Федеральное государственное автономное образовательное  
 учреждение высшего образования   
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт компьютерных технологий и информационной безопасности

Кафедра информационно-аналитических систем безопасности

имени профессора Л.С. Берштейна

|  |  |
| --- | --- |
| :  \_\_\_\_\_\_\_\_\_\_\_\_ \*\*\*\*\*\*\*\*\*\*\*  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. | К защите допустить:  Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_ А.Н. Целых  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ   
РАБОТА БАКАЛАВРА**

**по направлению 10.03.01 Информационная безопасность**

**(Информационно-аналитические системы финансового мониторинга)**

|  |  |
| --- | --- |
| на тему: | Разработка графово-аналитической модели выявления |
|  | взаимозависимых лиц для целей трансфертного ценообразования |

|  |  |
| --- | --- |
| Руководитель: | Князева Маргарита Владимировна |
|  | *(фамилия, имя, отчество)* |
|  | Доцент кафедры ИАСБ, к.т.н |
|  | *(должность, ученая степень и звание)* |
|  | « » июня 2020 г. |
|  | *(подпись) (дата)* |
|  |  |
| Студент: | Белохвостов Виктор Олегович |
|  | *(фамилия, имя, отчество)* |
|  | КТбо4-8 |
|  | *(группа)* |
|  | « » июня 2020 г. |
|  | *( подпись) (дата)* |

Таганрог 2020 г.

«Разработка графово-аналитической модели выявления

взаимозависимых лиц для целей трансфертного ценообразования»

Белохвостов Виктор Олегович

Группа КТбо4-8

Выпускная квалификационная работа

ЮФУ, Таганрог 2020

**АННОТАЦИЯ**

Данная выпускная квалификационная работа посвящена разработке графово-аналитической модели выявления взаимозависимых лиц для целей трансфертного ценообразования.

Актуальность темы работы состоит в том, выявление взаимозависимости между совершающими сделки контрагентами является одной из основных процедур, проводимых налоговыми органами. Знание и понимание признаков взаимозависимости является основой противодействия ряду финансовых преступлений, связанных с манипуляциями сумм налогового обложения.

В данном работе была разработана графово-аналитическая модель выявления взаимозависимых лиц для трансфертного ценообразования. По итогам разработки модель была реализована в виде веб-приложения с пользовательским интерфейсом с помощью программной платформы NodeJS и фреймворка Express на серверной стороне и фреймворка ReactJS и библиотеки Redux на клиентской стороне.

В заключении было проведено тестирование разработанной модели.

« The development of a graph-analytical model for identifying  
interdependent entities for transfer pricing purposes»

Belokhvostov Viktor Olegovich

Group KTbo4-8

Graduation qualification thesis

SFedU, Taganrog 2020

**ABSTRACT**

This thesis paper is devoted to the development of graph-analytical model for identifying interdependent entities for transfer pricing purposes.

The relevance of the topic is that the identification of interdependence between counterparties performing transactions is one of the main procedures carried out by tax authorities. Knowledge and understanding of the signs of interdependence is the basis for countering a number of financial crimes related to the manipulation of taxable amounts.

In this paper, we developed a graph-analytical model for identifying interdependent entities for transfer pricing. As a result of development, the model was implemented as a web application with a user interface using the NodeJS software platform and the Express framework on the server side, and the ReactJS framework and the Redux library on the client side.

In conclusion, the developed model was tested.

Оглавление

[ГЛАВА 1 АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 8](#_Toc42996104)

[1.1 Понятие информационной безопасности 8](#_Toc42996105)

[1.2 Угрозы информационной безопасности 9](#_Toc42996106)

[1.3 Классификация угроз информационной безопасности 14](#_Toc42996107)

[1.4 Методы классификации, основанные на методах атаки 15](#_Toc42996108)

[1.4.1 Трех ортогональная размерная модель 15](#_Toc42996109)

[1.4.2. Гибридная модель для классификации угроз 15](#_Toc42996110)

[1.5. Методы классификации, основанные на воздействии угрозы 16](#_Toc42996111)

[1.5.1. STRIDE модель 16](#_Toc42996112)

[1.5.2. Модель ISO 16](#_Toc42996113)

[Выводы 1 главы 17](#_Toc42996114)

[ГЛАВА 2 АНАЛИЗ СПОСОБОВ КЛАСТЕРИЗАЦИИ ОБЪЕКТОВ 18](#_Toc42996115)

[2.1 Кластеризация 18](#_Toc42996116)

[2.2 Классификация методов кластеризации 19](#_Toc42996117)

[2.2 Использование кластерного анализа 21](#_Toc42996118)

[2.3 Искусственные нейронные сети 22](#_Toc42996119)

[2.4 Сети Кохонена 26](#_Toc42996120)

[2.5 Структура сети Кохонена 27](#_Toc42996121)

[2.6 Карты Кохонена 28](#_Toc42996122)

[2.7 Алгоритм самоорганизации карты Кохонена 29](#_Toc42996123)

[2.8 Свойства самоорганизующихся карт Кохонена 32](#_Toc42996124)

[Выводы 2 главы 33](#_Toc42996125)

[ГЛАВА 3 ФОРМИРОВАНИЕ КЛАССИФИКАЦИИ УГРОЗ С ПОМОЩЬЮ САМООРГАНИЗУЮЩЕЙСЯ КАРТЫ КОХОНЕНА 34](#_Toc42996126)

[3.1 Разработка базы внутренних инцидентов информационной безопасности 34](#_Toc42996127)

[3.2 Сбор информации и формирование базы внутренних инцидентов информационной безопасности 35](#_Toc42996128)

[3.3 Подготовка данных для моделирования 37](#_Toc42996129)

[3.4 Моделирование сети кластеризации данных в MATLAB NEURAL NETWORK TOOLBOX 39](#_Toc42996130)

[3.5 Формирование классификации внутренних угроз информационной безопасности 48](#_Toc42996131)

[Выводы к главе 3 51](#_Toc42996132)

[ЗАКЛЮЧЕНИЕ 52](#_Toc42996133)

[СПИСОК ИСТОЧНИКОВ 53](#_Toc42996134)

[ПРИЛОЖЕНИЕ 55](#_Toc42996135)

Введение

В условиях современного мира объем информации, обрабатываемой человеком при выполнении своих должностных обязанностей, неуклонно растет, а вследствие этого возникает все больше внутренних угроз информационной безопасности, ведь чаще всего возникновение такого вида угроз происходит из-за человеческого фактора. По этой причине многие предприятия составляют классификацию внутренних угроз информационной безопасности при помощи различных средств интеллектуального анализа данных (ИАД).

На сегодняшний день Data Mining является перспективным направлением, ведь при помощи использования различных инструментов можно с легкостью применять разнообразные методы ИАД, в том числе и для автоматического анализа данных. Одним из таких методов интеллектуального анализа является кластеризация данных.

Цель кластеризации данных состоит в том, чтобы в наборе «сырых» данных выделить кластеры – группы объектов, плотно связанных между собой. При этом связи внутри кластера должны быть плотнее, чем связи, которые соединяют различные группы объектов. Методы кластерного анализа получили широкое распространение в связи с тем, что при их помощи возможно решить различные проблемы, от анализа изображений до выявления признаков мошенничества и анализа рисков.

Для решения проблемы кластеризации и визуализации данных применяются и другие методы интеллектуального анализа, например, нейронные сети. Одним из типов искусственных нейронных сетей, применяемым для решения задач, указанных ранее, являются самоорганизующиеся карты Кохонена.

Поиск структур в обширных многомерных наборах данных, будь то данные измерений, статистика или текстовые документы, является сложным и отнимающим много времени занятием. Интересные, новые отношения между элементами зачастую сложно обнаружить, ведь они могут быть скрыты среди большого количества многомерных данных. При исследовании набора данных с целью поиска новых закономерностей могут помочь методы, которые обнаруживают и эффективно иллюстрируют структуры в данных. Алгоритм самоорганизующейся карты Кохонена может быть использован для помощи в исследованиях, ведь структуры в наборах данных могут быть проиллюстрированы на специальных картах.

Самоорганизующаяся карта Кохонена, или сокращенно SOM, объединяет кластеризацию данных с сохранением топологии. Кластеры, найденные в данных, представлены, как правило, в двумерной сетке. SOM позволяет визуализировать высокоразмерные данные в двух измерениях.

**Целью работы** является составление классификации внутренних угроз информационной безопасности, путем их кластеризации с помощью самоорганизующихся карт Кохонена. Для достижения заявленной цели в работе решаются следующие **задачи**:

1. Анализ литературы о внутренних инцидентах информационной безопасности с целью использования полученных знаний при дальнейшей работе.
2. Составление базы внутренних инцидентов информационной безопасности.
3. Формирование классификации внутренних угроз с помощью самоорганизующейся карты Кохонена.

**Объектом исследования** является процесс построения самоорганизующейся карты Кохонена, а также процесс классификации внутренних угроз информационной безопасности.

**Предметом исследования** являются внутренние угрозы информационной безопасности на предприятии.

**Методы исследования.** Методы интеллектуального анализа данных.

# ГЛАВА 1 ТРАНСФЕРТНОЕ ЦЕНООБРАЗОВАНИЕ И ПРИЗНАКИ ВЗАИМОЗАВИСИМОСТИ ЛИЦ

# 1.1 Понятие цены и ценообразования

В результате непрекращающегося процесса информатизации общества информация стала играть одну из важнейших ролей в любой сфере жизни человека, ведь она является главной составляющей информационной сферы, а также обладает большой ценностью. Любые составляющие информационной сферы, будь то информационные системы и технологии, или же непосредственно сама информация оказывают большое влияние на все сферы комплексной безопасности Российской Федерации, а именно: на экономическую, экологическую, транспортную, информационную безопасность и многие другие. Исходя из указанного влияния компонентов на различные сферы безопасности, можно с уверенностью сказать, что влияние информационной безопасности на жизнь современного человека в будущем будет только возрастать, поэтому необходимо развивать культуру информационной безопасности, а также внедрять новые методики для анализа и предотвращения рисков.

Информационная безопасность (ИБ) – это защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре [12].

Информационная безопасность (ИБ) – это состояние защищенности интересов организации в условиях угроз в информационной сфере, которое достигается путем обеспечения совокупности свойств информационной безопасности, а именно конфиденциальности, целостности и доступности информационных активов [9].

Если рассматривать понятие информационной безопасности для предприятий, то можно сказать, что ИБ — это состояние информации, при котором отсутствует риск уничтожения, изменения, модификации или раскрытия информации, который связан с причинением вреда пользователю информации или же владельцу данного ресурса.

Для обеспечения высокого уровня информационной безопасности необходимо, чтобы соблюдалась каждая целевая характеристика информации, а именно ее конфиденциальность, целостность, доступность, подлинность, а также ее недоказуемость. При этом помимо информации в качестве объектов, подлежащих непосредственной защите, должны рассматриваться любые носители данных, средства хранения и процессы ее обработки и передачи.

# 1.2 Угрозы информационной безопасности

Угрозой называется некое событие, процесс или явление, которое может нанести косвенный или прямой ущерб информационной безопасности при помощи воздействия на саму информацию, процессы обработки информации или на ее носители.

В соответствии с ГОСТ Р 51275-2006 [1] все факторы, оказывающие воздействия на безопасность защищаемой системы, по отношению к природе их возникновения делят на объективные и субъективные. Объективные или естественные угрозы возникают за счет влияния на защищаемую систему природных процессов или физический явлений, а субъективные возникают из-за деятельности человека. Субъективные угрозы могут быть разделены на преднамеренные и непреднамеренные. Наглядно данная классификация представлена на рисунке 1.1.

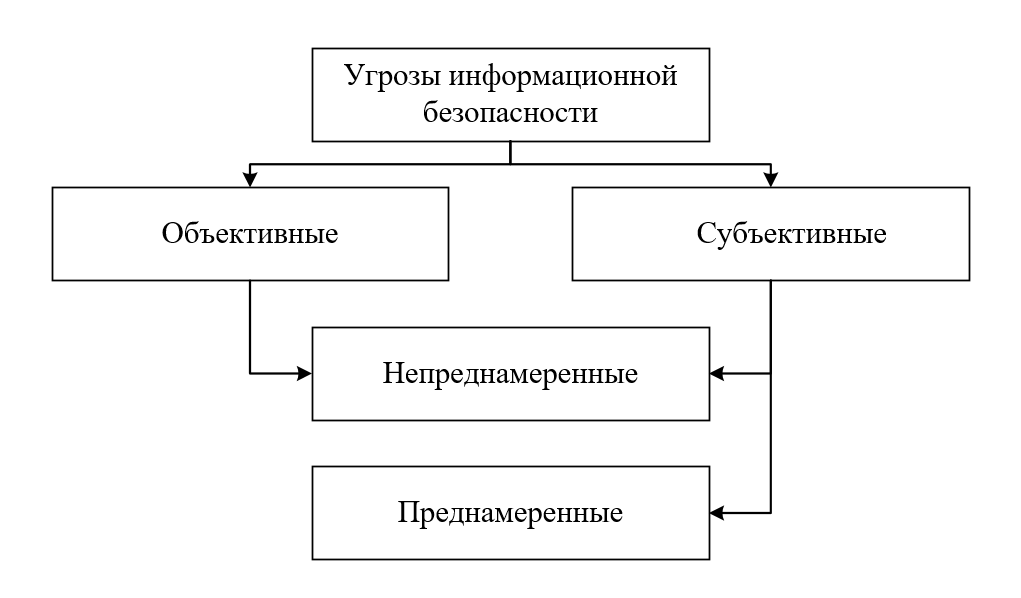


Рисунок 1.1 – Классификация угроз информационной безопасности

Помимо этого, происходит деление факторов по отношению к объекту информатизации на внутренние и внешние. Такое разделение источников угроз вполне оправдано, так как оно имеет практический смысл и позволяет лучше определить механизмы защиты. Внутренние и внешние угрозы информационной безопасности также делятся на преднамеренные и непреднамеренные, а преднамеренные, в свою очередь, делятся на пассивные и активные угрозы. Пассивные угрозы, в отличие от активных, не наносят большого ущерба, так как чаще всего они представляют собой несанкционированный доступ к информации, но без каких-либо модификаций, будь то уничтожение или искажение.

Основное отличие между внутренними и внешними угрозами информационной безопасности заключается в том, что при реализации внутренней угрозы нарушители, являющиеся сотрудниками, имеют значительное преимущество перед внешними злоумышленниками. Они не только осведомлены о политике, процедурах и технологиях своей организации, но и знают о тех уязвимостях, которые не устранены в организации, например, слабые политики безопасности или наличие уязвимостей в сети. Злоумышленник может даже быть тем, кто настроил меры безопасности организации.

Нет сомнения в том, что внутренние угрозы информационной безопасности представляют большую опасность для компании, чем внешние, ведь именно персонал знает обо всех существующих лазейках, которые можно использовать для совершения неправомерных действий с информацией или системой в целом.

Данное утверждение подтверждают многие исследования, проводимые различными компаниями, работающими в сфере ИБ. Одним из таких исследований является аналитическое исследование «Защита конечных точек: проблемы и решения», проведенное компанией «Код безопасности» в 2019 году. В результате данного исследования был сделан вывод, что одной из самых больших угроз для информационной безопасности является персонал, ведь в актуальных векторах атак наиболее распространенным стал вектор, связанный с непреднамеренными ошибками персонала.

В соответствии с данными исследования уровня информационной безопасности в компаниях России и СНГ за 2019 год, проведенного компанией «SearchInform», только 9% российских и 17% компаний из СНГ не зафиксировали никаких внутренних инцидентов информационной безопасности за этот год. Такие показатели являются достаточно низкими, ведь в настоящее время большинство компаний уделяют вопросу информационной безопасности большое внимание. Если обратиться к исследованию, то можно увидеть, что организации применяют множество методов защиты, при этом контролируя корпоративную и общедоступную почту, внешние носители, телефонию, мессенджеры, облачные хранилища и многое другое. Данная статистика представлена в таблице 1.

По результатам исследования компании «SearchInform» было выявлено, что 75% специалистов информационной безопасности считают, что их компания недостаточно защищена. Как заявил руководитель отдела аналитики компании «SearchInform» Алексей Парфентьев в данном исследовании: «Опрошенные единодушны: сотрудники могут нанести бизнесу больше вреда, чем киберпреступники и мошенники со стороны. Довольно однозначна и картина по типичному нарушителю. Это те, кто имеет доступ к ресурсам компании. Менеджеры снабжения, финансисты, секретари и помощники, которые близки к информации из «первых рук», к сожалению, оказываются в зоне риска…».

Таблица 1

Статистика методов защиты, применяемых в организациях России и СНГ

|  |  |  |
| --- | --- | --- |
|  | Россия | СНГ |
| Разграничение доступов | 99 | 84 |
| ИБ-инструктаж | 75 | 63 |
| Изоляция критичных объектов IT-инфраструктуры (DMZ, закрытые подсети и т.д.) | 60 | 52 |
| Сканирование инфраструктуры (инвентаризация, поиск уязвимостей и т.д.) | 59 | 49 |
| Автоматизированный мониторинг IT-инфраструктуры (доступности, целостности и т.д.) | 45 | 36 |
| Уменьшение времени детектирования и реагирования (SOC, SIEM) | 12 | 10 |

Анализируя исследования, проведенные компаниями, специализирующимися на средствах защиты информации, нельзя не упомянуть об исследованиях компании «InfoWatch». В сравнительном исследовании за 2013-2019 года «Утечки данных организаций по вине или неосторожности внутреннего нарушителя» сказано, что в 2019 году впервые за все время наблюдения объем скомпрометированных данных в результате внутренних утечек превысил объем таких записей для внешних утечек и составил 9879,9 миллиона записей. Для сравнения в 2018 году данный показатель был равен 2766,6 миллиона. На рисунке 1.2 продемонстрировано число внутренних утечек информации за каждый год, а на рисунке 1.3 представлено, какой процент от всех утечек информации занимают утечки данного типа.

Рисунок 1.2 – Число внутренних утечек информации за период с 2013 по 2019 год

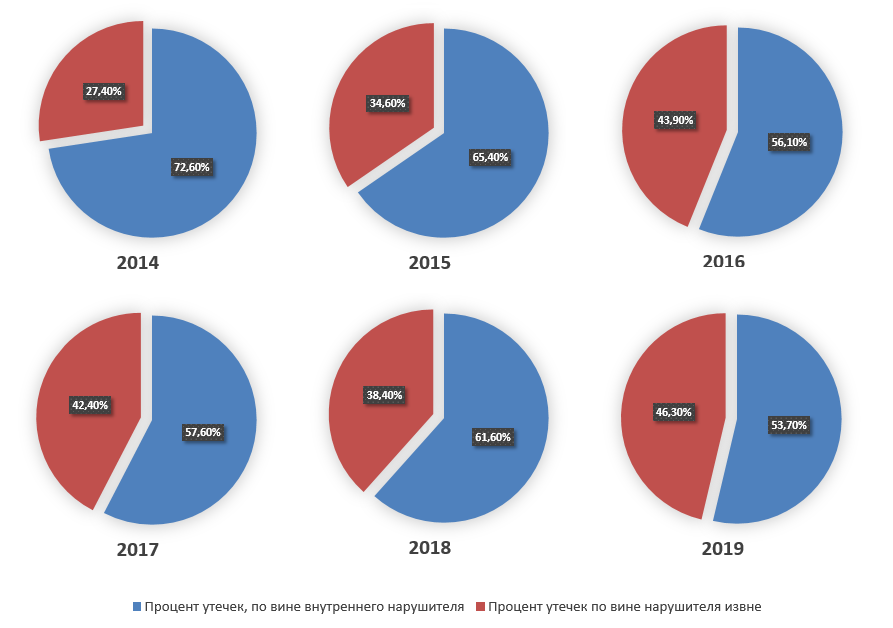


Рисунок 1.3 – Доля внутренних утечек информации от общего числа утечек за каждый год с 2014 по 2019

В другом исследовании 2018 года этой же компании, посвященном анализу инцидентов информационной безопасности, связанных с действиями увольняющихся сотрудников, указано, что в 68% случаев злоумышленник, который является уволенным сотрудником, не только просматривает и копирует информацию, но и передает конфиденциальные данные, будь то коммерческая тайна или персональные данные, заинтересованным лицам, которые чаще всего являются конкурентами. При этом почти в 80% случаев это делается для личной выгоды и только в 14,3 % из-за мести работодателю.

Все рассмотренные исследования подтверждают тот факт, что внутренние угрозы информационной безопасности играют большую роль в уязвимости компании, ведь, согласно исследованиям, количество инсайдерских угроз с каждым годом растет, а это значит, что мер, предпринимаемых для защиты организаций, все еще недостаточно.

# 1.3 Классификация угроз информационной безопасности

Нет сомнения в том, что составление классификации угроз важно, так как с ее помощью становится возможно идентифицировать и понимать характеристики и источники угроз, что помогает грамотно организовать защиту.

Проведенный обзор источников литературы позволил выявить несколько различных классификаций.

Угрозой информационной безопасности являются различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые способны нанести ущерб различным системам организации.

Угрозу можно определить двумя способами: методами, которые злоумышленники используют для эксплуатирования уязвимостей в компонентах системы, или воздействиями угроз на активы. Поэтому подходы к классификации угроз делятся на два основных класса:

1. Методы классификации, основанные на методах атак
2. Методы классификации, основанные на воздействии угроз

# 1.4 Методы классификации, основанные на методах атаки

### 1.4.1 Трех ортогональная размерная модель

Для улучшения понимания угроз и облегчения существующих моделей классификации угроз Lukas Ruf, совместно с соавторами, [13] предложили новую модель угроз для их классификации. Для составления модели угроз ими было использовановведения трехмерной модели, разделяющей пространство угроз на подпространства в соответствии с тремя ортогональными измерениями, обозначенными как мотивация, локализация и агент:

Агент угроз — это субъект, который налагает угрозу на конкретный актив системы. Данное измерение представлено тремя классами: человеческий, технологический и форс-мажорный.

Мотивация угрозы представляет собой причину создания угрозы, и она подразделяется на два класса: преднамеренная и случайная угроза

Локализация угроз представляет собой источник угроз, как внутренних, так и внешних.

### 1.4.2. Гибридная модель для классификации угроз

В [10] **Sandro Gerić**, совместно с соавторами, предложили гибридную модель классификации угроз безопасности информационной системы, названную моделью классификации кубов угроз безопасности информационной системы или моделью C3. Они рассматривали три основных критерия [10]:

1. Частота угроз, которая показывает частоту появления угроз безопасности.
2. Область действия угроз безопасности
3. Источник угрозы безопасности указывает типы источников угрозы.

# 1.5. Методы классификации, основанные на воздействии угрозы

### 1.5.1. STRIDE модель

В [11] описан метод классификации, STRIDE, разработанный Microsoft. STRIDE позволяет охарактеризовать известные угрозы в соответствии с целями и задачами атак или мотивацией атакующего. Аббревиатура STRIDE формируется из первой буквы каждой из следующих категорий:

1. Spoofing ­­­– подделка идентификации
2. Tampering – несанкционированное изменение данных
3. Repudiation – отказ от ответственности;
4. Information disclosure- раскрытие информации
5. Denial of service – отказ в обслуживании
6. Elevation of privilege ­– повышение привилегий

### 1.5.2. Модель ISO

В стандарте ISO 7498-2 перечислено пять основных угроз безопасности и услуг защиты информации в качестве эталонной модели [2]: разрушение информации и/или других ресурсов; искажение или модификация информации; хищение, удаление или потеря информации и/или других ресурсов, раскрытие информации и прерывание обслуживания. При этом угрозы информационной безопасности в данном стандарте классифицированы на случайные и преднамеренные, а преднамеренные, в сою очередь, делятся на активные и пассивные.

## Выводы 1 главы

В данной главе были рассмотрены основные понятия информационной безопасности, приведен ряд исследований внутренних инцидентов информационной безопасности, подтверждающих актуальность исследуемой темы. Были описаны несколько существующих классификаций угроз, выявленных в ходе анализа источников литературы.

## ГЛАВА 2 АНАЛИЗ СПОСОБОВ КЛАСТЕРИЗАЦИИ ОБЪЕКТОВ

# 2.1 Кластеризация

В процессе обработки больших наборов данных необходимо реализовать множество шагов, одним из которых является автоматическая классификация или кластеризация данных. Основная задача кластеризации состоит в нахождении оптимального разбиения набора данных, то есть группировку данных, имеющих сходные характеристики, по классам [3]. Другими словами, цель кластеризации заключается в идентификации групп в сырых данных на основе семантического сходства между ними. Это позволяет в дальнейшем построить когнитивную модель исходного набора данных, помогающую обнаружить внутреннюю структуру тех данных, которые были обработаны. Выполнение разбиения исходных данных на кластеры представлено на рисунке 2.1.

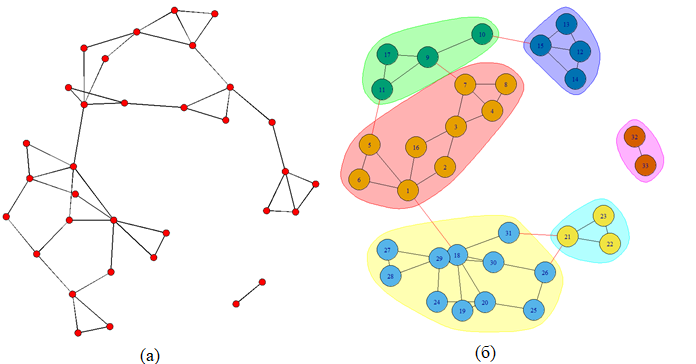


Рисунок 2.1 – (а) Исходный набор данных, (б) набор данных с выделенными кластерами

Суть работы алгоритмов кластеризации можно выразить следующим образом. Имеется обучающая последовательность (набор данных) и функция расстояния между объектами . Требуется разбить последовательность на кластеры, которые представляют собой непересекающиеся подмножества, так, чтобы объекты разных кластеров отличались, но при этом каждый кластер состоял из объектов, близких по метрике ρ. Алгоритм кластеризации — это функция , которая любому объекту ставит в соответствие метку кластера . Множество меток заранее неизвестно [4].

# 2.2 Классификация методов кластеризации

Все методы кластерного анализа можно разделить по способу разбиения данных на кластеры на два больших типа, а именно на иерархическую и неиерархическую. Каждый тип характеризуется своими особенностями и представлен рядом различных алгоритмов поиска групп данных.

Суть иерархической кластеризации состоит в последовательном объединении меньших кластеров в большие или разделении больших кластеров на меньшие. Данные разделяются по определенному правилу, по которому определяется, какие два кластера объединяются или какой большой кластер разделяется. Для каждого алгоритма иерархической кластеризации это правило различно. Иерархия кластеров представлена в виде дерева (или дендрограмы). Корень дерево является уникальным кластером, который собирает все образцы, листья кластеры только с одной выборкой. Конечным результатом алгоритма является дерево кластеров, называемое дендрограмой, которое показывает, как связаны кластеры.

Существует немало алгоритмов иерархической кластеризации, среди них различают два основных типа. Дивизимные или нисходящие алгоритмы разбивают выборку на всё более и более мелкие кластеры. Более распространенными являются агломеративные или восходящие алгоритмы. В таких алгоритмах используется подход «снизу-вверх», при котором каждое наблюдение начинается в собственном кластере, а затем кластеры последовательно объединяются.

Два наиболее популярных алгоритма, используемых в иерархической кластеризации, строят разбиение используя подход «снизу-вверх»:

1. Single-link- на каждом шаге объединяются два кластера имеющие наименьшее расстояние между двумя любыми точками, входящими в них
2. Complete-link- на каждом шаге объединяются два кластера имеющие наименьшее расстояние между двумя точками, наиболее удаленными друг от друга.

При большом количестве экспериментов иерархические методы кластерного анализа непригодны. В таких случаях используют неиерархические методы. Процесс неиерархической кластеризации всегда является итеративным. Итеративные методы кластеризации различаются выбором параметров, таких как начальная точка, правило формирования новых кластеров или правило остановки. В процессе деления новые кластеры формируются до тех пор, пока не будет выполнено правило остановки.

Существует множество неиерархических методов кластеризации, но наиболее распространенным является алгоритм k-means, который часто называют быстрым кластерным анализом. Отличительной особенностью данного алгоритма от остальных иерархических методов является то, что для проведения анализа данных с использованием k-means нужно заранее предположить количество кластеров, на которые необходимо разделить входные данные. Алгоритм неиерархической кластеризации k-means тесно связан с алгоритмов самоорганизующихся карт Кохонена, именно поэтому он будет рассмотрен подробнее.

Данный алгоритм группирует данные, пытаясь разделить выборки в n групп равной дисперсии, минимизируя критерий, известный как инерция или внутрикластерная сумма квадратов расстояний [5]. Благодаря хорошей масштабируемости на большой объем данных алгоритм k-means применяется в различных областях деятельности человека. Существенным недостатком данного алгоритма является то, что для разбиения данных на группы необходимо заранее указать желаемое число групп, которое необходимо определить до начала кластерного анализа.

Работа алгоритма k-means заключается в следующем. Сначала набор данных делится на k непересекающихся кластеров (число кластеров указывается вручную), каждый из которых описывается средним выборок в кластере. В алгоритмах кластеризации данные группируются некоторым понятием «близости» или «подобия». Этот алгоритм предназначен для выбора центроидов, минимизирующих инерцию, или внутрикластерной суммы квадратного критерия (формула 1).

|  |  |
| --- | --- |
|  | (1) |

В k-means в качестве меры близости используется Евклидово расстояние, которое вычисляется по формуле 2.

|  |  |
| --- | --- |
|  | (2) |

Алгоритм k-means состоит из трех шагов. На первом шаге выбираются начальные центроиды. После этого работа алгоритма k-means представляет собой цикл между двумя другими шагами. Сначала каждому образцу присваивается ближайший центр масс, а далее создаются новые центроиды, принимая среднее значение всех выборок, назначенных каждому предыдущему центроиду. Вычисляется разница между старым и новым центром, и алгоритм повторяет последние два шага, пока это значение не будет меньше порога. Другими словами, он повторяется до тех пор, пока происходит изменения внутрикластерного расстояния.

## 2.2 Использование кластерного анализа

Проблема с методами кластеризации заключается в том, что интерпретация кластеров может быть затруднена. Большинство алгоритмов кластеризации выделяют кластеры определенной формы, и алгоритмы всегда будут выделять кластеры таких форм, даже если в данных не было кластеров. Поэтому если цель состоит не только в сжатии набора данных, но и в том, чтобы сделать выводы о структуре данных, важно проанализировать, имеет ли набор данных тенденцию кластеризации.

Кластеризация может использоваться для уменьшения количества данных и для категоризации. Однако в исследовательском анализе данных категории имеют лишь ограниченную ценность. Для более ясного понимания структуры данных кластеры должны быть проиллюстрированы. Например, в случае алгоритма k-means центроиды, которые представляют кластеры, все еще являются многомерными, и для их визуализации необходимы дополнительные методы визуализации.

Использование искусственных нейронных сетей для решения задач кластеризации часто является оптимальным вариантом, так как у такого подхода есть ряд отличительных особенностей, а именно:

1. В силу своей природы они легко работают в распределенных системах с большим объемом параллельных вычислений;
2. Способность искусственных нейронных сетей подстраивать весовые коэффициенты, основываясь на исходных данных, позволяет сделать более объективным выбор значимых характеристик.
3. Возможно построение удовлетворительной модели на нейронных сетях даже в условиях неполноты данных;

## 2.3 Искусственные нейронные сети

Искусственные нейронные сети (ИНС) – это набор алгоритмов, смоделированных по принципу человеческого мозга, которые предназначены для распознавания различных паттернов. Они интерпретируют сенсорные данные при помощи своего рода машинного восприятия, маркировки или кластеризации необработанных данных.

Доктор Роберт Хехт-Нильсен, являющийся изобретателем первого нейрокомпьютера, определяет нейронную сеть как: «… вычислительная система, состоящая из ряда простых, сильно взаимосвязанных элементов обработки, которые обрабатывают информацию путем их динамического реагирования на внешние воздействия».

ИНС состоят из нескольких узлов, называемых нейронами, которые имитируют биологические нейроны мозга человека. Узлы в ИНС связаны между собой связями, а именно синапсами, которые являются взвешенными значениями. Это означает, что нейрон учитывается число синапса и выполняет некоторое вычисление, после этого результат данного вычисления умножается на определенный вес. Вывод на каждом узле называется значением этого узла или его активацией.

Любая ИНС состоит из различного количества слоев, которые представляют собой простой набор нейронов. В ИНС есть входной слой, представляющий собой данные, которые в дальнейшем будут обрабатываться нейронной сетью. Также есть скрытые слои, в которых и реализуются все операции, проделываемые нейронами. В выходном слое ИНС содержатся результаты работы сети. Наглядное изображение структуры ИНС представлено на рисунке 2.2.

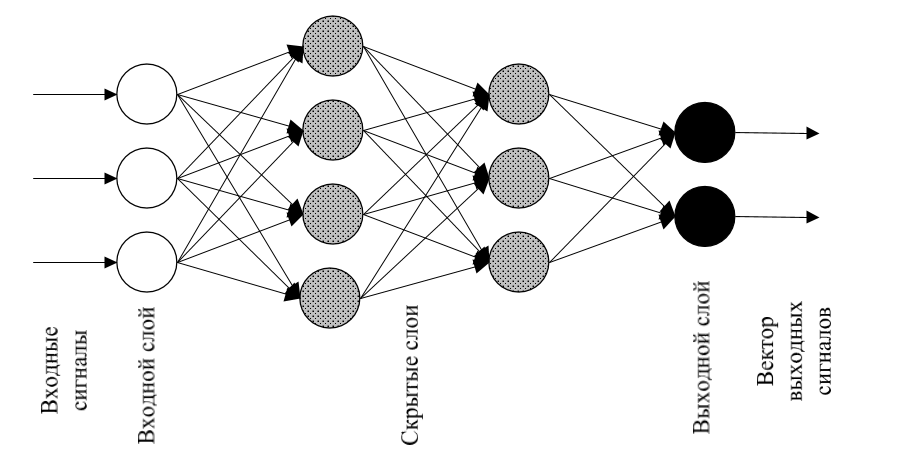


Рисунок 2.2 – Структура искусственной нейронной сети

Искусственные нейронные сети условно можно разделить на четыре группы:

1. Однослойные и многослойные сети прямого распространения
2. Рекуррентные сети: Хопфилда (Hopfield), Хэмминга (Hamming), сети адаптивного резонанса (ART)
3. Самоорганизующиеся сети Кохонена (Self-Organising Maps, SOM)
4. Гибридные сети: радиально-базисные сети, иерархические классификаторы.

Работа однослойного персептона заключается в умножении входного вектора на матрицу коэффициентов. Особенностью данного подхода является то, что любой элемент S соответствует одному элементу A, а S-A связи имеют вес +1.

В многослойных персептронах связи нейронов направлены строго от входных к выходным нейронам, а выход узлов одного слоя образует вход для узлов следующего слоя.

Рекурентные нейронные сети также имеют отличительную особенность. При работе нейронной сети данного типа нейроны получают информацию как от предыдущего слоя, так и от самих себя с предыдущего прохода. Вследствие этого при работе с рекурентными сетями порядок подачи данных и порядок обучения сети является важным.

Самоорганизующиеся карты Кохонена успешно применяется для решения задач распознавания, так как сети этого класса могут выявлять новые закономерности во входных данных. Данный тип нейронных сетей будет рассмотрен подробнее в дальнейшем.

Гибридные нейронные сети представляют собой объединение нескольких разных типов нейронных сетей, различных по структуре и принципам работы, с целью декомпозиции сложных задач на более простые.

Для более наглядного представления, после проведения подробного анализа источников информации [14], была составлена сравнительная таблица 2 моделей нейронных сетей, в которой отмечены задачи, решаемые при помощи той или иной модели.

Таблица 2

Сравнительный анализ моделей нейронных сетей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Однонаправленные многослойные сети | Рекурентные нейронные сети | Сети Кохонена | Радиальные нейронные сети |
| Ассоциативная память | + | + | \_ | + |
| Сжатие информации | + | + | \_ | - |
| Прогнозирование | + | + |  | + |
| Оптимизация | - | + | + |  |
| Классификация | + | - | + | + |
| Кластеризация | - | - | + | + |

Как видно из таблицы, для решения задач кластеризации используются только сети Кохонена и радиальные нейронные сети. Но, в отличии от сетей Кохонена, радиально базисные сети не используются для задачи оптимизации, которая заключается в нахождении наилучшего решения задачи при заданных ограничениях и условиях.

Кластеризация является задачей, относящейся к стратегии "обучение без учителя", то есть не требует наличия значения целевых переменных в обучающей выборке. Для нейросетевой кластеризации данных могут использоваться различные модели сетей, но наиболее эффективным является использование сетей Кохонена или самоорганизующихся карт.

## 2.4 Сети Кохонена

Сеть Кохонена представляет собой однослойную нейронную сеть, в которой входные данные представляются в виде вектора, состоящего из описания объекта [6]. Данный вектор в процессе работы подлежит кластеризации. Входные данные изображаются в виде точек в пространстве, каждая из которых проецируется на нейрон. При этом каждый из этих нейронов связан с опорным вектором. В качестве меры близости при этом используется Евклидово расстояние.

Большинство данных реального мира, например, текстовые данные или данные из биоинформатики, являются многомерными, и сети Кохонена являются отличным инструментом для уменьшения размеров и помощи в анализе таких данных. Это достигается благодаря свойству самоорганизации, которое создает набор векторов-прототипов так, что векторы, соответствующие сходным точкам во входном пространстве, топографически ближе на карте признаков, а векторы, соответствующие разнородным точкам, находятся дальше друг от друга.

Работа алгоритма заключается в том, что в качестве обучающей выборки берется каждая точка данных, которая при дальнейшей работе направляет движение опорных векторов к значениям данных, который составляют эту выборку. Векторы, которые связанны с нейронами, называются весами и изменяются в процессе обучения, стремясь к характерным значениям распределения входных данных. В конце работы алгоритма набор входных данных разделяется на кластеры, и вес, связанный с каждым нейроном, является характеристическим значением кластера, связанного с нейроном.

Основными свойствами, делающие сети Кохонена полезными для кластеризации, являются:

* 1. Низкий размер сети и ее простая структура.
  2. Простое представление кластеров с помощью векторов, связанных с каждым нейроном.
  3. Обучение без учителя

## 2.5 Структура сети Кохонена

Сеть Кохонена представляется собой плоскую прямоугольную решетку размером , состояющую из M нейронов. Такой элемент называется слоем. Модель такой сети представлена на рисунке 3.

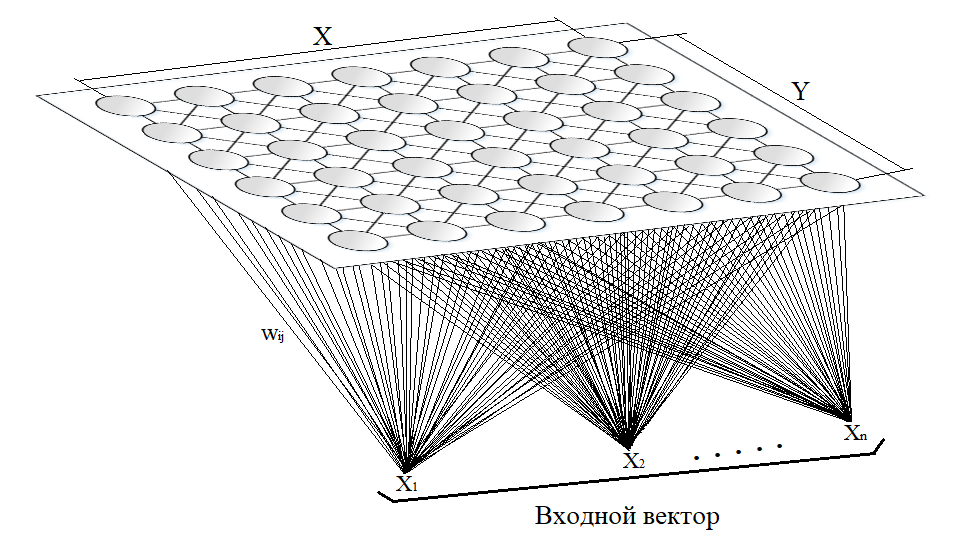


Рисунок 2.3 – Модель сети Кохонена

Нейроны, которые расположены в одном слое, представляют собой двумерную плоскость. К каждому нейрону, содержащемуся в слое, поступает входной сигнал, представляющий собой N-мерный вектор данных. Далее производится обработка входных сигналов, в результате которой можно получить характеристику каждого нейрона. Она складывается из двух показателей – веса нейрона и его положения в слое.

Положение нейронов характеризуется некоторой метрикой и определяется топологией слоя, при которой соседние нейроны во время обучения влияют друг на друга сильнее, чем расположенные дальше. При этом значение синапсов может быть ускоряющими или тормозящими. Если синапсы являются ускоряющими, то каждый нейрон образует взвешенную сумму входных сигналов с и , если синапсы тормозящие.

Так как нейроны связаны между собой, то возбуждение одного нейрона позволяет вычислить возбуждение остальных нейронов в слое. При этом с увеличением расстояния от возбужденного нейрона это возбуждение уменьшается. Поэтому центр возникающей реакции слоя на полученное раздражение соответствует местоположению возбужденного нейрона. Для изменения реакции слоя необходимо изменить входной обучающий сигнал, так как это приведет к возбуждению другого нейрона.

## 2.6 Карты Кохонена

Самоорганизующаяся карта Кохонена (Kohonen SelfOrganizing Maps, SOM) представляет собой алгоритм нейронной сети, который используется для инженерных задач, а также для анализа данных [8]. Если данные являются многомерными или не числовыми, можно использовать самоорганизующуюся карту для представления данных в двумерном пространстве. Данные карты можно рассматривать как пространственно ограниченную форму кластеризации k-means или как проекцию на заранее определенную сетку правильной формы, поддерживающую отношения соседства в данных.

Нейроны – это элементарные ячейки системы, способные передавать электрические и химические сигналы. Они организованы в сети, где тесно связаны друг с другом с помощью различных связей - синапсов. У данных связей есть параметр вес, благодаря которому информация при передаче между нейронами изменяется.

Сети Кохонена состоят из сетки нейронов, также называемых узлами, каждая единица сетки связана с входным вектором X через веса синапса . Эта сборка нейрона в сетке представляет собой сеть неконтролируемых искусственных нейронов.

Карты Кохонена применяются для решения различных задач, но в основном они используется для обнаружения новых закономерностей в данных или для разведочного анализа.

Для распознавания кластеров в наборе данных или же для установления близости классов можно использовать карты Кохонена, так как их использование позволяет пользователю улучшить понимание структуры исследуемых данных для дальнейшего уточнения нейросетевой модели. Если же классы в сети уже заданы, то использование карт Кохонена позволит выявить различные сходства между выделенными классами.

Помимо решения задачи классификации сеть Кохонена способна распознавать кластеры во входных обучающих данных. Если в дальнейшем обученная сеть сталкивается с набором данных, отличающимся от обучающего, то она не способна классифицировать этот набор данных и вследствие этого выявляет его новизну.

## 2.7 Алгоритм самоорганизации карты Кохонена

Алгоритм самоорганизации карты Кохонена является одной из старейших нейронных моделей. Он стремится проецировать высокоразмерные данные в низкоразмерное пространство. Принцип этого алгоритма заключается в выполнении кластеризации сложных баз данных путем выявления похожих групп.  Основное отличие самоорганизующейся карты Кохонена от нейронной сети заключается в том, что самоорганизующаяся карта является примером использования неконтролируемого обучения, поэтому при работе с ней результат зависит исключительно от структуры входных данных.

Алгоритм самоорганизующихся карт является одним из типов кластеризации многомерных векторов. Важным отличием алгоритма SOM является то, что все нейроны, представленные узлами сети, структурированы, как правило в двумерной сети. В процессе обучения модифицируется не только нейрон-победитель, но и его соседи, хоть и в меньшей степени. В связи с этим алгоритм SOM ​​можно считать одним из методов проецирования многомерного пространства в пространство меньших измерений. При использовании этого алгоритма векторы, аналогичные исходному пространству, на выходной карте располагаются также близко.

Алгоритм SOM ​​использует упорядоченную структуру нейронов. Обычно используются одно или двухмерные сетки. Каждый нейрон представляет собой *n-* мерный вектор-столбец, где *n* определяется размерами исходного пространства (формула 3)

|  |  |
| --- | --- |
|  | (3) |

Для неконтролируемого обучения искусственной нейронной сети используются следующие шаги алгоритма [7]:

1. Сначала необходимо инициализировать сеть со случайными значениями веса W входных нейронов X
2. Далее на каждой итерации t необходимо:

* Выбор случайным образом учебного примера X (t).
* Определение нейрона победителя k, вес которого ближе всего к входным данным X, по формуле 4.

|  |  |
| --- | --- |
|  | (4) |

где – расстояние во входном пространстве

* Оценка окрестности победившего нейрона на карте происходит в соответствии с формулой 5.

|  |  |
| --- | --- |
| , | (5) |

где – это расстояние в карте, а - функция окрестности.

* Ближайший нейрон-победитель k называется лучшим совпадением и все нейроны в его окрестности скорректированы. Корректировка проходит по формулам 6 и 7.

|  |  |
| --- | --- |
|  | (6) |
|  | (7) |

это шаг обучения, который уменьшается во времени, чтобы обеспечить лучшую регулировку весов.

Этот алгоритм итеративно ищет сходства среди данных и на выходе представляет карту Кохонена, которая позволяет визуализировать и кластеризовать данные.

В результате работы алгоритма могут быть полечены различные карты, позволяющие лучше проанализировать полученные результаты. После работы алгоритма самоорганизующихся карт Кохонена можно поучить следующие карты:

* 1. карта входов нейронов;
  2. карта выходов нейронов;
  3. различные специальные карты.

Карта входов нейронов инициализируется специально для каждого входа нейрона и раскрашивается в соответствии со значением веса нейрона. Так как для самоорганизующейся карты Кохонена применяется неконтролируемое обучение веса нейронов каждый раз подстраиваются под значения входных переменных. В результате такой подстройки они отображаются внутреннюю структуру входных данных. Для анализа данных обычно используют несколько карт входов.

При анализе полученных результатов самой важной является карта выхода нейронов, полученная после выполнения алгоритма, так как на нее проецируется взаимное расположение исследуемых входных данных. Если нейроны имеют одинаковое значение выходов, то они помещаются в один кластер. Кластеры представляют собой области на карте, в которые заключены нейроны с одинаковыми значениями выходов.

Использование только карты входов нейронов и карты выходов допустимо, но, для наиболее точного анализа полученных результатов, следует проводить анализ и других карт. Данные карты представляют собой карты кластеров, матрицу расстояний, матрицу плотности попадания или другие карты, характеризующие кластеры, которые были получены после работы сети Кохонена.

Главное, что необходимо помнить при анализе карт, которые были созданы в результате работы алгоритма, это то, что все упомянутые карты являются лишь различными представлениями одних и тех же нейронов. Эти карты в основном различаются лишь раскраской этих нейронов.

## 2.8 Свойства самоорганизующихся карт Кохонена

Некоторые свойства, которые отличают самоорганизующихся карт от других инструментов интеллектуального анализа данных, заключаются в том, что они являются числовыми и непараметрическими, а также способными к обучению без учителя. Данный метод является полезным в обработке данных, так как не требуется делать никаких предположений о распределении данных, поэтому он может даже найти довольно неожиданные структуры из данных.

Хотя алгоритм кластеризации k-means и SOM очень тесно связаны, способы их использования при анализе данных различны. В то время как в алгоритме кластеризации k-means число кластеров должно выбираться в соответствии с количеством кластеров в данных, в SOM число опорных векторов может быть выбрано значительно большим, независимо от количества кластеров.

Метод SOM имеет преимущества сжатия данных. То есть данные выборок из многомерного пространства отображаются в низкоразмерном пространстве при сохранении топологии без изменений. Независимо от того, сколько пространственных измерений имеют входные данные, они могут отображаться в одной области выходного слоя SOM. Метод SOM извлекает, захватывает и сохраняет особенности. После моделирования процесса векторы в многомерном пространстве могут быть более четко выражены в низкоразмерном пространстве признаков.

Преимущества этого метода также включают устойчивость к шумным данным, а также возможность обучать нейронную сеть без участия «учителя». При таком методе обучающий набор состоит из значений входных переменных, а в процессе обучения нет сравнения выходов нейронов с желаемыми значениями

Кроме описанных преимуществ самоорганизующиеся карты Кохонена, как и любая нейронная сеть, имеет ряд сложностей, которые затрудняют реализацию. Одной из таких сложностей является то, что алгоритм работает только с числовыми данными, а это значит, что текстовые данные нуждаются в преобразовании. Помимо этого, при работе алгоритма, необходимо изначально задавать количество кластеров для задачи кластеризации, а это значит, что предварительно необходимо произвести анализ исходных данных для определения оптимального количества кластеров. Главным недостатком самоорганизующихся карт Кохонена является то, что оптимальное разбиение набора данных в результате может быть не найдено.

## Выводы 2 главы

В этой главе были рассмотрены искусственные нейронные сети, которые применяются для решения широкого круга задач, таких как классификация, кластеризация, категоризация образов, прогнозирование. Был произведен подробный разбор задачи и методов кластеризации, сетей и самоорганизующихся карт Кохонена, используемых для выявления закономерностей в исходных данных.

ГЛАВА 3 ФОРМИРОВАНИЕ КЛАССИФИКАЦИИ УГРОЗ С ПОМОЩЬЮ САМООРГАНИЗУЮЩЕЙСЯ КАРТЫ КОХОНЕНА

## 3.1 Разработка базы внутренних инцидентов информационной безопасности

Большинство существующих классификаций угроз безопасности обычно ограничиваются использованием одного или двух критериев для классификации, а другие представляют неисчерпывающий список угроз, и их категории не являются взаимоисключающими. Этого может быть достаточно для небольшой организации, где угрозы безопасности относительно стабильны, но в постоянно меняющихся условиях организации не могут выстроить защиту от внутренних угроз.

На самом деле, организации подвержены нескольким видам угроз, которые влияют на их репутацию, и для снижения рисков важно, идентифицировать все характеристики угроз.

Основная идея разрабатываемой классификации – объединить критерии классификации большинства угроз и показать их потенциальные воздействия. При это использовать следующие основные критерии классификации:

* 1. Источники угроз безопасности: лица, которые вызывают угрозы. Были определены три основных класса: сотрудники, руководители, подрядчики.
  2. Мотивация угроз безопасности: цель злоумышленников в системе, которая может быть злонамеренной или не злонамеренной.
  3. Воздействия угроз: нарушение безопасности, возникающее в результате действия угрозы. Они были определены как нарушение конфиденциальности, целостности или доступности информации.

## 3.2 Сбор информации и формирование базы внутренних инцидентов информационной безопасности

Процесс создания классификации внутренних угроз информационной безопасности состоит из нескольких шагов, первым из которых является создание общей базы инцидентов.

При реализации внутренних угроз для обеспечения ИБ в организации должно происходить два типа действий, а именно противодействие возникновению и предотвращение этих угроз. Для противодействия угрозе необходимо обнаружить нарушителя по различным поведенческих и техническим характеристикам и выбрать те меры, которые будут уместны в конкретной ситуации. Но описанные действия возможно реализовать только в том случае, если организация имеет актуальную классификацию угроз ИБ, именно поэтому так важно ее составление. Для составления такой классификации оптимальным решением будет проведение анализа уже случавшихся ранее внутренних инцидентов ИБ.

Несмотря на то, что IT-сфера стремительно развивается, в настоящий момент времени нет ни одной общедоступной базы инцидентов ИБ, что существенно усложняет проведение работы. Однако в сети существует множество различных источников, которые публикуют информацию о произошедших инцидентах. Существенным недостатком таких источников является то, что данные не упорядочены в виде базы данных, а, следовательно, затрачивается множество времени на поиск инцидентов. Одним из таких источников является сайт научного центра «CERT» на котором можно найти две базы инцидентов, одна из которой очень большая по объему, а другая, наоборот, недостаточного объема. Другим хорошим источником является сайт российской компании «Infowatch»[16], которая специализируется на информационной безопасности в корпоративном секторе. На сайте компании публикуется аналитика отрасли ИБ, в которой можно найти аналитические отчеты и сведения о произошедших утечках информации. К сожалению, данные не сформированы в одну базу, а представляют собой множество различных источников информации. Именно этот ресурс и был выбран главным источником для формирования базы внутренних инцидентов ИБ.

При составлении базы внутренних инцидентов было исследовано около 700 различных источников с описанием инцидентов, произошедших в период с 2015 по 2020 год. В результате составлена база инцидентов, состоящая из 192 записей, сформированная по подходу, который используется научным центром «CERT», а именно «Портрет организации – Портрет нарушителя – Портрет инцидента». Однако, составленная база инцидентов содержит меньше параметров, нежели база инцидентов «CERT», так как в открытых источниках содержится лишь малая часть информации. Составление базы внутренних инцидентов происходило в программа для работы с электронными таблицами Microsoft Excel.

После проведения анализа была получена база внутренних инцидентов, состоящая из наиболее важных критериев классификации, а именно должности инсайдера, мотив неправомерного действия, свойство информации, которое было нарушено в результате инцидента (конфиденциальность информации, целостность и доступность), наличие внутреннего или внешнего сговора, а также категория информации, которая была затронута (модифицирована, удалена или разглашена) в результате произошедшего инцидента. Для последующего анализа было добавлено описание каждого инцидента и ссылка на источник данных, а также название организации, пострадавшей в ходе инцидента. К сожалению, собрать информацию о материальном ущербе в результате каждого инцидента собрать не удалось, так как в открытом доступе находятся не полные данные об инцидентах ИБ. На рисунке 3.1 приведена часть получившейся базы инцидентов, так как полное перечисление всех критериев затруднило бы отображение данных.



Рисунок 3.1 – Созданная база внутренних инцидентов информационной безопасности

## 3.3 Подготовка данных для моделирования

Для дальнейшей обработки данных должности инсайдеров были разделены на три группы, а именно: сотрудник, подрядчик и руководитель. В качестве мотива было решено указать получение личной выгоды от совершения неправомерных действий, халатность сотрудника или его идейные соображения, которые были целью совершения данных действий. Поле название организации служило ориентиром для того, чтобы избежать повторяющихся инцидентов, ведь часто в различных источниках описывают одно и то же происшествие. Описание инцидента было добавлено с целью дальнейшей обработки полученных результатов, ведь недостаточно просто кластеризовать данные, нужно провести анализ для того, чтобы понимать правильно ли было выполнено разделение данных, а также чтобы в итоге составить классификацию инцидентов.

В получившейся базе внутренних инцидентов информационной безопасности каждый элемент данных имеет избыточное количество параметров, которые будут лишь затруднять процесс кластеризации. Для выявления наиболее важных параметров было решено составить матрицу попарных сравнений параметров.

Матрицей парных сравнений элементов называется квадратная матрица размера *,* в клетках которой расположены приоритеты, которые являются весовыми показателями, количественно характеризующими веса элементов , по отношению к некоторому элементу вышестоящего уровня иерархии.

Для составления матрицы каждый из параметров был сравнен с другими. На главной диагонали располагаются единицы, так как в этом случае параметр сравнивается сам с собой. В результате проведенного попарного сравнения параметров была получена матрица, отраженная в таблице 3.

Таблица 3   
Матрица попарных сравнений параметров для кластеризации

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Критерий | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |  |
| Описание (1) | 1 | 2 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 7 |
| Название организации (2) | 0,5 | 1 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 5,5 |
| Должность (3) | 2 | 2 | 1 | 0,5 | 1 | 1 | 1 | 1 | 2 | 1 | 12,5 |
| Мотив (4) | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 14 |
| Конфиденциальность (5) | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 13 |
| Целостность (6) | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 13 |
| Доступность (7) | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 13 |
| Внешний сговор (8) | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 13 |
| Внутренний сговор (9) | 2 | 2 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 1 | 1 | 9 |
| Категория информации (10) | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 12 |

После проведения попарного сравнения всех элементов было выявлено, что такие поля, как описание инцидента, название организации и факт внутреннего сговора не являются достаточно информативными для того, чтобы правильней разделить исходные данные на кластеры. Их было решено исключить из тренировочной выборки и данных, которые будут исследоваться сетью. Но учет этих параметров, при дальнейшей оценке экспертом качества проведенной кластериазции, будет произведен.

## 3.4 Моделирование сети кластеризации данных в MATLAB NEURAL NETWORK TOOLBOX

Для реализации любого алгоритма машинного обучения требуется соответствующее программное обеспечение. Алгоритм самоорганизующихся карт Кохонена не стал исключением. На данный момент существует множество различных программ, которые позволяют работать с данным алгоритмом. Это такие программы как Statistica, NeuroShell, а также Matlab, который и был выбран для кластеризации инцидентов ИБ.

Matlab это пакет прикладных программ, который позволяет решать различные технические вычисления. Для выполнения кластеризации был использован пакет Neural Network Clustering в котором уже реализован алгоритм SOM. Данный пакет полезен тем, что позволяет получить множество разных визуализаций в итоге работы алгоритма. Перед началом работы была подробно изучена программная документация по данному прикладному пакеты программ [15].

В программе Matlab реализовано множество различных функций для работы с самоорганизующимися картами, которые также можно использовать при помощи графического интерфейса. Для открытия графического интерфейса используется команды После выполнения команды пользователю открывается окно, в котором предлагается сделать выбор алгоритма для работы (рисунок 3.2). Для работы с самоорганизующейся картой следует выбрать Clustering App (Кластерное приложение).

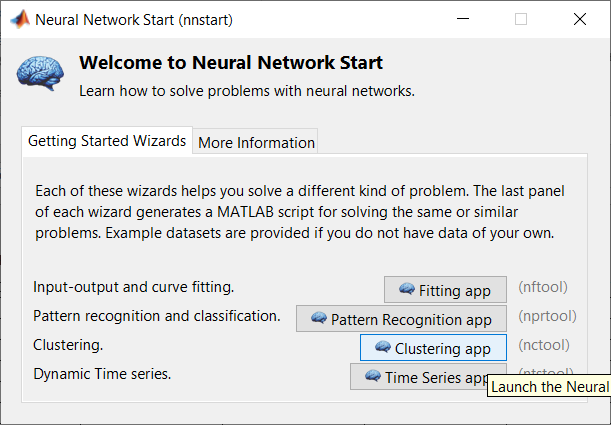


Рисунок 3.2 – Стартовое окно Neural Network Clustering

Для получения объектов, разделенные на кластеры, сначала необходимо на тестовых данных провести тренировку сети. Для этого из составленной базы инцидентов было выбрано 45 записей. Помимо этого, необходимо определить на сколько кластеров будут разделяться данные. После проведения анализа данных перед началом работы с самоорганизующейся картой было решено, что четыре кластера является оптимальным количеством для решения поставленной задачи.

Для работы с самоорганизующейся картой данные должны быть представлены в числовом формате. Так как для кластеризации матрицы объектов не столь важен контекст слов, сколько важна принадлежность данного набора данных к тому или иному классу, было решено тестовые данные заменить на числовые. Для этого был составлен небольшой словарь, где каждому слову соответствовало число, а далее в базе внутренних инцидентов был произведены соответствующие замены. Далее получившийся набор данных был загружен для анализа в Matlab, что показано на рисунке 3.3.

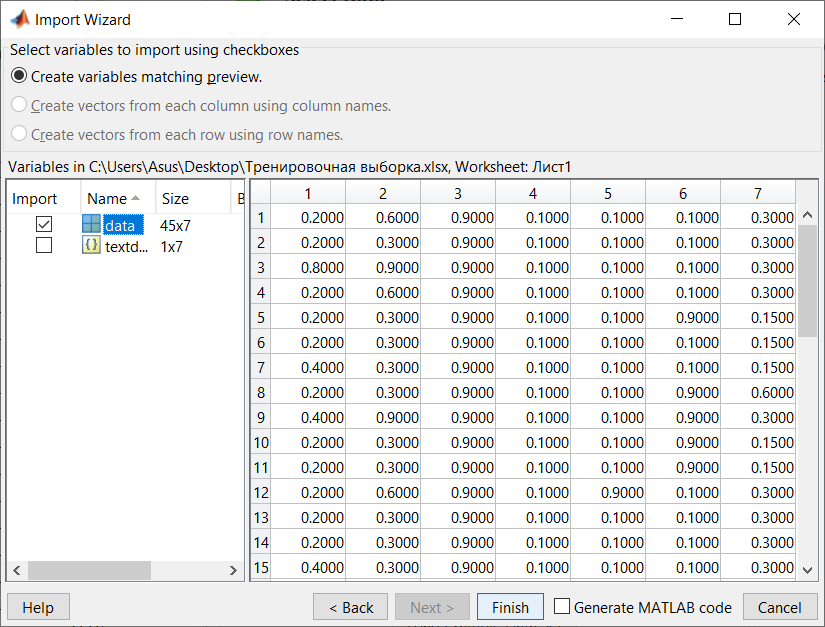


Рисунок 3.3 – Окно импорта данных

Так как после предварительного анализа данных было решено производить разделение на 4 кластера, то размер самоорганизующейся карты был выбран 2\*2, ведь количество кластеров равно количеству нейронов в карте. Структура построенной карты приведена на рисунке 3.4.

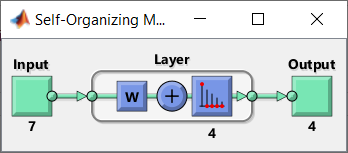


Рисунок 3.4 – Структура самоорганизующейся сети

После этого можно приступать к тренировке сети. Инструмент обучения самоорганизующейся карты показывает структуру обучаемой сети и алгоритмы, используемые для ее обучения. Он также отображает состояние тренировки, а критерии, которые ее остановили, выделяются зеленым цветом. Демонстрация обучения самоорганизующейся карты приведена на рисунке 3.5.

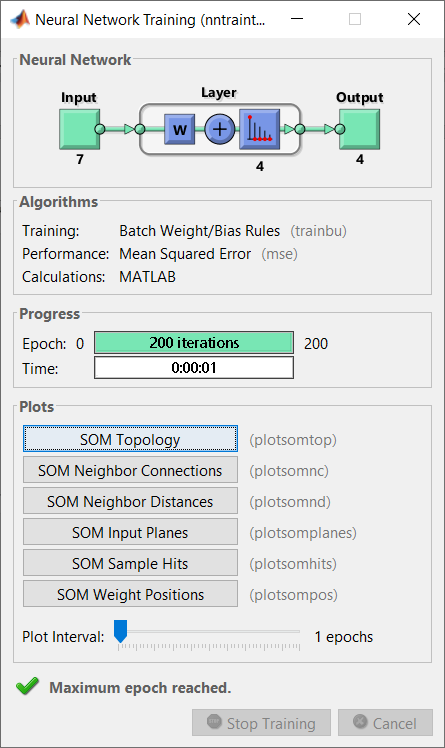


Рисунок 3.5 – Окно модуля с демонстрацией обучения

По умолчанию для самоорганизующейся карты стоит выполнение максимального количество итераций в секунду, а именно двухсот. Так как входные данные были не большого размера сеть обучилась очень быстро, что отображено на рисунке.

Кнопки, расположенные ниже, позволяют получить полезные визуализации, которые можно открывать вовремя и после тренировки.

Для понимания того, как распределяются веса можно использовать функцию **SOM Neighbor Distances, которая наиболее актуальна при работе с самоорганизующейся картой, имеющей больший размер. На рисунке 3.6. нейроны представлены синими шестиугольниками, а красные линии показывают соединение соседних нейронов. Цвета** в областях, которые содержат красные линии, указывают расстояния между нейронами, при этом более темные цвета представляют большие расстояния

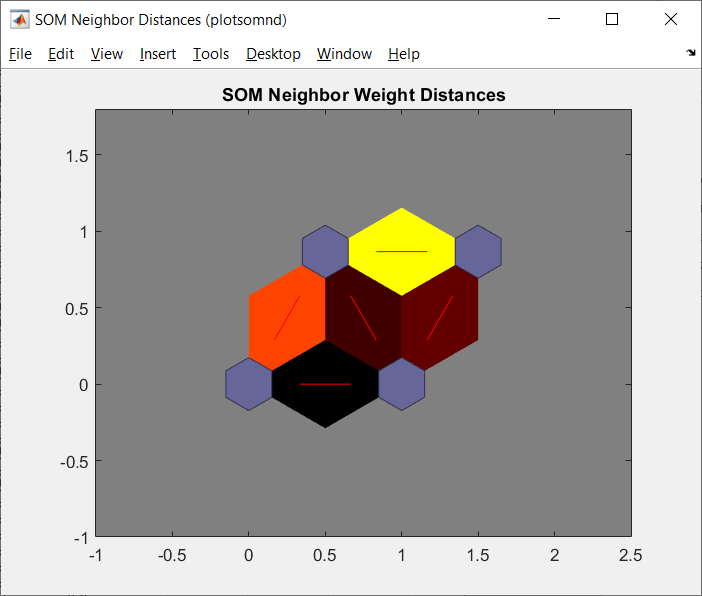


Рисунок 3. 6 – Соединение соседних нейронов и дистанции между ними

Для каждого элемента входного вектора существует компонентная плоскость, которую также называют весовой. В данном случае было выделено семь таких плоскостей, что изображено на рисунке 3.7.

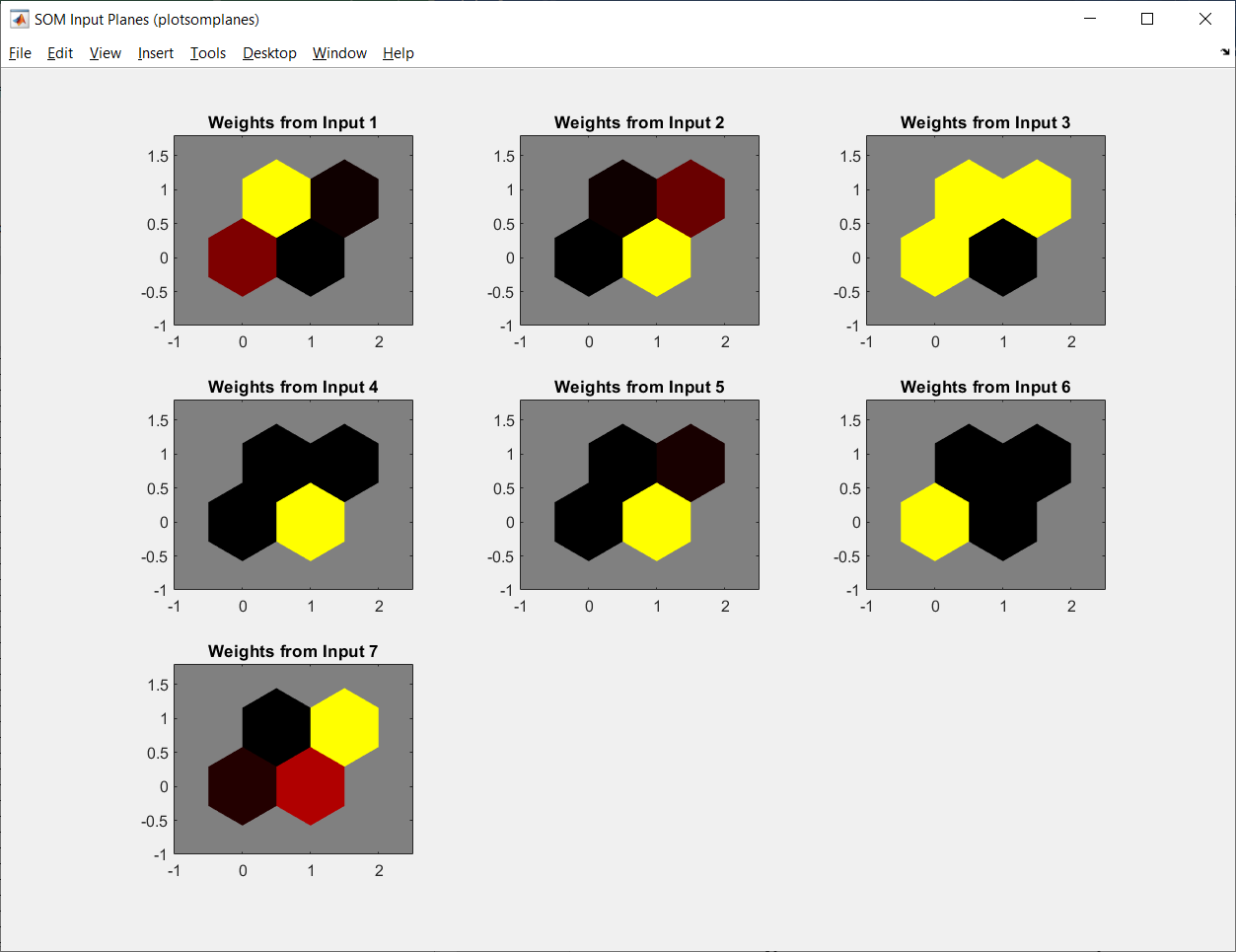


Рисунок 3.7 – Распределения весов для каждого входа

Данная плоскость представляет собой визуализацию весов, которые соединяют каждый вход с каждым из нейронов.  При этом более темный цвет нейрона означает больший вес, а светлый, соответственно, меньший. Если схемы для двух входов имеют одинаковую окраску, можно предположить, что входы были сильно похожи. Из рисунка видно, что вход 4 и 5 являются практически идентичными. На эти входы подаются значения нарушения целостности и доступности информации в результате инцидента, а так как в основном нарушается конфиденциальность инцидентов, то данные характеристики действительно практически идентичны, но исключать их было бы неправильно. Остальные же входы имеют достаточно заметные различия между собой.

Обычно векторы входа, распределяются неравномерно так как решаемые задачи, чаще всего, имеют нелинейный характер, а нейроны на карте Кохонена будут имеют тенденцию распределяться в соответствии с плотностью размещения векторов входа. Из этого следует, что при обучении самоорганизующейся карты Кохонена помимо задачи кластеризации данных выполняется их классификация.

Для того чтобы увидеть сколько точек данных стало связанно с каждым нейроном в результате обучения можно воспользоваться функцией **SOM Sample Hits. Обучение было проведено множество раз, с целью получения наилучшего результата. Из полученной визуализации, приведенной на рисунке 3.8, видно, что данные разделились не равномерно и есть два одинаковых по размеру класса.**

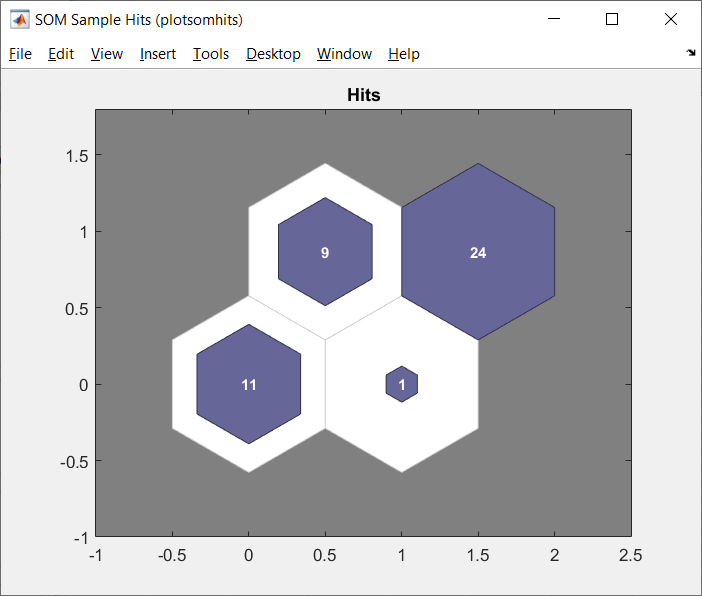


Рисунок 3.8 – Частота выигрышей нейронов карты Кохонена при обучении

В результате тренировки сети было получено разделение тренировочной выборки на кластеры, которое было сохранено в отдельный файл, представляющий собой список векторов, где принадлежность объекта к определенному классу обозначается единицей. При этом получившийся результат нуждается в обработке для определения принадлежности объекта к некоторому классу. Для этого можно воспользоваться функцией vec2ind, которая преобразует векторы в индексы, обозначающие номер класса (рисунок 3.9).

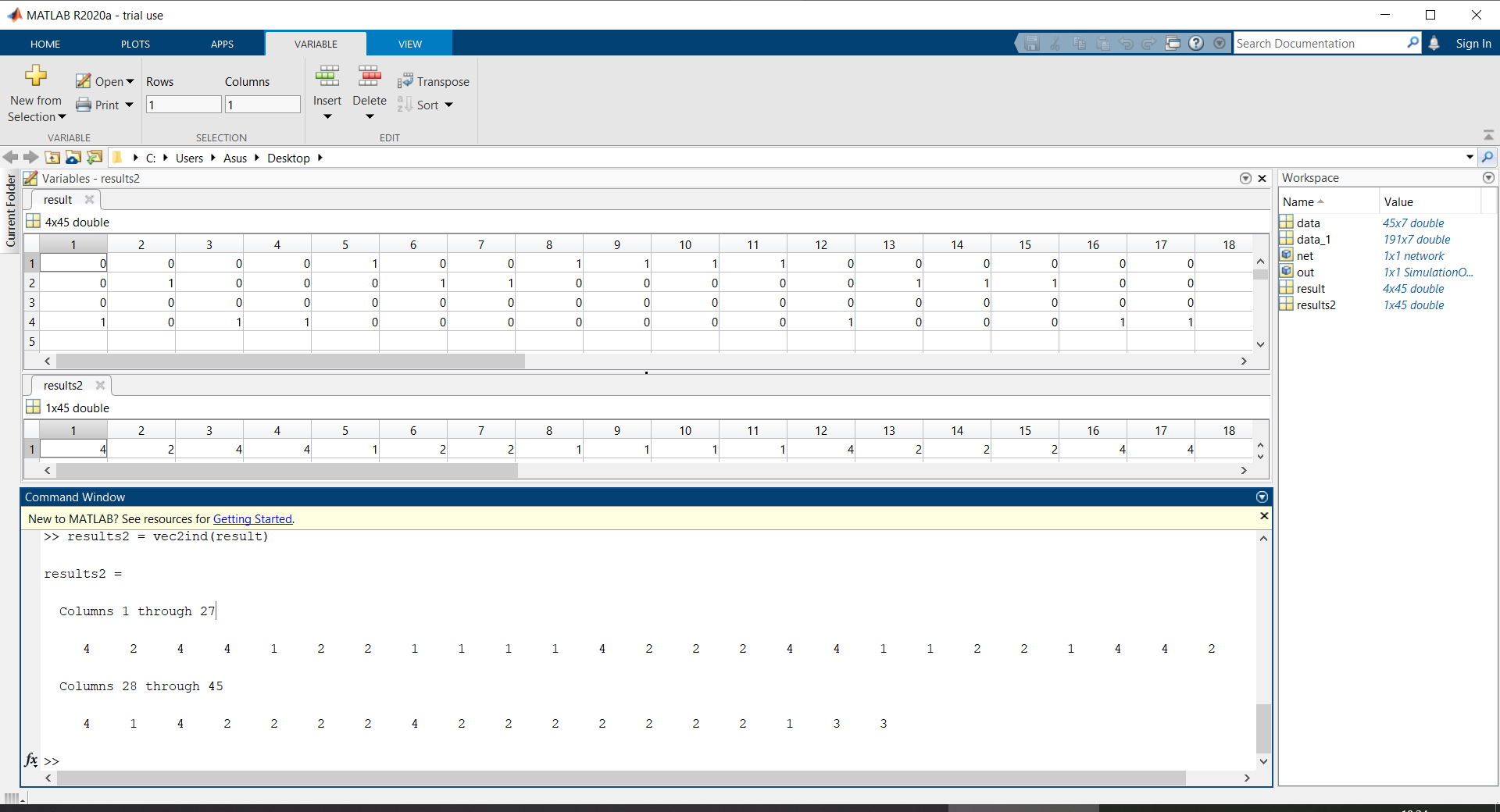


Рисунок 3.9 – Преобразование данных из векторной формы

После преобразования данных было произведено сравнение полученных результатов разбиения с тем разбиением, которое производилось непосредственно перед обучением самоорганизующейся карты. Безусловно, предварительное разбиение является субъективным, ведь при его проведении помимо данных, предоставляемых сети, учитывалось описание инциденты, но именно благодаря этому данное разбиение является наиболее верным и эталонным.

В результате сравнения двух разбиений было выявлено, что самоорганизующаяся карты при разбиении имеет большой процент ошибочного определения принадлежности к тому или иному классу. Для уменьшения процента ошибки был произведен ряд действий, а именно: был увеличен размер сети, но получившееся разбиение было далеко не однородным, также был введен ряд новых параметров для кластеризации, чтобы алгоритм произвел лучшее разделение. Вводились такие параметры как получение непосредственно денежной выгоды, а также намеренность действий, чтобы избежать путаницы между набором данных, характеризующих халатные действия, и данными, которые указывают на действия из идейных соображений. Помимо этого, с целью получения лучшего разбиения, удалялись некоторые параметры, такие как мотив и внешний сговор. В результате всех проделанных действий не было получено лучшего разбиения и поэтому было принято решение использовать ранее полученную сеть для кластеризации всего набора данных.

После того, как сеть обучилась на тренировочном наборе данных, ее следует использоваться для обработки всей базы внутренних инцидентов, которая была предварительно обработана, по тому же принципу, что и тренировочная выборка. Самый простой способ узнать, как использовать функции командной строки панели инструментов, — это сгенерировать сценарии из графического интерфейса (приложения), а затем изменить его для анализа всего набора данных. Измененный сценарий работы представлен в приложении.

В результате было получено разбиение исходных данных, представленное на рисунке 3.10, на 4 кластера, которые после произведенного анализа условно можно разделить по мотиву действий на инциденты, произошедшие в результате халатности сотрудника, этот класс состоит из 44 элемента данных, а также инциденты, произошедшие с целью получения выгоды, к этому кластеру был отнесен 101 элемент. К кластеру, содержащему элементы данных, соответствующие инцидентам, произошедшим из-за различных идейных интересов сотрудника, было отнесено 37 элементов данных. Последний кластер наиболее состоит из 9 элементов и включает в себя данные, характеризующие мошеннические действия сотрудника.

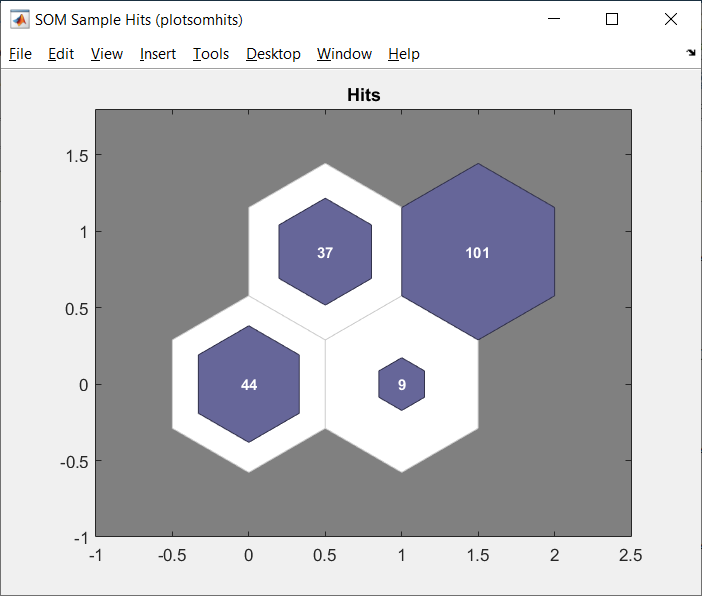


Рисунок 3.10 – Частота выигрышей нейронов карты Кохонена

## 3.5 Формирование классификации внутренних угроз информационной безопасности

После проведения кластеризации базы внутренних инцидентов был произведен анализ соответствия данных кластеру. В результате этого анализа было выявлено, что оптимальным разбиение отличает от предоставленных сетью. Результаты проведенного анализа представлены в таблице

Таблица 4

Сравнение экспертной оценки с разбиением сети

|  |  |  |
| --- | --- | --- |
|  | Разбиение с помощью самоорганизующейся карты Кохонена | Экспертная оценка принадлежности к кластеру |
| Идейные соображения | 37 | 21 |

Продолжение табл. 5

|  |  |  |
| --- | --- | --- |
| Получение выгоды | 101 | 116 |
| Халатность сотрудника | 44 | 40 |
| Мошеннические действия | 9 | 14 |

Помимо этого, не все классы, выделенные сетью, являются однозначными, так как в одном кластере могут содержаться данные, однозначно отнесенные к кластеру ошибочно. Это явление может быть объяснено тем, что любые нейронные сети имею процент ошибки и самоорганизующаяся карта не является исключением.

Самоорганизующиеся карты Кохонена используются не только для кластеризации данных. С помощью данного алгоритма выявляются нетипичные закономерности, поэтому для составления итоговой классификации внутренних угроз информационной безопасности были учтены оба разбиения сети.

Составление итоговой классификации происходило путем анализа описания инцидента, параметров, используемых для кластеризации, а также с учетом разбиений. Описание инцидента позволило разделить полученные классы на подклассы. В результате была составлена классификация угроз, представленная в таблице 6.

Таблица 6

Классификация внутренних угроз информационной безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| Кластер | Объединенный класс угроз | Класс угроз | Наиболее распространенный мотив инсайдера |
| Идейные соображения | Нарушения из-за собственных интересов | Неправомерный доступ к информации в личных целях | Идея |
| IT-саботаж из-за мести или обиды | Удаление информации | Месть/обида |

Продолжение табл. 6

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Внесение неправомерных изменений при удаленном подключении | Месть/обида |
| Порча оборудования или изменение параметров системы | Месть/обида |
| Выгода | Шпионаж | Длительная кража информации для собственной выгоды | Деньги |
| Разовая кража информации | Деньги |
| Кража информации для открытия своего бизнеса или перехода к конкуренту | Деньги |
| Мошенничество | Мошеннические действия с целью получения выгоды | Незаконная модификация счетов | Деньги |
| Незаконное оформление кредитов | Деньги |
| Мошенничество с банковскими картами | Деньги |
| Халатность | Халатное нарушение ИБ | Потеря носителя информации | Нет мотива |
| Неправильная утилизация носителя информации | Нет мотива |
| Непреднамеренное разглашение информации | Нет мотива |

## Выводы к главе 3

В данной главе была разработана и сформирована база инцидентов информационной безопасности, произошедших по вине инсайдеров. Помимо этого, собранные данные были подготовлены для дальнейшей работы с самоорганизующейся картой Кохонена. В среде программирования Matlab было проведено построение сети и ее обучение на тестовых данных. После этого алгоритм самоорганизующихся карт был применен к общему набору данных. Полученные результаты были использованы при дальнейшей разработке классификации внутренних угроз.

По результатам работы, проделанной в данной главе, было выявлено, что, в результате работы алгоритма самоорганизующейся карты Кохонена, было получено не совсем верное разбиение входных данных на кластеры, так как при обучении сети не было получено максимально точного разделения на кластеры.

## ЗАКЛЮЧЕНИЕ

В процессе подготовки выпускной квалификационной

## СПИСОК ИСТОЧНИКОВ

1. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
2. ISO. Information Processing Systems-Open Systems Interconnection-Basic Reference Model. Part 2: Security Architecture, ISO 7498-2; 1989 г

## ПРИЛОЖЕНИЕ

ыфв