Учреждение образования

«Белорусский государственный технологический университет»

**Отчет к лабораторной работе № 14**

по дисциплине «Защита информации и надежность информационных систем»

Выполнил:

Cтудент 3 курса 1 группы

Парибок И. А.

Вариант 5

2023 г.

**Согласование криптографических ключей на основе технологий искусственных нейронных сетей**

**Цель:** изучение основ построения и функционирования искусственных нейронных сетей (ИНС), а также использования ИНС в криптографии; приобретение практических навыков программной реализации алгоритма согласования ключевой информации на основе технологии ИНС.

**Задачи:**

1. Закрепить теоретические знания по основам построения и функционирования ИНС.

2. Усвоить особенности построения, основные алгоритмы взаимного обучения двух связанных нейронных сетей на основе модели ТРМ.

3. Разработать приложение для реализации модели ТРМ с целью согласования двумя сторонами совместного тайного ключа.

4. Познакомиться с методиками оценки криптостойкости алгоритма на основе ТРМ.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теоретические сведения**

Современные суперкомпьютеры превосходно справляются с задачами математических вычислений. Однако существует группа задач, решение которых не является для компьютеров простым. К основным из таких общих функциональных задач относятся: распознавание образов (букв, форм, сигналов), классификация и идентификация объектов, ассоциации. Нейронные сети, в которых были реализованы указанные основные функции, нашли применение в очень многих областях науки и техники:

• проектирование космических кораблей;

• распознавание речи;

• нечеткая логика;

• компрессия (сжатие) изображений;

• генетические алгоритмы;

• ряды Фурье;

• анализ и прогнозирование в финансовой сфере;

• безопасность информационных систем;

• системы идентификации;

• бизнес-системы принятия решений;

• переработка изображений;

• прогнозирование временных рядов;

• распознавание текста;

• интеллектуальный анализ данных;

• анализ медицинских исследований

• и др., а также:

• криптоанализ RSA;

• вычисление хеш-функций;

• протокол обмена ключами.

Именно последнее из указанных применений ИНС и является предметом нашего исследования

**Основные принципы построения и основы моделирования ИНС**

Как известно, мозг человека состоит, главным образом, из большого числа соединенных друг с другом элементарных нервных клеток, называемых нейронами. Основная способность нейронов – это возможность управления и выработки нервных импульсов. Каждый нейрон (рис. 1) состоит из коротких ветвистых дендритов, тела клетки, а также длинного волокна, называемого аксоном. Дендриты имеют древовидную структуру, каждая ветвь которой соединена с одним из нейронов. Полученные сигналы передаются посредством дендритов к телу клетки. Аксон – это длинный отросток нейрона, который руководит импульсами от тела клетки к другим нейронам. Он соединен с дендритами других нейронов через биохимические стыки, называемые синапсами. Благодаря дендритам тело клетки получает и суммирует сигналы, приходящие от всех его входов. Если общий сигнал, который достиг тела клетки, превысит пороговой уровень, то возбуждающий сигнал с выхода нейрона пересылается посредством аксона к другим нейронам. К нейрону приходят сигналы, которые могут быть модифицированы через синапсы.

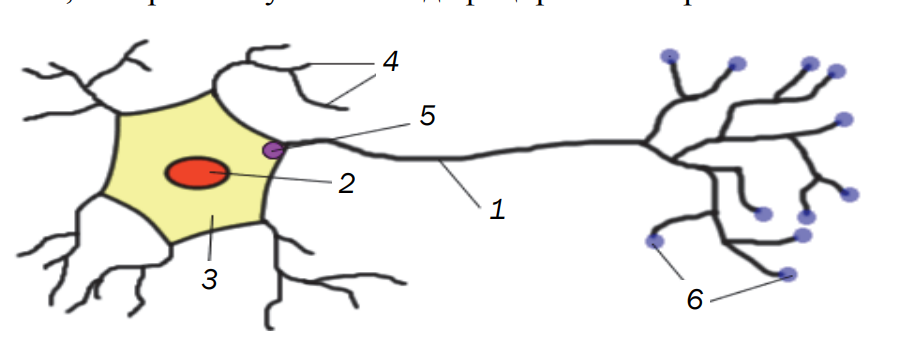
****

Рисунок 1 – Биологическая модель нейрона

На основании вышеуказанного описания спроектирован искусственный нейрон, называемый также персептроном или перцептроном (англ. perceptron), симулирующий работу биологического нейрона (рис. 14.2). Впервые модель искусственного нейрона была представлена У. МакКаллоком и У. Питтсом в 1943 г. в исторической работе [74]. Эта модель содержит главные элементы биологического нейрона. Вот их эквиваленты: входные значения – дендриты, весовые коэффициенты – синапсы, суммирующий блок – ядро, функция активации – основание аксона, а выходное значение – это аксон.

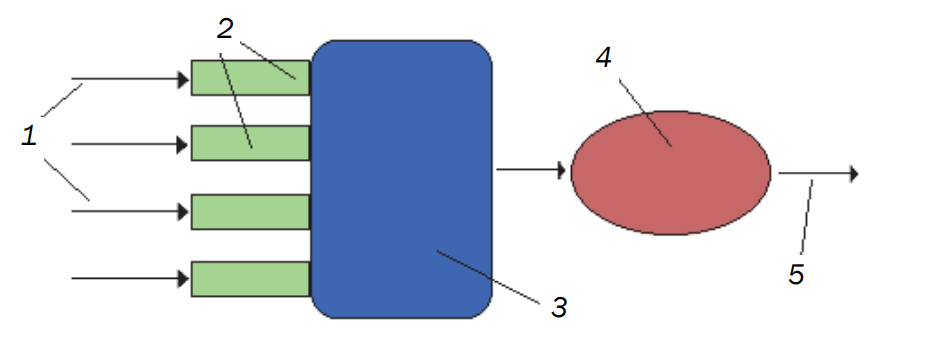
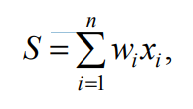
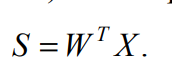
****

Рисунок 2 – Модель искусственного нейрона – персептрона

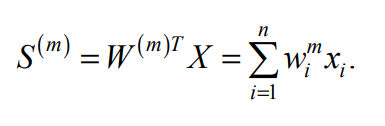
Математически работу персептрона можно описать так [75]:

(14.1)

где xi и wi – соответственно i-e входной сигнал и весовой коэффициент нейрона. Соотношение (14.1) в векторной форме выглядит так:

(14.2)

В соответствии с вышеизложенным нейронная сеть (соединение отдельных нейронов), как элементарный эквивалент человеческого мозга, должна состоять из нейронов. Такую самую простую сеть с прямой связью составляет одиночный нейронный слой. В таком слое каждый нейрон получает одинаковый набор входных сигналов. Выходной сигнал m-го нейрона может быть подсчитан следующим образом:

(14.3)

Таким образом, значение выхода нейрона равно скалярному произведению входных значений на векторы весовых коэффициентов (нейрон с линейной функцией активации). Действие такой сети основывается на вычислении выходов каждого из нейронов на основе общего входного вектора X. Представленная выше модель нейронной сети в принципе бесполезна, так как она не способна решать поставленные задачи до тех пор, пока не будет соответствующим способом «натренирована». Этот процесс называется обучением и основан на соответствующем подборе коэффициентов вектора весов в контексте решаемой задачи.

Взаимное обучение двух ИНС касается простейшей однонаправленной модели, в которой участвуют два персептрона. Роли таких нейронных сетей заранее не определены, каждая может выполнять функции как учителя, так и ученика (в зависимости от этапа обучения). Это значит, что сети учатся друг у друга, используя для этого полученные результаты, и, стремясь к «общей цели», находят общие элементы в результате своих вычислений. Эта модель обучения, благодаря своим свойствам, может быть использована в криптографии, а именно в определении и согласовании двумя сторонами (двумя ИНС) криптографического ключа (аналогично известному нам протоколу Диффи – Хеллмана).

**Синхронизация дискретных персептронов. Модель ТРМ**

Рассмотренный выше процесс взаимного обучения двух персептронов может применяться в криптографии. Общую идею такого подхода изложили И. Кантер и В. Кинцель [76]. Именно общее значение векторов весов обоих персептронов, отличающееся только знаком, может быть использовано в качестве секретного ключа. Протокол этого типа выполняет ту же роль, что и хорошо известный протокол обмена ключами Диффи – Хеллмана. Однако следует обратить внимание на два обстоятельства. Первый из них касается безопасности всей системы. Поскольку если у третьей стороны, наблюдающей за процессом обмена, появится возможность получить внутреннее состояние вектора весов одного из персептронов, участвующих в процессе обмена ключами, то она сможет синхронизироваться с ним. Вторая проблема касается особенностей практического применения всей системы. Обмен информацией в компьютерных системах базируется на пространстве битов, или на дискретных величинах. Поэтому обоснованным является вопрос: будет ли правильным (или сходящимся к общему вектору) процесс обмена ключами для векторов весов с дискретными (битовыми) величинами? Задача решается с помощью многослойной ИНС. Это сеть, называемая машиной четности (англ. parity machine) или, более точно, древовидной машиной четности (англ. Tree Parity Machine, ТРМ). Нейроны представляют собой персептроны с дискретными векторами весов.

Архитектуру сети составляют K классических персептронов, принадлежащих внутреннему уровню; внешний уровень (обозначен римской цифрой II) объединяет выходы персептронов внутреннего уровня (I) (рис. 3, здесь K = 3).

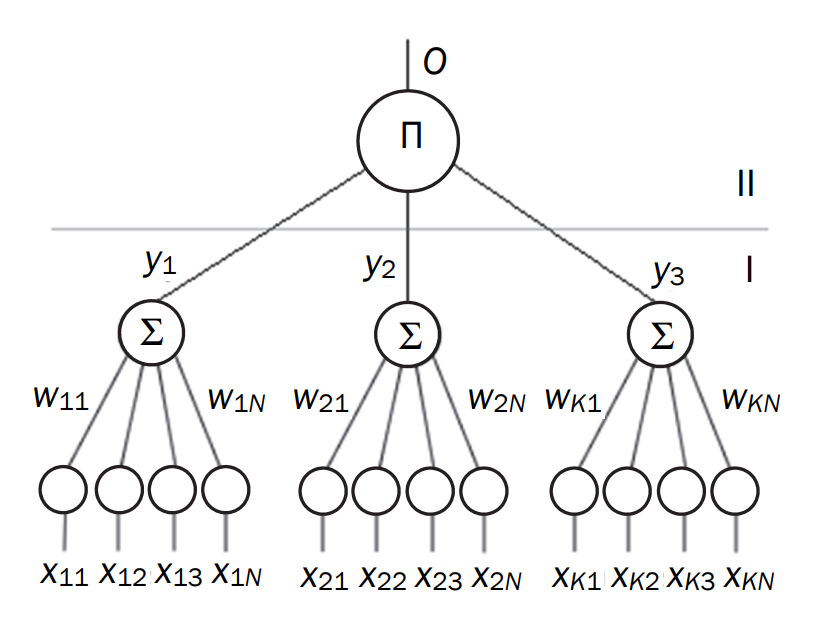


Рисунок 3 – Схема двух уровней модели TPM

Каждый из персептронов имеет N входов. Следовательно, вектор входных значений всей сети равен KN. В этой архитектуре приняты следующие обозначения: xkj – j-тый вход k-того персептрона, yk – выход k-того персептрона, где k = 1, 2, ..., K и j = 1, 2, ..., N. Для упрощения принято, что величины входного вектора бинарны: xkj = {–1, +1}. Каждый из персептронов имеет веса, которые получают j-тую величину входа в k-том персептроне. Следовательно, величины векторов весов обозначаются как wkj. Выход всей архитектуры О – это произведение всех выходных величин внутренних персептронов. Для простоты в дальнейшем будем говорить о рассматриваемой архитектуре как о TPM-архитектуре с тремя внутренними элементами. На величины вектора весов налагаются следующие ограничения: wkj = {–L, –L + 1, ..., 0, ... L – 1, L}.

Представленная выше архитектура, как и все ее параметры, идентичны для обеих сетей, участвующих в процессе синхронизации. Все структурные элементы (как и в других криптографических системах) известны, однако это не представляет угрозы для всей системы. Секретные элементы, на которых основывается конструкция системы, – это начальные состояния векторов весов. Естественно, сети, участвующие в процессе синхронизации, также взаимно «не знают» векторов весов.

Общая схема процесса синхронизации двух сетей в графическом виде представлена на рис. 14.4. Кратко проанализируем особенности процесса синхронизации сетей на основе архитектуры ТРМ.

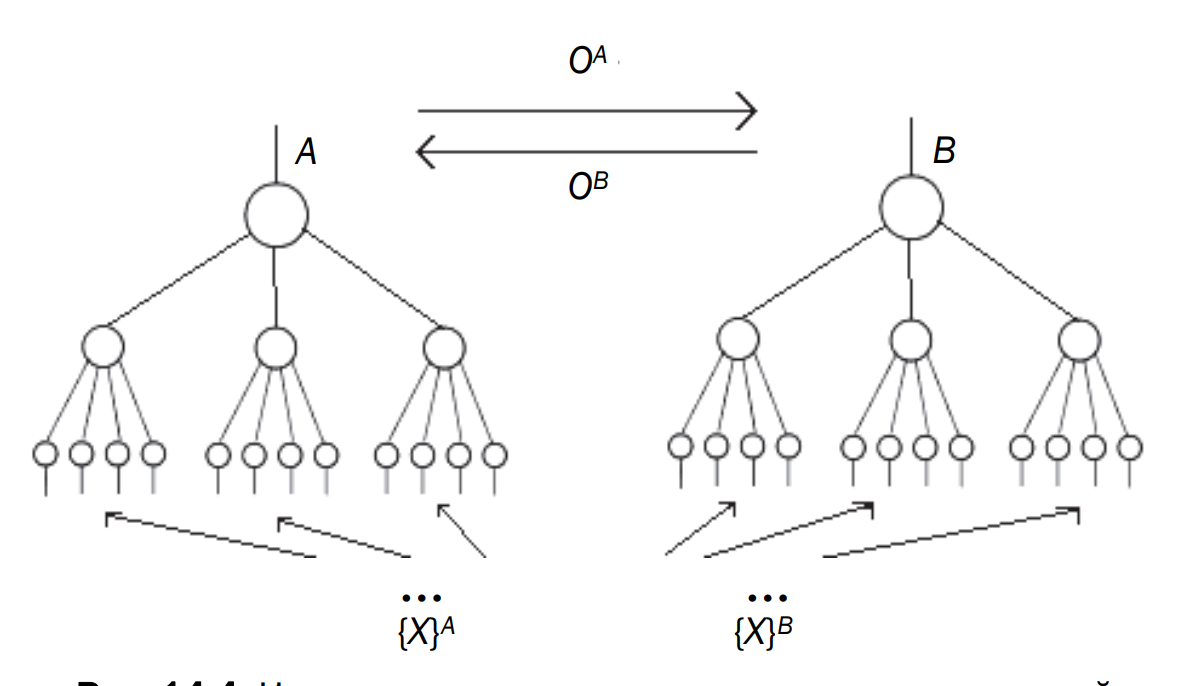


Рисунок 4 – Иллюстрация процесса синхронизации двух сетей

Процесс взаимного обучения, или синхронизации, начинается с инициализации весовых параметров обеих сетей подачей на вход соответствующих бинарных последовательностей (для упрощения на рис. 14.4 обозначены соответственно {X}A и {X}B). Их начальное состояние, выбираемое случайным образом, остается секретным на протяжении всего процесса обучения. Каждый последующий шаг (t + 1) начинается с подачи на входы обеих сетей выбранного случайным образом вектора X.

Две ИНС, обученные на основании вышеуказанной схемы, впоследствии достигают состояния синхронизации. Это означает, что их векторы весов имеют идентичные величины (wA = wB).

Число шагов, за которое векторы весов достигают одинаковых значений, зависит от начальных состояний векторов весов, входных значений и от таких параметров системы, как K и N. Вся процедура взаимного обучения никак не влияет на два первых параметра, так как выбор начальных состояний векторов весов и значение входных величин генерируются случайным способом. Однако параметры K и N пропорционально влияют на увеличение времени синхронизации.

Самый простой способ атаки на синхронизирующиеся сети А и В (со стороны С) основывается на том, что оппонент может знать архитектуру обеих сетей, а также иметь всю информацию, которой обмениваются между собой сети.

**Практическое задание**

Разработать приложение, реализующее модель ТСР, – эмулятор процесса синхронизации весовых коэффициентов двух ИНС. С использованием разработанного приложения произвести не менее 500 реализаций алгоритма синхронизации сетей А и В, параметры которых соответствуют варианту задания.

**Ход работы**

В процессе выполнения конкретной задачи была создана программа, использующая алгоритм Анти-Хэбба для решения проблемы синхронизации между двумя машинами: Alice и Bob. Обновление состояний машин было осуществлено с целью достижения синхронизации. Для этого были инициализированы состояния машин, а затем применен алгоритм Анти-Хэбба для обновления весов связей между нейронами в нейронных сетях машин. В каждой итерации алгоритма машины взаимодействовали друг с другом, обмениваясь информацией о своих текущих состояниях, и затем обновляли свои веса связей в соответствии с полученной информацией. Этот процесс повторялся до достижения состояния синхронизации, когда состояния машин становятся идентичными или очень близкими. Рисунок 1 показывает вызов функций, связанных с синхронизацией машин.

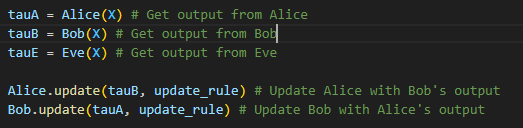


Рисунок 1 – Обновление машин

В функции принимаются входные параметры, включающие выходные значения двух машин и правило, которое будет использоваться для синхронизации. Правило выбирается из массива строк update\_rules, представленного на рисунке 2:

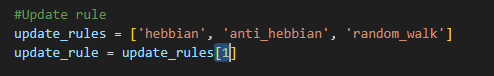


Рисунок 2 – Задание способа реализации

Функция, изображенная на рисунке 3, используется для вычисления состояния синхронизации машин Alice и Bob. В этой функции применяется весовой коэффициент W.

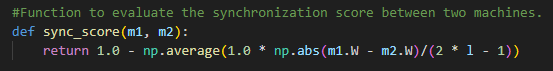


Рисунок 3 – Функция проверки синхронизации

Рисунок 4 показывает сообщение, которое система выводит после завершения процесса синхронизации. Сообщение содержит информацию о количестве выполненных обновлений, необходимых для достижения синхронизации, а также общем времени, затраченном на этот процесс..

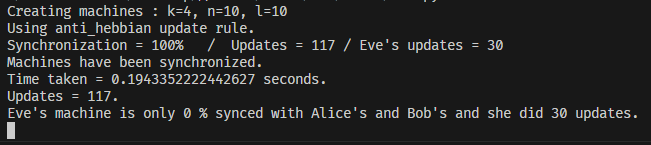


Рисунок 4 – Результат работы приложения

Рисунок 5 отображает график, построенный на основе всех значений, вычисленных в процессе синхронизации.

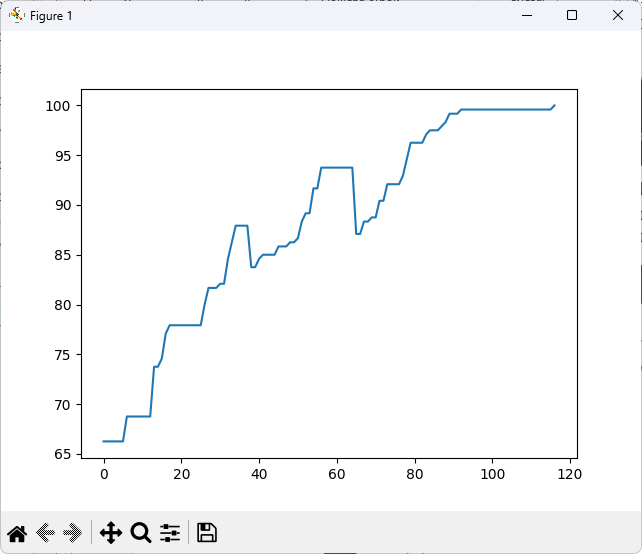


Рисунок 5 – График синхронизации

**Вывод**

Рассматриваемая система была разработана для решения задачи синхронизации между двумя машинами Alice и Bob. Для этого использовался алгоритм Анти-Хэбба, который основывается на обновлении весов связей между нейронами в нейронных сетях машин.

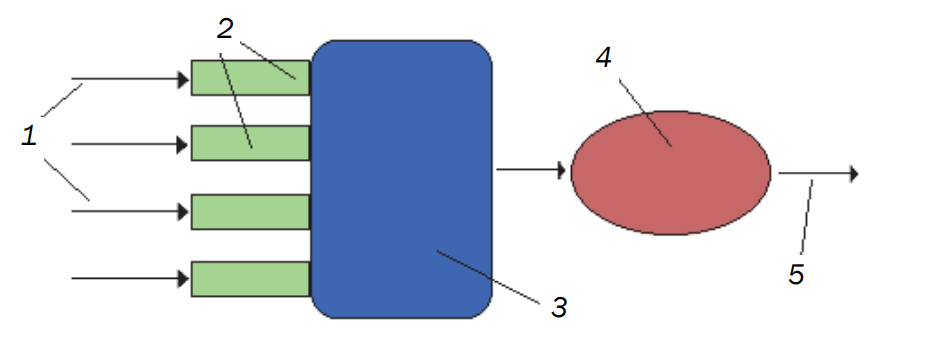
Процесс синхронизации начинается с инициализации состояний машин, затем применяется алгоритм Анти-Хэбба, который выполняется до достижения состояния синхронизации между машинами. После завершения процесса система выводит сообщение с информацией о количестве выполненных обновлений и общем времени, затраченном на процесс синхронизации.

Работа системы является эффективным решением задачи синхронизации между двумя машинами, основываясь на алгоритме Анти-Хэбба.

Для указанных параметров среднее количество шагов для полной синхронизации составляет 117. Среднее время, необходимое для полной синхронизации двух машин, примерно равно 0.19 секунды.

**Контрольные вопросы**

**1. Изобразить схематично структуру персептрона и пояснить аналогии между его компонентами и частями биологического нейрона.**

****

Модель искусственного нейрона – персептрона

Данная модель содержит главные элементы биологического нейрона. Вот их эквиваленты: входные значения – дендриты, весовые коэффициенты – синапсы, суммирующий блок – ядро, функция активации – основание аксона, а выходное значение – это аксон.

**2. Охарактеризовать (и показать на примерах) области использования ИНС.**

Искусственные нейронные сети (ИНС) являются мощным инструментом машинного обучения и находят широкое применение во многих областях. Вот несколько примеров областей использования ИНС:

Обработка изображений: ИНС используются для различных задач обработки изображений, таких как распознавание объектов, классификация изображений, сегментация изображений, реконструкция изображений и многое другое. Например, ИНС могут быть применены для автоматического распознавания лиц в фотографиях или для классификации объектов на изображениях (автомобили, животные и т. д.).

Обработка естественного языка: ИНС применяются для обработки и анализа текстовых данных, включая задачи машинного перевода, распознавания и синтеза речи, определения тональности текста, автоматического ответа на вопросы и другие. Например, ИНС могут использоваться для автоматического перевода текстов с одного языка на другой или для создания голосовых помощников.

Прогнозирование и анализ данных: ИНС широко применяются для прогнозирования и анализа данных в различных областях, включая финансы, экономику, маркетинг и науку о данных. Например, ИНС могут быть использованы для прогнозирования финансовых рынков, анализа покупательского поведения или обнаружения аномалий в данных.

Медицина и биология: ИНС находят применение в медицине и биологии для различных задач, таких как диагностика заболеваний, анализ медицинских изображений, прогнозирование эффективности лекарственных препаратов и других медицинских параметров. Например, ИНС могут использоваться для автоматического обнаружения раковых опухолей на снимках маммографии или для прогнозирования прогноза заболевания.

Автономные системы и робототехника: ИНС играют важную роль в разработке автономных систем и роботов. Они могут быть использованы для навигации, планирования маршрутов, управления роботами и принятия решений на основе восприятия окружающей среды. Например, ИНС могут помочь автономным автомобилям определять и анализировать окружающую дорожную обстановку.

**3. Как в простейшем виде записывается формальное представление персептрона?**

Персептрон представляет собой простую модель искусственного нейрона, используемого в области машинного обучения. В простейшем виде, формальное представление персептрона можно записать следующим образом:

Пусть у нас есть входные данные, представленные вектором x = (x₁, x₂, ..., xₙ), где xᵢ — это значения признаков или характеристик объекта. Каждому признаку xᵢ соответствует весовой коэффициент wᵢ, который отражает важность этого признака.

Сумма взвешенных входов вычисляется как:

z = w₁x₁ + w₂x₂ + ... + wₙxₙ

Затем, на основе этой суммы, применяется функция активации, обычно ступенчатая функция или сигмоидная функция, чтобы получить выходной сигнал:

y = f(z)

Где y — это выходной сигнал или предсказание персептрона.

В простейшем случае, персептрон может выдавать два класса ответов: 1 или 0, что соответствует бинарной классификации. Но его можно модифицировать для многоклассовой классификации.

Это основное формальное представление персептрона. Однако, в реальных задачах обучения нейронных сетей, персептроны обычно объединяются в более сложные архитектуры, такие как многослойные нейронные сети, где каждый персептрон является элементом слоя.

**4. Охарактеризовать (и показать на примерах) области использования ИНС в криптографии.**

Искусственные нейронные сети (ИНС) находят применение в различных аспектах криптографии. Вот несколько примеров областей использования ИНС в криптографии:

Анализ и взлом шифров: ИНС могут использоваться для анализа и взлома различных криптографических шифров. Например, ИНС могут быть применены для атаки на шифр замены или шифр перестановки, путем обучения на большом наборе зашифрованных исходных текстов и попытке восстановить ключ или исходное сообщение. Это позволяет исследователям и криптоаналитикам улучшать методы шифрования и повышать их стойкость.

Создание криптографических функций: ИНС могут использоваться для создания криптографических функций, таких как хэш-функции или генераторы псевдослучайных чисел. ИНС способны обучаться на больших наборах данных и находить сложные статистические закономерности, которые могут быть использованы для генерации высококачественных псевдослучайных последовательностей или создания надежных хэш-функций.

Аутентификация и распознавание: ИНС могут быть применены для аутентификации и распознавания пользователей в криптографических системах. Например, ИНС могут использоваться для распознавания уникальных биометрических параметров, таких как отпечатки пальцев, лица или голоса, для аутентификации пользователей перед предоставлением доступа к зашифрованным ресурсам или выполнению криптографических операций.

Защита от атак и обнаружение аномалий: ИНС могут быть применены для обнаружения аномального поведения или подозрительных активностей в криптографических системах. ИНС могут обучаться на нормальном поведении системы и выявлять отклонения от этого образца, что может указывать на попытки атаки или нарушение безопасности. Это помогает в обнаружении и предотвращении криптографических атак.

**5. Дать пояснение к структуре и функционалу информационной системы на основе ИНС, предназначенной для согласования ключевой информации.**

Информационная система на основе искусственных нейронных сетей (ИНС) для согласования ключевой информации представляет собой комплексную систему, которая использует ИНС для автоматического анализа и обработки информации с целью достижения согласованности и соответствия между различными наборами ключевых данных.

Структура информационной системы на основе ИНС может включать следующие основные компоненты:

Входные данные: это ключевая информация, которую необходимо согласовать. Входные данные могут включать различные наборы ключей, параметры или другую информацию, которая должна быть согласована между различными источниками или системами.

ИНС модель: это нейронная сеть, которая обучается на основе предоставленных данных и используется для анализа и обработки информации. Модель ИНС может состоять из различных слоев нейронов, функций активации и алгоритмов обучения, чтобы достичь требуемой функциональности.

Обучающие данные: это наборы данных, которые используются для обучения ИНС модели. Обучающие данные должны содержать примеры согласованной информации, чтобы модель ИНС могла выявить закономерности и обучиться выполнять согласование на основе этих данных.

Процесс обучения: это шаг, в котором ИНС модель обучается на основе предоставленных обучающих данных. В процессе обучения ИНС модель анализирует исходные данные, настраивает веса своих нейронов и улучшает свою способность согласовывать ключевую информацию.

Выходные данные: это результат работы ИНС модели, который представляет собой согласованную ключевую информацию. Выходные данные могут быть представлены в удобной форме для использования другими системами или для принятия решений на основе согласованной информации.

Функционал информационной системы на основе ИНС включает в себя следующие основные возможности:

Автоматическое согласование ключевой информации: ИНС модель обучается анализировать и согласовывать различные наборы ключевой информации, обнаруживая связи и закономерности между ними и выявляя расхождения или несогласованности.

Выявление и исправление ошибок: ИНС модель может помочь обнаружить ошибки или несогласованности в ключевой информации и предложить решения для их исправления или согласования.

Принятие решений: Информационная система на основе ИНС может использоваться для принятия решений на основе согласованной ключевой информации, что позволяет улучшить точность и надежность принимаемых решений.

**6. Дать характеристику известным алгоритмам обучения ИНС.**

Существует несколько известных алгоритмов обучения искусственных нейронных сетей (ИНС). Каждый из них имеет свои особенности, преимущества и ограничения. Вот некоторые из наиболее известных алгоритмов обучения ИНС:

Обратное распространение ошибки (Backpropagation): Это один из самых распространенных и широко используемых алгоритмов обучения ИНС. Он основан на градиентном спуске и позволяет настраивать веса связей нейронов, минимизируя ошибку между предсказанными и желаемыми выходами сети. Обратное распространение ошибки работает в многослойных нейронных сетях, где ошибки распространяются от выходного слоя к входному для обновления весов.

Алгоритм Левенберга-Марквардта (Levenberg-Marquardt): Этот алгоритм также используется для обучения многослойных нейронных сетей. Он комбинирует методы наименьших квадратов и градиентного спуска для эффективной оптимизации весов. Алгоритм Левенберга-Марквардта обычно сходится быстрее, чем обратное распространение ошибки, но требует больше вычислительных ресурсов.

Алгоритм обучения Хебба (Hebbian Learning): Этот алгоритм основан на принципе ассоциативной памяти и осуществляет обучение нейронных сетей путем усиления или ослабления связей между нейронами в зависимости от их активности и взаимодействий. Алгоритм Хебба позволяет ИНС самостоятельно формировать веса связей на основе входных данных и может использоваться для реализации самоорганизующихся карт и ассоциативных памятей.

Генетические алгоритмы (Genetic Algorithms): Этот класс алгоритмов основан на эволюционном принципе и вдохновлен биологической эволюцией. Генетические алгоритмы используют операторы скрещивания, мутации и отбора для эффективного поиска оптимальных решений в пространстве параметров нейронных сетей. Они позволяют найти глобальные оптимумы, но могут требовать больше вычислительных ресурсов и времени для сходимости.

Алгоритмы кластеризации (Clustering Algorithms): Эти алгоритмы используются для группировки данных в нейронных сетях. Например, алгоритм Кохонена и самоорганизующиеся карты (SOM) позволяют ИНС автоматически выявлять структуры и кластеры в данных без учителя. Они широко применяются в области анализа данных, распознавания образов и кластеризации.

**7. Какие алгоритмы используются для обучения ИНС, предназначенных для согласования ключевой информации между двумя сторонами?**

Для обучения искусственных нейронных сетей (ИНС), предназначенных для согласования ключевой информации между двумя сторонами, можно использовать различные алгоритмы обучения. Вот некоторые из них:

Обратное распространение ошибки (Backpropagation): Это наиболее распространенный и широко используемый алгоритм обучения ИНС. Он основан на градиентном спуске и позволяет настраивать веса связей нейронов для минимизации ошибки между предсказанными и желаемыми выходами сети. Обратное распространение ошибки может быть применено для обучения ИНС на согласование ключевой информации, где выходы сети должны быть согласованы с желаемыми значениями ключей.

Алгоритм Хопфилда (Hopfield): Этот алгоритм обучения применяется для обучения рекуррентных нейронных сетей, которые способны хранить и восстанавливать ассоциативные паттерны. Алгоритм Хопфилда может использоваться для обучения ИНС на согласование ключевой информации путем представления ключевых значений в виде ассоциативных паттернов, которые сеть будет восстанавливать при предъявлении входных данных.

Алгоритм самоорганизации карт Кохонена (Self-Organizing Maps, SOM): Этот алгоритм обучения используется для обучения нейронных сетей, которые способны выявлять структуры и кластеры в данных. Алгоритм SOM может быть применен для обучения ИНС на согласование ключевой информации, где сеть будет строить карту, отображающую ключевые значения и их схожесть, чтобы обнаружить несогласованности или расхождения.

Генетические алгоритмы (Genetic Algorithms): Эти алгоритмы основаны на принципах естественного отбора и эволюции. Они могут быть применены для обучения ИНС на согласование ключевой информации путем эффективного поиска оптимальных решений в пространстве параметров сети. Генетические алгоритмы могут использоваться для оптимизации весов нейронной сети и настройки ее параметров для достижения согласования ключевой информации.

**8. Могут ли легитимно участвовать в процессе синхронизации более трех сетей? Мотивируйте ответ.**

Да, легитимно участвовать в процессе синхронизации могут и более трех сетей. Однако, возможность и эффективность такой синхронизации будет зависеть от нескольких факторов, таких как:

Ресурсы: Синхронизация большего числа сетей может потребовать больших вычислительных и сетевых ресурсов. Необходимо убедиться, что доступные ресурсы достаточны для обработки и передачи данных между всеми сетями.

Сложность: С увеличением числа сетей возрастает сложность управления и согласования между ними. Необходимо разработать соответствующие алгоритмы и протоколы синхронизации, которые могут обеспечить эффективную коммуникацию и координацию между всеми участниками.

Цель и задачи: важно определить, какие конкретные цели и задачи требуют синхронизации более трех сетей. Если синхронизация требуется для выполнения сложных вычислительных задач или решения сложных проблем, то участие более трех сетей может быть оправданным.

Одним из примеров, где может потребоваться синхронизация более трех сетей, является распределенные вычисления. Например, в сети из нескольких серверов, каждый из которых обрабатывает свою часть задачи, синхронизация между сетями может быть важна для обмена промежуточными результатами и координации работы.

**9. Дать характеристику криптостойкости системы на основе двух взаимодействующих ИНС.**

Система на основе двух взаимодействующих искусственных нейронных сетей (ИНС) может обладать определенными характеристиками криптостойкости. Вот некоторые из них:

Ключевое пространство: Использование двух ИНС позволяет создать большое пространство возможных ключей. Ключевое пространство представляет собой набор всех возможных комбинаций параметров и весов сетей. Чем больше ключевое пространство, тем сложнее подобрать правильный ключ для расшифровки или проникновения в систему.

Нелинейность: Использование ИНС в системе обеспечивает нелинейность в процессе шифрования и дешифрования. Нелинейные функции активации и сложные взаимодействия между нейронами могут усложнить задачу анализа и восстановления ключевой информации.

Устойчивость к атакам: Взаимодействие между двумя ИНС может обеспечить устойчивость системы к различным атакам. Например, если одна сеть подвергается атаке, вторая сеть может продолжать работать и защищать ключевую информацию. Это усложняет задачу атакующего и повышает криптостойкость системы.

Обучение и адаптация: Система на основе двух ИНС может быть обучаемой и способной к адаптации. Это позволяет системе улучшать свою производительность и эффективность с течением времени, а также адаптироваться к изменяющимся условиям и новым угрозам.

Параллелизм и вычислительная мощность: Использование двух ИНС позволяет распараллеливать вычисления и использовать вычислительную мощность более эффективно. Это может быть особенно полезно при обработке больших объемов данных или выполнении сложных вычислительных операций.

**10. Какие виды атак на нейрокриптографические системы вам известны? В чем заключается их сущность?**

Нейрокриптография — это область, которая объединяет методы искусственных нейронных сетей и криптографии. В нейрокриптографических системах также могут возникать различные виды атак, которые могут направляться на нарушение безопасности и функциональности системы. Вот некоторые известные виды атак на нейрокриптографические системы:

Атаки на ключи:

Атака перебора: это тип атаки, при которой злоумышленник пытается перебрать все возможные ключи, чтобы найти правильный ключ и получить доступ к зашифрованным данным.

Атака посредника: В этом типе атаки злоумышленник пытается перехватить обмен ключами между двумя сторонами и подменить ключи своими собственными, чтобы получить доступ к защищенным данным.

Атака словарного перебора: Злоумышленник пытается перебрать все возможные комбинации ключевых фраз или паролей из заданного словаря, чтобы найти правильный ключ.

Атаки на данные:

Атака выбранного шифротекста: Злоумышленник имеет доступ к зашифрованным данным и может выбирать произвольные тексты для расшифровки. Целью атаки является выявление закономерностей или слабостей в системе шифрования.

Атака на перенос: Этот тип атаки основан на изменении или повреждении передаваемых данных между нейрокриптографическими системами. Целью атаки является нарушение целостности или аутентичности данных.

Атаки на саму нейрокриптографическую систему:

Атака на обучение: В этом типе атаки злоумышленник пытается внести изменения в процесс обучения нейронной сети, чтобы ослабить безопасность системы или изменить ее поведение.

Атака на модель: Злоумышленник пытается анализировать модель нейронной сети и получить информацию о ключах или других конфиденциальных данных, используемых в системе.

Атака на архитектуру: Злоумышленник пытается нарушить работу нейрокриптографической системы путем эксплуатации уязвимостей или слабостей в ее архитектуре.

Атака на физическую реализацию: это тип атаки, когда злоумышленник пытается получить доступ к физическим компонентам или устройствам, используемым в нейрокриптографической системе, для получения конфиденциальных данных.

Цель этих атак может быть различной, включая получение доступа к конфиденциальной информации, подрыв безопасности системы или нарушение ее функциональности. Для защиты от таких атак важно разработать надежные нейрокриптографические алгоритмы, протоколы и меры безопасности, а также проводить тщательное тестирование и анализ уязвимостей системы.