснованность и своевременность этих решений зависят от знаний, умений и навыков должностных лиц, отвечающих за УИБ [2].

Принятие решений, согласно [3], есть выбор одной альтернативы из полученного или заданного множества альтернатив. Реализация любой альтернативы предполагает наступление тех или иных последствий, анализ и оценка которых по векторному критерию эффективности полностью характеризуют альтернативу. Векторный критерий эффективности предполагает использование некоторой функции полезности, являющейся математическим выражением в виде комбинации частных показателей, выражающих количественную модель достижения цели некоторой функцией эффективности [4].

Принятие тех или иных решений часто осложнено недостаточностью достоверных знаний об истинном состоянии системы в конкретный момент времени. В данной ситуации говорят, что СУИБ работает в условиях неопределенности.

**2. Понятие неопределенности**.

Под неопределенностью, как правило, понимают недостаточно полную осведомленность лиц или систем, принимающих управленческие решения. Неполнота и неточность сведений часто являются следствием невозможности полного сбора и учета информации об информационной системе, а также недостаточными знаниями экспертов в анализируемой прикладной области, что позволяет говорить о влиянии человеческого фактора в задачах принятия решений в условиях неопределенности.

Говоря о неопределенности в информационных системах, можно рассматривать следующие типы неопределенности:

1. Неопределенность среды (1-го рода);

2. Неопределенность принятия решений (2-го рода);

3. Неопределенность последствий принятия решений. Неопределенности данного типа напрямую зависят от неопределенности среды, неопределенности используемых моделей или их параметров.

4. Вариационная неопределенность, к которой относятся факторы, находящиеся вне сферы влияния лиц, принимающих решения. К ним можно отнести решения правительства и независящие от лица, принимающего решения, форс-мажорные обстоятельства.

**Неопределенность среды (1-го рода).**

Различают следующие типы сред, зависящие от степени имеющихся знаний о ней (таб. 1) [5]:

*Таблица 1. Описание типов сред.*

|  |  |
| --- | --- |
| **Тип среды** | **Описание** |
| Детерминированная | Среда, действие которой на систему полностью определено. |
| Стохастическая | Среда, действие которой на систему подчинено известным, либо неизвестным, вероятностным законам. Принятие решений в условиях стохастической среды основано на описании неопределенности с помощью функций распределения (аппарата теории вероятности).  Это зачастую позволяет ликвидировать неопределенность путем замены случайных функций на некоторые усредненные значения (математические ожидания) или вероятностями превышения заданного порога случайной функцией. |
| Целенаправленная | Среда, действие которой подчинено определенным целям. Принятие решений в условиях целенаправленной среды затруднено столкновением интересов нескольких сторон, преследующих различные цели (зачастую, известные).  Для формального описания целенаправленной среды задают: состав сторон; множества контролируемых ими параметров; формулировки правил, по которым производится выбор параметров и оценивается эффективность сторон; рекомендации по рациональному поведению в условиях целенаправленной среды.  В случае целенаправленной среды часто приходится иметь дело с понятием конфликта или конфликтной ситуации, которые возникают в результате воздействия на объект или процесс группы лиц, чьи интересы могут не совпадать. Для решения конфликтных ситуаций применяются методы из области теории игр. |
| Неизвестная | Среда, информация о которой отсутствует в той или иной степени. Неизвестная среда, как правило, характеризуется её индифферентным поведением, т.е. у среды как таковой нет цели негативного воздействия на систему, при этом нет достаточных оснований предполагать, какие значения будут принимать параметры, характеризующие состояние среды на том или ином временном интервале.  Иногда информацию о параметрах, характеризующих состояние среды, можно получить с помощью наблюдений изменения среды во времени и прогнозировании этих изменений.  Процесс принятия решений в случае неизвестной среды может быть организован с помощью: введения гипотез о направленности воздействия среды на систему, а также, на основании воздействия с лицом, принимающим решение, введения аксиом поведения (в частности, аксиомы пессимизма/оптимизма, минимума риска и пр.); экспертных оценок поведения среды и их формализации в той или иной форме в моделях принятия решений. |

**Неопределенность принятия решений (2-го рода).**

Говоря о неопределенности принятия решений, необходимо затронуть понятие риска и его отличия от неопределенности. Отдельные исследователи высказывают мнение об одинаковости данных категорий, поэтому часто не приводятся различия между этими понятиями. Однако, хоть данные термины и взаимосвязаны, ситуации, происходящие в условиях риска и ситуации, происходящие в условиях неопределенности, не равнозначны. Их отличия приведены в таблице 2 [6]:

*Таблица 2. Типы ситуаций при принятии решения.*

|  |  |
| --- | --- |
| **Тип ситуации** | **Описание** |
| Ситуация определенности | Выбор конкретного плана действий из множества возможных исходов всегда приводит к конкретному и точно определенному исходу. |
| Ситуация в условиях риска | Выбор конкретного плана действий может привести к любому исходу из их фиксированного множества, при этом вероятности этих исходов заранее известны или их можно вычислить, каждый план характеризуется конечной вероятностной схемой или дискретным распределением вероятностей осуществления возможных исходов. |
| Ситуация в условиях неопределенности | Выбор конкретного плана действий может привести к любому исходу из их фиксированного множества, однако вероятности этих исходом неизвестны. Здесь выделяют два случая, когда вероятности не определены в силу отсутствия необходимой статистической информации, и в случаях, когда об объективных вероятностях нет смысла говорить вообще. |

Как видно, принятие решений в условиях неопределенности осложнено и требует применения специфических методов. Одним из таких методов является применение системы поддержки принятия решений на основе нейро-нечетких сетей.

**3. Теория нечетких множеств. Нечеткая система вывода.**

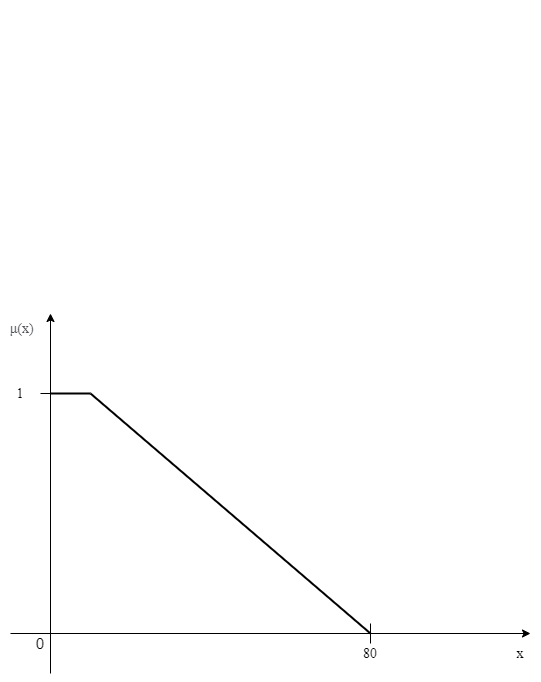
Применение теории нечетких множеств позволяет формализовать неточные и многозначные понятия, вроде <*большая скорость*>, <*низкая температура*>, <*высокий человек*> и пр., называемые лингвистическими переменными. В отличие от четкой логики, в которой принадлежность элемента *x* к некоторому множеству *A* четко определена и равна либо 0, либо 1, нечеткая логика позволяет определить степень принадлежности элемента *x*, определенному на области рассуждения *X*, к нечеткому множеству *A* с помощью функции принадлежности .

Нечеткое множество записывается в общем виде:

Так, для определения лингвистической переменной <*холодный кофе*> на области рассуждения X = {0, 100}, нечеткое множество может иметь следующий вид:

Приведенная запись имеет символьный характер, поэтому запись не является нарушением математических правил, а отражает принадлежности = 1 к температуре для лингвистической переменной <*холодный кофе*>.

*Рис. 1. График функции принадлежности лингвистической переменной <холодный кофе>.*



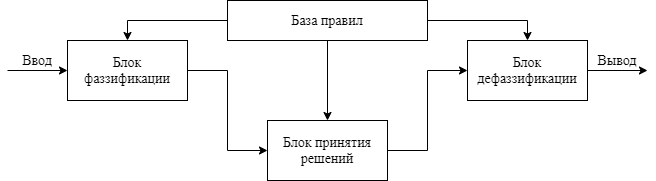
Теория нечетких множеств устанавливает систему нечеткого вывода, в основе которой лежат нечеткие правила вида if-then, являющиеся выражениями IF *A* THEN *B*, где *A* и *B* — нечеткие множества, характеризующиеся соответствующими функциями принадлежности и . Нечеткие правила вида if-then часто используются для фиксации неточных способов рассуждения, которые играют существенную роль в способности человека принимать решения в условиях неопределенности или неточности.

Примером такого правила может быть выражение «Если скорость автомобиля большая, то уровень шума в автомобиле высокий». "Скорость автомобиля" и "уровень шума" — это лингвистические переменные, а "большая" и "высокий" — лингвистические значения, которые характеризуются функциями принадлежности.

Существует также форма нечеткого правила вида if-then, сформулированная Такаги и Сугено [7], содержащая нечеткие множества только в части предпосылки (т.е. после IF), тогда как в THEN содержатся функциональные зависимости. Например, таким правилом будет нечеткое правило вида «Если скорость высока, то ».

Нечеткая система вывода, или нечеткий контроллер, представляет собой следующий модуль, состоящий из четырех функциональных блоков:

*Рис. 2. Нечеткая система вывода.*



— **База правил**, иногда называемая лингвистической моделью и содержащая то или иное количество нечетких правил вида if-then. При проектировании моделей нечеткого вывода следует оценивать достаточность количества нечетких правил, их непротиворечивость и наличие корреляции между ними [8].

— **Блок фаззификации** (fuzzification interface), который преобразует четкие входные данные в степени принадлежности к лингвистическим переменным.

— **Блок принятия решений**, который выполняет операции вывода по сформулированным правилам.

— **Блок дефаззификации** (defuzzification interface), который преобразует нечеткие результаты вывода в четкие выходные данные.

Рассмотрим более детально процесс построения модуля нечеткого вывода по Такаги-Сугено [9]:

Пусть заданные правила записаны в следующем виде:

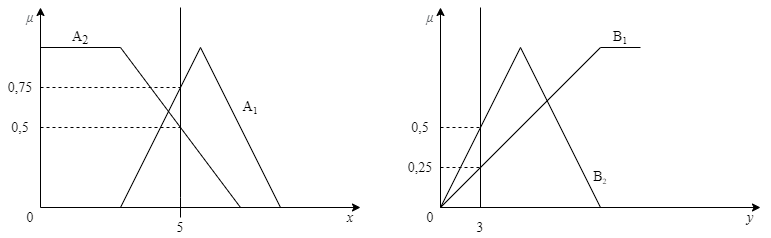
,

.

Предполагаем, что величины являются четкими входными величинами. —нечеткие терм-множества, заданные для этих переменных. Также предполагаем, что в момент времени t были получены значения .

Определим выходные сигналы z с учетом следующих графиков функций принадлежности:

*Рис. 3. Графики функций принадлежности для переменных и*



0,75

1. Найдем степени принадлежности после операции min, где нечеткая операция T-нормы определяется по формуле:

или

*;*

*;*

Данные формулы носят название «правило Мамдани».

= 0,25,

= 0,5.

2. Рассчитаем «индивидуальные выходы»:

где коэффициенты заданы в сформулированных изначально правилах.

= 5

= 11

3. Методом центроида приводим к четкости переменную выхода:

**4. Нейро-нечеткая сеть.**

Трансформация модуля нечеткого вывода в нейро-нечеткую сеть выполняется с помощью поочередного преобразования блока фаззификации, базы правил и блока дефаззификации во фрагменты нейро-нечеткой сети. Обучение нейро-нечеткой сети предполагает наличие обучающей выборки, представляющей собой вектор из точных значений входных и выходной лингвистических переменных [10].

При определении входных лингвистических переменных, соответствующих факторам риска информационной безопасности предприятия (табл. 3), могут быть использованы следующие терм-множества:

Т1 = {Низкий (Н); Средний (С); Высокий (В)},

Т2 = {Очень низкий (ОчН); Низкий (Н); Средний (С); Высокий (В); Очень высокий (ОчВ)}.

При определении входных лингвистических переменных, соответствующие показателям риска (табл. 4), могут быть использованы терм-множества:

Т3 = {Низкая очевидность риска (НОР); Средняя очевидность риска (CОР); Высокая очевидность риска (ВОР)};

Т4 = {Очень низкая очевидность риска (ОчНОР); Низкая очевидность риска (НОР); Средняя очевидность риска (СОР); Высокая очевидность риска (ВОР); Очень высокая очевидность риска (ОчВОР)}.

*Таблица 3. Факторы риска ИБ.*

|  |  |  |
| --- | --- | --- |
| **Переменная** | **Наименование лингвистической переменной** | **Терм-множество** |
|  | Программно-аппаратный уровень защиты | Т1 = {Н; С; В} |
|  | Уровень организационной защиты | Т1 = {Н; С; В} |
|  | Уровень правовой защиты | Т1 = {Н; С; В} |
|  | Мотивация источника угроз | Т2 = {ОчН; Н; С; В; ОчВ} |
|  | Возможности источника угроз | Т2 = {ОчН; Н; С; В; ОчВ} |

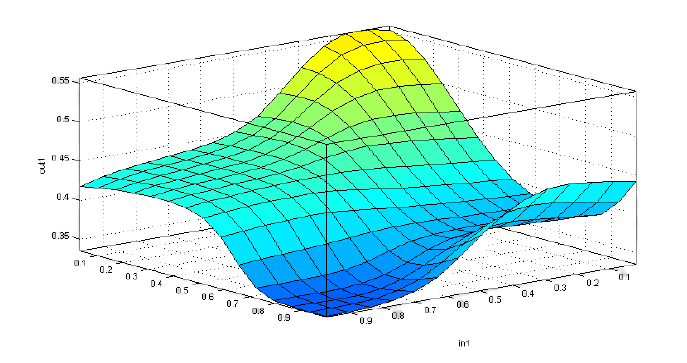
*Таблица 4. Риски ИБ.*

|  |  |  |
| --- | --- | --- |
| **Переменная** | **Наименование лингвистической переменной** | **Терм-множество** |
|  | Риск снижения эффективности защиты | Т3 = {НОР; СОР; ВОР} |
|  | Риск возникновения потенциальных угроз | Т4 = {ОчНОР; НОР; СОР; ВОР; ОчВОР} |
|  | Риск ИБ организации | Т4 = {ОчНОР; НОР; СОР; ВОР; ОчВОР} |

Пакет MATLAB Neuro-Fuzzy Designer позволяет смоделировать нейро-нечеткую сеть на основе нечеткого вывода ANFIS (adaptive neuro-fuzzy inference system). Обучение нейро-нечеткой сети было выполнено на основе обучающей выборки, содержащей 118 наборов, представляющих собой вектор значений факторов риска и значений уровня риска (входные и выходные лингвистические переменные, соответственно). Данные не были получены с помощью независимой экспертной оценки и, ввиду своей субъективности, несут показательный характер. При обучении нейро-нечеткой сети использовался метод обратного распространения ошибки.

На рисунке 4 изображена поверхность обученной нечеткой модели, которая показывает зависимость значения выходной лингвистической переменной от входных и .

*Рис. 4. Зависимость риска ИБ предприятия от и*



**Заключение.**

Предложенная нечеткая нейронная продукционная сеть в качестве модели системы поддержки принятия решения, на мой взгляд, позволяет сформировать более объективный подход к управлению ИБ, чем подход, основанный на экспертной оценке, благодаря высокой масштабируемости и гибкости системы, заключающейся в индивидуальном подборе параметров к любой интересующей ситуации.

**Библиографический список:**

1. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью, дата обращения — (17.02.2021).

2. Паращук И.Б., Башкирцев А.С., Михайличенко Н.В. Анализ уровней и видов неопределенности, влияющей на принятие решений по управлению информационными системами. Информация и космос №1, 2017 г. С. 112-120. Дата обращения — (17.02.2021).

3. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей: Примеры использования. — Рига: Зинатне, 1990. — 184 с. — ISBN 5-7966-0459-7. Дата обращения — (18.02.2021).

4. Лапыгин Ю.Н. Управленческие решения: учебное пособие. — Эксмо; Москва, 2009. —540 с. — ISBN 978-5-699-29521-0. Дата обращения — (18.02.2021).

5. Москвин Б.В. Теория принятия решений: Учебник / Б.В. Москвин. — СПб.: ВКА имени А.Ф. Можайского, 2005. — 383 с. Дата обращения — (18.02.2021).

6. Аралбаева Ф.З., Карабанова О.Г., Круталевич-Леваева М.Г. Риск и неопределенность в принятии управленческого решения. Вестник ОГУ 4’2002, С. 132-139. Дата обращения — (18.02.2021).

7. Jyh-Shing Roger Jang. ANFIS: Adaptive-Network-Based Fuzzy Inference System. *IEEE Trans. on Systems, Man and Cybernetics, vol. 23, no. 3, pp. 665-685, May 1993*. Дата обращения — (21.02.2021).

8. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы.: Пер. с польск. И.Д. Рудинского — М.: Горячая линия — Телеком, 2006. — 452 с. — ISBN 5-93517-103-1. Дата обращения — (20.02.2021).

9. Хижняков Ю.Н. Алгоритмы нечеткого, нейронного и нейро-нечеткого правления в системах реального времени: учеб. пособие. Пермь: Изд-во ПНИПУ, 2013. – 160 с. Дата обращения — (22.02.2021).

10. Глушенко С.А. Нейро-нечеткая система поддержки принятия решений управления рисками проектов в условиях неопределенности. Г. Ростов-на-Дону: Труды ВЭО России: 212 том. С. 481-502. Дата обращения — (24.02.2021).