Modeling of Artificial Intelligence

Has been issued since 2014.
E-ISSN 2413-7200
2019. 6(1). Issued once a year

Journal is indexed by: **CrossRef (USA)**, **EBSCOhost Electronic Jornals Service (USA)**, **Journal Index (USA)**, **Open Academic Journals Index (USA)**, **Sherpa Romeo (Spain).**

All manuscripts are peer reviewed by experts in the respective field. Authors of the manuscripts bear responsibility for their content, credibility and reliability.

Editorial board doesn't expect the manuscripts' authors to always agree with its opinion.

Postal Address: 1367/4, Stara Vajnorska str., Bratislava – Nove Mesto, Slovak Republic, 831 04

Website: http://ejournal11.com/en/index.html
E-mail: aphr.sro@gmail.com

Founder and Editor: Academic Publishing House Researcher s.r.o.

Release date 15.12.19.
Format 21 × 29,7/4.

Headset Georgia.

Order № 115.

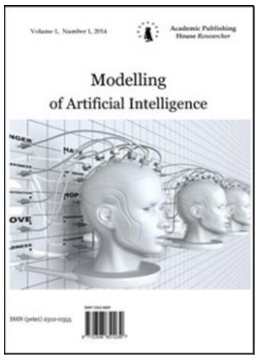
Modeling of Artificial Intelligence

2019

Is 1

C O N T E N T S

Articles



Published in the Slovak Republic
Modeling of Artificial Intelligence
Has been issued since 2014.
E-ISSN: 2413-7200
2019, 6(1): 3-12

DOI: 10.13187/mai.2019.1.3
www.ejournal11.com

Articles

Method of Building a Goal Tree in a System-Conceptual Approach to Information Security

Georgi A. Popov [a, *], Simon Zh. Simavoryan [b], Arsen R. Simonyan [b], Elena I. Ulitina [b]

[a] Astrakhan State Technical University, Russian Federation
[b] Sochi State University, Russian Federation

Abstract

The task of improving the quality of results in the design, construction and improvement of complex structures has always been one of the key positions in the process of creation and operation of systems of various purposes. Especially those characterized by a large structural structure, a significant territorial distribution and a complex technological structure. Research based on both a system-conceptual approach and system analysis is widely used to ensuring information security (EIS) challenges. However, the lack of comparative analysis of the advantages of using these methods in solving the various problems of the OIB requires its current and timely solution, which is the subject of research.

The methodology of the study is based on a system-conceptual approach and system analysis using modeling, generalization, comparison, analysis, synthesis and algorithms. A procedure has been developed to converge initial poorly formalized and poorly structured tasks in the field of EIS to a set of separate well-structured tasks based on the method of building a goal tree according to the method of V.N. Sagatovsky.

The task of developing a method (procedure) of building a goal tree within the framework of a system-conceptual approach has been set and solved. A new procedure for building the target tree of interest has been proposed, which includes five steps to detail the original goal of the EIS domain, namely: 1) the global goal (or goals); 2) end results; 3) components of the EIS system; 4) control cycle (functions); 5) work plans and schedules. For the first time, a comparative analysis of the possibilities of using systems analysis methods and a system-conceptual approach in EIS systems was carried out. It has been shown that a system-conceptual approach is generally preferable when there is a large set of constraints combined by existing technology of operation of the EIS system.

Keywords: information security, system approach, system analysis, goal tree, V.N. Sagatovsky method.

[*] Corresponding author
E-mail addresses: popov@astu.org (G.A. Popov), simsim58@mail.ru (S.Zh. Simavoryan), oppm@mail.ru (A.R. Simonyan), elenaulitina@mail.ru (E.I. Ulitina)

1. Введение

В настоящее время, актуальность указанной задачи значимо возросла по целому ряду причин и факторов, среди которых выделим следующие:

- непрерывно возрастающая рыночная конкуренция на всех уровнях, как на межкорпоративном, так и межгосударственном, подтолкнула многие фирмы (компании, организации, предприятия) искать новые методы повышения эффективности функционирования фирмы как системы, в том числе и системы ОИБ;
- повышение эффективности функционирования различных систем часто связано с ростом их сложности и, как следствие, необходимости использования более мощных и более наукоемких средств и методов проектирования и совершенствования структуры и технологии функционирования систем;
- массовое использование информационных технологий (ИТ) во всех сферах деятельности человека, связанное с цифровизацией экономики страны, привело к увеличению разнообразия различных типов информационных систем (ИС), их уникальности. Учет специфических особенностей (показателей) конкретных систем стал еще более актуален и востребован. Одним из существенных показателей качества сложных структур является показатель безопасности, обрабатываемой и хранимой в них информации.

Однако, широко распространенный на практике эмпирический подход к процессам построения и модернизации ИС, опирающийся на опыт компаний и организаций, занимающихся задачами создания и сопровождения информационных и автоматизированных систем, а также на опыт отдельных специалистов в этой сфере, со временем уже часто не давал желаемых результатов ввиду большой сложности искомой системы и жестких требований к результату ее создания и совершенствования. Поэтому требовались новые подходы к этим процессам. В последние три десятилетия в результате накопления большого научно-практического опыта, связанного с использованием разных способов и методов к решению указанной задачи, сформировались ряд конкретных подходов по проектированию и совершенствованию ИС, и современных систем ОИБ (Исаев, 2015). Среди указанных подходов выделим два наиболее значимых и известных в сфере ИТ, в частности, в сфере ОИБ: системно-концептуальный подход (СКП) (Герасименко, 1994; Симаворян и др., 2013; Герасименко, 1989) и системный анализ (Волкова, Денисов., 2014; Антонов, 2004; Попова, 2007).

В предлагаемой работе проводится сравнительный анализ возможностей этих подходов, а также анализируются их достоинства и недостатки. Применительно к СКП рассматривается процедура построения дерева задач, сводящая некоторые исходные слабо формализованные задачи, к ранжированной совокупности структурированных и часто формализованных задач.

2. Обсуждение

А) Сравнение системно-концептуального подхода с системным анализом

Исходным посылом является то, что некоторые задачи, решаемые на основе системно-концептуального подхода, могут быть решены и на основе методов системного анализа. Естественно встаёт важный принципиальный вопрос, какой из подходов и в каких случаях более эффективен и даёт более хорошие результаты. Прежде всего, отметим: основное отличие указанных двух подходов заключается в том, СКП опирается на определённую предписанную полную и непротиворечивую концепцию, в рамках которой и должна решаться поставленная задача. Подобная постановка задач особенно типична при проектировании и совершенствовании систем различного назначения. В качестве примера опишем типовые постановки в задачах ОИБ. Например, появление новых нормативно-правовых документов в сфере информационной безопасности, развитие механизмов и методов злоумышленного проникновения в защищенные системы и связанное с этим совершенствование средств противодействия угрозам порождают необходимость перманентного совершенствования систем ОИБ. Однако, процесс совершенствования отталкивается от уже существующей, функционирующей системы защиты и не предполагает изменения ее общей структуры и технологии функционирования. Все изменения в системе

должны быть произведены в рамках существующей общей структуры системы ОИБ, то есть в рамках существующей общей концепции ее функционирования.

Другой пример. Задача разработки новых методов и средств защиты информации является весьма актуальной, поскольку развитие и внедрение ИТ проходят параллельно с совершенствованием систем защиты информации, в частности, систем обнаружения атак (вторжений) (Simavoryan et al., 2016). При этом особое внимание следует обратить на разработку интеллектуальных методов защиты информации, например, искусственных нейронных сетей и механизмов искусственных иммунных систем, которые также можно отнести к сложным структурам (Васильев, 2013; Самарин, Симаворян и др. 2017а; Samarin et al., 2017). Однако процесс модификации и совершенствования внедрения таких механизмов должен проводиться в рамках общих установленных принципов и механизмов функционирования существующей системы защиты информации. В настоящее время это направление является приоритетным и требует разработки с точки зрения предлагаемой в данной работе процедуры формирования искомого дерева задач.

Рассмотрим теперь, как и насколько существующие подходы к совершенствованию систем способны учитывать существующие реалии функционирования систем. Отметим, что во многих случаях исходная концепция по существу описывает рассматриваемую реальную систему в разрезе.

В методах системного анализа указанная концепция перерабатывается и представляется в виде набора ограничений, которые учитываются в процессе решения задачи. Но сам процесс переформулирования концепции решения задачи в общем случае не обеспечивает, вообще говоря, полной идентичности полученного набора ограничений с описанием имеющейся концепции решения задачи. То есть часть исходной информации, связанной с концепцией, теряется. Кроме того, концепция даёт общее представление о самой задаче и поэтому полезна при сравнении различных методов и процедур ее решения; в то время как при системном анализе вместо концепции имеется набор отдельных слабо связанных условий и ограничений, не позволяющих обычно целиком охватить задачу.

Таким образом, при наличии предписанной концепции решения задачи, СКП принципиально более предпочтителен по сравнению с подходом на основе системного анализа, поскольку позволяет осуществлять поиск решения без отрыва от общей концепции задачи. В случае же, если как таковой концепции решения задачи нет, а имеется лишь набор отдельных ограничений и условий (в частности, при проектировании новой системы), методы системного анализа часто оказываются более эффективными. Следует отметить также, что в настоящее время в системном анализе имеется большое количество конкретных методов, процедур и алгоритмов, то есть инструментарий решения, позволяющий эффективно, в режиме реального времени решать поставленные задачи, что не скажешь о методах СКП – в СКП крайне мало конкретных методов решения задач, учитывающих специфические его особенности. Это обстоятельство существенно повышает привлекательность методов системного анализа по сравнению с СКП. Поэтому актуальной является задача развития инструментария решения задач на основе СКП.

Ниже предлагается процедура сведения в рамках СКП исходной задачи, которая часто слабо формализована и слабо структурирована, к совокупности отдельных хорошо структурированных задач на основе метода построения дерева целей. Данный метод в системном анализе является одним из ключевых. Целесообразно в СКП иметь метод, который также позволял свести исходную неструктурированную цель (задачу) к некоторой совокупности структурированных (даже формализованных) задач. Данная задача и рассматривается в следующем разделе.

Б) Построение дерева с целей в рамках системно-концептуального подхода

Для разбиения исходной цели (задачи) на совокупность более простых задач ниже предлагается использовать процедуры, связанные с построением дерева целей. Одной из наиболее эффективных процедур подобного типа в системном анализе является метод В.Н. Сагатовского (Попов, Попова, 2009). Суть метода кратко состоит в следующем. Выделяются семь уровней детализации сущности (объекта, цели, задачи), по которым последовательно проводится детализация каждой из задач предыдущего уровня. Уровни детализации применительно к сфере ОИБ могут иметь следующее содержание.

1) *Уровень 1. Формирование глобальной цели системы*. Цель должна быть ориентирована на конечный продукт, для получения которого существует или создается система; в рассматриваемом случае она ориентирована на качественные и количественные показатели информационной безопасности; например, на показатели безопасности выходной информации.

На уровнях 2–4 происходит уточнение цели по причинно-следственным, пространственным и временным связям системы. Порядок расположения этих уровней, в зависимости от специфики системы, может быть изменен.

2) *Уровень 2. Декомпозиция по признаку «виды конечного продукта»*. Под конечным продуктом понимается все, что выдается системой для внешнего потребления: оперативная, стратегическая, справочная и статистическая информации; варианты управленческих решений по ОИБ; показатели безопасности указанных видов информации.

3) *Уровень 3. Декомпозиция по признаку «пространство инициирования целей»*. Происходит детализация подцелей в зависимости от требований, предъявляемых всеми участниками процесса функционирования системы: вышестоящей инстанцией, которой подчиняется система; нижестоящими подразделениями, имеющие определенные ограничения по реализации стоящих перед ними задач; окружающей средой (социальной и природной), накладывающей определенные ограничения на процесс функционирования системы; непосредственно системой и ее составляющими, возможности и намерения которых также необходимо учитывать. Таким образом, все системы и объекты, с которыми взаимодействует рассматриваемая система, делятся на четыре класса:

а) *надсистема* (или вышестоящая система), которая формирует базовые требования к конечному продукту. Применительно к системе ОИБ в качестве надсистемы выступают система управления объектом обработки информации, международные и отечественные стандарты, законодательные и нормативные акты, имеющие отношение к сфере обработки информации и ее безопасности, регламентированные Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Федеральной службой безопасности Российской Федерации (ФСБ России), Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

б) *нижестоящие* (или подчиненные, подведомственные) *системы*, которые определяют ограничения на конечный продукт и процесс его создания. Большинство ИС не имеют нижестоящих подсистем, и поэтому уточнение целей по данному признаку не производится. Тем не менее, применительно к системе ОИБ в качестве нижестоящих систем могут выступать ИС филиалов и удаленных подразделений объекта обработки информации, подсистемы сбора и подготовки исходных данных для систем реального времени (например, метеорологических, экологических, сейсмологических характеристик; датчиков и аппаратуры, установленных непосредственно на технологических объектах предприятия и др.).

в) *актуальная среда*, то есть окружение и те системы и объекты внешней среды, которые непосредственно не являются частью рассматриваемой системы, но которые могут оказать влияние на процесс реализации целей системы. Обычно окружающую среду подразделяют на три составляющие: дружественную, конкурентную и безразличную, которая в будущем может стать либо дружественной, либо конкурентной. Применительно к системе ОИБ в качестве составляющих актуальной среды выступают решения регионального правительства, региональной комиссии по информационной безопасности, региональные и муниципальные структуры власти, компании, производящие и распространяющие программно-аппаратные средства, и технологии, а также средства безопасности, другие организации и учреждения, интересы которых пересекаются с интересами данной системы и объекта обработки информации в сфере информационной безопасности. Дружественная среда включает внешних партнеров и пользователей ИС, обрабатывающих закрытую информацию, поставщиков товаров, услуг и исходной информации. Конкурентная среда включает всех тех юридических и физических субъектов, которые конкурируют с ИС и системой ОИБ на рынке услуг. Безразличная среда включает всех тех субъектов на рынке информационных услуг и услуг по безопасности информации, которые в данный момент занимаются задачами, не представляющими интерес для ИС в настоящий момент, но которые потенциально могут заняться решением задач, решаемых в ИС в настоящее время, либо ИС может со временем заняться решением тех задач, которыми занимаются эти субъекты.

г) *собственно система*, то есть непосредственно рассматриваема система со своими целями и интересами. Применительно к системе ОИБ – это, прежде всего, интересы руководства, персонала ИС и системы ОИБ, а также пользователей ИС.

4) *Уровень 4. Декомпозиция по признаку «жизненный цикл»*. Применительно к системе ОИБ выделяют обычно следующие этапы жизненного цикла: предпроектный анализ, проектирование и разработка, создание, внедрение и адаптация, опытная эксплуатация, постоянная эксплуатация, совершенствование и модернизация, ликвидация и уничтожение.

На рассмотренных четырех уровнях процесс декомпозиции происходит только исходя из общего содержания поставленных целей и общего характера рассматриваемой системы, не затрагивая ее внутренних особенностей. Начиная с уровня 5, процесс декомпозиции осуществляется по внутренним параметрам с учетом особенностей непосредственно системы. Поэтому на уровне 5 подцели перерастают в целевые функции, учитывающие особенности типа рассматриваемой системы.

5) *Уровень 5. Декомпозиция по структуре системы.* Декомпозиция осуществляется по основным элементам системы, которые могут быть сгруппированы в следующие группы: кадры, средства деятельности, предмет деятельности. Применительно к системе ОИБ: кадры – это руководство, служба защиты информации, персонал, пользователи; средства деятельности – это основные фонды и программно-аппаратные средства, входящие в состав ИС и системы ОИБ, предметом деятельности является закрытая информация, обрабатываемая в ИС.

6) *Уровень 6. Декомпозиция по технологии функционирования системы.* Поскольку в эффективно организованной системе процесс функционирования системы сформирован в форме взаимосвязанной совокупности функций управления, то декомпозиция на данном уровне равносильна декомпозиции по функциям управленческого цикла.

7) *Уровень 7. Декомпозиция по ограничениям*. На данном уровне сформированная выше совокупность целевых функций декомпозируется с учетом возможностей и ограничений, а также условий функционирования конкретной системы, то есть целевые функции адаптируются к особенностям данной системы. Применительно к системе ОИБ – это здания и помещения с учетом их физических параметров, конкретные виды программно-аппаратных средств с учетом их статуса (в частности, отсутствия/наличия сертификатов), срока использования, состава и квалификации пользователей и персонала ИС и системы ОИБ, принятых схем и технологий обработки информации и др. На данном уровне целевые функции перерастают в макрозадачи, где под макрозадачей понимается целевая функция, уточненная по возможным способам действия: по задействованным или используемым ресурсам, средствам, проводимым мероприятиям и т.д.

Как следует из приведенного описания метода, учесть структуру и основные положения концепции построения системы в рамках данного метода крайне затруднительно. Единственная возможность, как отмечалось выше, переформулировать основные элементы и положения концепции в виде требований и ограничений самой системы, которые необходимо учесть в процессе построения дерева целей.

Таким образом, непосредственный учёт особенностей концепции построения системы в рамках метода В.Н. Сагатовского крайне затруднителен. Кроме того, не все из приводимых в методе В.Н. Сагатовского параметров актуальны для систем ОИБ, их приоритетность отличается от их приоритетности в методе В.Н. Сагатовского для открытых систем. В частности, параметр «актуальная среда», существенно менее важен по сравнению с параметром «состав системы», поскольку существенная часть параметров актуальной среды уже учтены в рамках концепции системы. Далее, менее значим параметр «конечная цель», поскольку этот параметр чаще всего имеет типовую форму, и в системах ОИБ обычно заключается в повышении уровня ОИБ. Поэтому предлагается существенно изменить общую структуру и содержание метода В.Н. Сагатовского с учетом специфики задач в сфере ОИБ и особенностей СКП.

В рамках предлагаемого подхода выделяются четыре класса сущностей:

1. Компонент и элементы проектируемой системы, представленные в концепции.
2. Все приведенные в концепции связи между компонентами и элементами системы.

3. Технологии, которые предполагается реализовывать в рамках представленной концепции.

4. Общесистемные требования и ограничения к проектируемой (модернизируемой) системе.

Отметим, что степень детализации всех перечисленных выше элементов сущностей может быть самой разной: от описания на лингвистическом уровне до детального и полного описания всех элементов этих сущностей.

На предварительном этапе рассматриваемая концепция модернизации (построения) системы анализируется на предмет соответствия всем существующим законодательным и нормативно-правовым документам. В случае выявления несоответствия в концепцию вносятся соответствующие изменения и уточнения. Предполагается, что имеется некоторая база знаний, содержащая все существующие требования к системам ОИБ, которая постоянно обновляется и пополняется в режиме реального времени.

Общая структура предлагаемой процедуры совершенствования системы ОИБ приведена на Рисунке 1. В рамках предлагаемого подхода весь процесс реализации процедуры построения дерева задач по совершенствованию (проектированию) системы ОИБ на основе СКП проводится параллельно применительно к каждому из выделенных четырех классов.

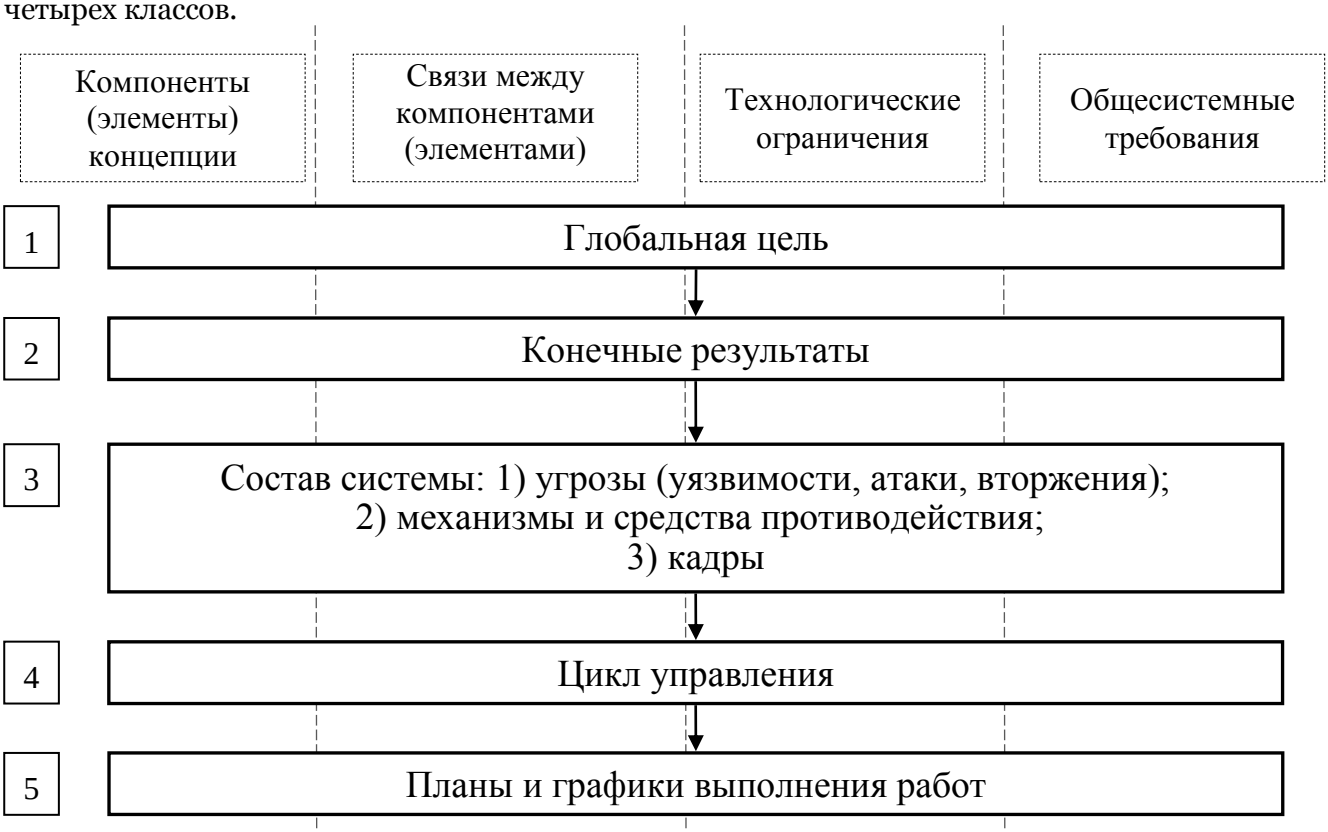


Рис. 1. Общее описание процедуры построения дерева задач при системно-концептуальном подходе

На первом этапе, по аналогии с методом В.Н. Сагатовского (Попов, Попова, 2009), формируется глобальная цель (или цели) совершенствования системы. На практике в большинстве случаев указанная глобальная цель одна, и связана она с совершенствованием системы ОИБ с учетом некоторых дополнительных требований. Далее, данная цель может быть привязана к конкретному направлению ОИБ; например, к созданию подсистемы обнаружения атак (вторжений) (Simavoryan et al., 2016). Однако, возможны ситуации, когда целей может быть несколько. Например, применительно к деятельности службы защиты информации, могут быть актуальны следующие цели:

1. Совершенствование процесса обучения и подготовки специалистов по защите информации, с учетом новых законодательных и нормативных требований.

2. Повышение эффективности проведения работ по анализу собственной безопасности службы защиты информации.

На втором этапе процедуры, исходя из поставленных целей, формируется перечень конечных результатов, которые должны быть достигнуты по завершению процесса совершенствования системы. Как отмечалось выше, в подавляющем большинстве случаев глобальные цели носят типовой характер, и их можно будет свести к ранжированному конечному набору типовых вариантов. Поэтому и конечные результаты по своим видам могут быть отнесены к одному из нескольких типовых вариантов.

Наиболее типичный вид конечного результата – обеспечить заданные значения ряда показателей информационной безопасности. В качестве типовых целей можно выбрать следующие: 1) совершенствование системы ОИБ в соответствии с определенными законодательными или нормативными требованиями, 2) разработка процедуры рабочего взаимодействия двух специалистов, работающих по близким темам и т.д. Одним из конечных результатов, является методика с описанием требований, процедур и ограничений по реализации поставленной цели.

Анализ первых двух этапов процедуры, приведенной на рис.1, показал, что для указанных двух этапов применительно к сфере ОИБ может сформирована база данных, где каждой сформулированной типовой цели сопоставляется перечень возможных конечных результатов. Наличие указанной базы данных позволяет упростить процесс реализации первых двух уровней, приведенных на Рисунке 1 процедуры, а именно, вместо того, чтобы на основе анализа объекта и цели выявлять возможные конечные результаты, достаточно лишь выбрать нужную цель из базы, просмотреть соответствующие ей конечные результаты, отбросить лишние, а оставшиеся типы конечных результатов привязать к искомому объекту защиты. Авторы предполагают в дальнейшем реализовать данный проект.

На третьем этапе процедуры необходимо «привязать» каждый из выбранных конечных результатов к конкретных особенностям, возможностям искомого объекта защиты, а также к ограничениям, связанным с этим объектом. Наиболее важные ограничения связаны с составом возможных угроз информационной безопасности с перечислением параметров, связанных с этими угрозами, а также с составом имеющихся в распоряжении системы ОИБ средств защиты. При этом также необходимо учесть степень подготовленности персонала службы защиты информации, его готовности эффективно выполнять возложенные на него функции. Могут также быть учтены и ограничения других типов, например, особенности системы обработки данных, окружения и среды функционирования объекта защиты. Отличительная особенность данного этапа от предыдущего: на третьем этапе описательные формулировки, характерные для целей (первый уровень) и конечных результатов (второй уровень) переходят в утвердительные формулировки в виде перечня задач обычно общего содержания. Конкретизация задач с учетом возможностей и особенностей управления в процессе ОИБ осуществляется на последующих двух уровнях. Таким образом, конечным результатом третьего уровня является набор задач, решение которых обеспечивает достижение поставленных целей.

Четвертый этап предназначен для «привязки» сформированного множества задач к конкретной технологии функционирования системы ОИБ, к основным макропроцессам управления защитой информации. Из теории управления процессами функционирования систем защиты информации известно, что основными макропроцессами управления в системах организационно-технологического типа являются: планирование, оперативно-диспетчерское управление, календарно-плановое руководство и обеспечение повседневной деятельности службы защиты информации (Герасименко, 1994; Симаворян и др., 2013; Герасименко, 1989). Поскольку на уровне процесса управления технология функционирования структурируется путем разбиения всех технологических процессов на отдельные, относительно однородные группы и сопоставлению каждой группе своей функции управления, то на четвертом уровне осуществляется детализация каждой из сформированных на предыдущем уровне задач применительно к конкретной функции управления (Попов, Попова, 2018; Герасименко, 1989). Заметим, что все макропроцессы управления реализуются

в строго определенной последовательности и замыкаются в два пересекающихся цикла управления: цикл стратегического управления и цикл оперативного управления.

На пятом этапе для каждой из полученных на предыдущем этапе задач решаются все необходимые организационные вопросы по ее реализации, в частности, представляется график выполнения работ по последовательному решению конкретной задачи, выделяются требуемые ресурсы, назначаются исполнители и ответственные лица, фиксируется процедура контроля процесса выполнения работ и порядок принятия результатов.

В результате реализации описанной выше процедуры будет сформировано иерархическое дерево, состоящее из пяти уровней, на верхнем уровне расположены вершины, отображающие все глобальные цели (каждой цели сопоставляется одна вершина). Аналогично отображаются все перечни конечных результатов, задач и графики выполнения работ. Таким образом, поставленная в работе задача формирования процедуры построения дерева целей (задач) при системно-концептуальном подходе применительно к сфере ОИБ достигнута.

3. Результаты

Разработана новая процедура для построения искомого дерева решений задач, включающая пять этапов детализации исходной цели. Впервые проведен сравнительный анализ возможностей использования в системах ОИБ методов системного анализа и системно-концептуального подхода. Сделан вывод, что при наличии большого набора средств ограничений, объединенных существующей технологией функционирования системы ОИБ, системно-концептуальный подход в целом предпочтительнее.

4. Заключение

В работе поставлена и решена задача формирования процедуры построения дерева целей (задач) в рамках системно-концептуального подхода. Предложена новая процедура для формирования искомого дерева целей. Методология исследования основана на системно-концептуальном подходе и системном анализе с применением методов моделирования, обобщения, сравнения, анализа, синтеза и алгоритмизации. Полученный результат определяет приоритетное направление по дальнейшей разработке теоретических и практических основ построения интеллектуальных систем защиты информации на основе искусственных интеллектуальных систем обнаружения атак на базе системно-концептуального подхода.

5. Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-01-00383.

Литература

Антонов, 2004 – *Антонов А.В.* Системный анализ. М.: Высшая школа, 2004. 454 с.

Васильев, 2013 – *Васильев В.И.* Интеллектуальные системы защиты информации: учебное пособие. М.: Машиностроение, 2013. 172 с.

Волкова, Денисов, 2014 – *Волкова В.Н., Денисов А.А.* Теория систем и системный анализ. СПб, Изд-во Санкт-Петерб. политехн. Ун-та, 2014. 616 с.

Герасименко, 1989 – *Герасименко В.А.* Информатика, информатизация и индустриализация управления. М.: 1989. Деп. ВИНИТИ 18.12.89, № 7753-В89.

Герасименко, 1994 – *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. М.: Энергоатомиздат, кн. 1 и 2, 1994.

Исаев, 2015 – *Исаев Г.Н.* Проектирование информационных систем. Учебное пособие. Изд-во Омега-Л, 2015. 424с.

Попов, Попова, 2009 – *Попов Г.А., Попова Е.А.* Классификация функций и задач вуза на основе метода Сагатовского // *Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ.,* 2009, №1, С. 7-17.

Попов, Попова, 2018 – *Попов Г.А., Попова Е.А.* Системный подход к формированию состава функций управления в системах защиты информации // *Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ.,* 2018. №1, С. 71-80.

Попова, 2007 – *Попова Е.А.* О процедуре проведения системного анализа задач в сфере информационной безопасности // *Вестник Астраханского государственного технического университета*. 2007. № 4 (39). С. 228-230.

Самарин и др., 2017 – *Самарин В.И., Симаворян С.Ж., Симонян А.Р., Улитина Е.И.* Перспективы нейронных сетей как интеллектуальных средств защиты информации // American Scientific Journal. 2017. № 16. С. 19-25.

Симаворян и др., 2013 – *Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян Р.А.* Системный подход к проектированию интеллектуальных систем защиты информации // *Известия Сочинского государственного университета*. 2013. № 4-2 (28). С. 128-132.

Samarin et al., 2017 – *Samarin V.I., Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* Information security in neural-networked queuing systems // *Russian Journal of Mathematical Research. Series A*. 2017. № 3-2. Pp. 49-61. 2017. № 3-2. Pp. 49-61.

Simavoryan et al., 2016 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Simonyan R.A.* Creating the conditions for the theoretical and practical solution of the problem of automated intelligent search for the attacker's image in ADPS // *Modeling of Artificial Intelligence*. 2016. № 3 (11). Pp. 166-176.

References

Antonov, 2004 – *Antonov, A.V.* (2004). Sistemnyi analiz [System analysis]. M.: Vysshaya shkola, 454 p. [in Russian]

Gerasimenko, 1989 – *Gerasimenko, V.A.* (1989). Informatika, informatizatsiya i industrializatsiya upravleniya [Informatics, informatization and industrialization of management]. M. Dep. VINITI 18.12.89, № 7753-V89. [in Russian]

Gerasimenko, 1994 – *Gerasimenko, V.A.* (1994). Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh [Information security in automated data processing systems]. M.: Energoatomizdat, kn. 1 i 2. [in Russian]

Isaev, 2015 – *Isaev, G.N.* (2015). Proektirovanie informatsionnykh system [Design of information systems]. Uchebnoe posobie. Izd-vo Omega-L. 424 p. [in Russian]

Popov, Popova, 2009 – *Popov, G.A., Popova, E.A.* (2009). Klassifikatsiya funktsii i zadach vuza na osnove metoda Sagatovskogo [A systematic approach to the formation of the composition of management functions in information protection systems]. *Vestn. Astrakhan. gos. tekhn. un-ta. Ser. upravlenie, vychisl. tekhn. inform*. №1. Pp. 7-17. [in Russian]

Popov, Popova, 2018 – *Popov, G.A., Popova, E.A.* (2018). Sistemnyi podkhod k formirovaniyu sostava funktsii upravleniya v sistemakh zashchity informatsii [A systematic approach to the formation of the composition of management functions in information protection systems]. *Vestn. Astrakhan. gos. tekhn. un-ta. Ser. upravlenie, vychisl. tekhn. inform.* №1. Pp. 71-80. [in Russian]

Popova, 2007 – *Popova, E.A.* (2007). O protsedure provedeniya sistemnogo analiza zadach v sfere informatsionnoi bezopasnosti [On the procedure for conducting a systematic analysis of tasks in the field of information security]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta*. № 4 (39). Pp. 228-230. [in Russian]

Samarin et al., 2017 – *Samarin V.I., Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* (2017). Information security in neural-networked queuing systems. *Russian Journal of Mathematical Research. Series A*. № 3-2. Pp. 49-61. 2017. № 3-2. Pp. 49-61.

Samarin i dr., 2017 – *Samarin, V.I., Simavoryan, S.Zh., Simonyan, A.R., Ulitina, E.I.* (2017). Perspektivy neironnykh setei kak intellektual'nykh sredstv zashchity informatsii [Prospects for neural networks as intelligent information security tools]. *American Scientific Journal*. № 16. Pp. 19-25. [in Russian]

Simavoryan et al., 2016 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Simonyan R.A.* (2016). Creating the conditions for the theoretical and practical solution of the problem of automated intelligent search for the attacker's image in ADPS. *Modeling of Artificial Intelligence*. № 3 (11). Pp. 166-176.

Simavoryan i dr., 2013 – *Simavoryan, S.Zh., Simonyan, A.R., Ulitina, E.I., Simonyan, R.A.* (2013). Sistemnyi podkhod k proektirovaniyu intellektual'nykh sistem zashchity informatsii [A systematic approach to the design of intelligent information protection systems]. *Izvestiya Sochinskogo gosudarstvennogo universiteta*. № 4-2 (28). Pp. 128-132. [in Russian]

Vasil'ev, 2013 – *Vasil'ev, V.I.* (2013). Intellektual'nye sistemy zashchity informatsii: uchebnoe posobie [ntelligent information security systems: a training manual]. M.: Mashinostroenie, 172 p. [in Russian]

Volkova, Denisov, 2014 – *Volkova, V.N., Denisov, A.A.* (2014). Teoriya sistem i sistemnyi analiz [Theory of systems and systems analysis]. SPb, Izd-vo Sankt-Peterb. politekhn. Un-ta, 616 p. [in Russian]

Метод построения дерева целей в системно-концептуальном подходе обеспечения информационной безопасности

Георгий Александрович Попов [a, *], Симон Жоржевич Симаворян [b],
Арсен Рафикович Симонян [b], Елена Ивановна Улитина [b]

[a] Астраханский государственный технический университет, Российская Федерация
[b] Сочинский государственный университет, Российская Федерация

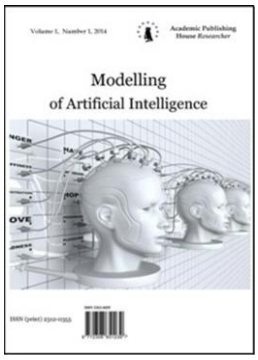
Аннотация. Задача повышения качества результатов при проектировании, построении и совершенствовании сложных структур всегда занимала одну из ключевых позиций в процессе создания и эксплуатации систем различного назначения. Особенно таких, которые отличаются большим структурным построением, значительным территориальным распределением и сложной технологической структурой. Для решения задач обеспечения информационной безопасности (ОИБ) широко используются исследования, основанные как на системно-концептуальном подходе, так и на системном анализе. Однако, отсутствие сравнительного анализа преимуществ использования этих методов при решении различных задач ОИБ требует её актуального и своевременного решения, что и является предметом исследования.

Методология исследования основана на системно-концептуальном подходе и системном анализе с применением методов моделирования, обобщения, сравнения, анализа, синтеза и алгоритмизации. Разработана процедура сведения исходных слабо формализованных и слабо структурированных задач в области ОИБ к совокупности отдельных хорошо структурированных задач на основе метода построения дерева целей по методу В.Н. Сагатовского.

В работе поставлена и решена задача разработки метода (процедуры) построения дерева целей в рамках системно-концептуального подхода. Предложена новая процедура для построения искомого дерева целей, включающая пять этапов детализации исходной цели, относящейся к сфере ОИБ, а именно: 1) глобальная цель (или цели); 2) конечные результаты; 3) компоненты системы ОИБ; 4) цикл (функции) управления; 5) планы и графики выполнения работ. В работе впервые проведен сравнительный анализ возможностей использования в системах ОИБ методов системного анализа и системно-концептуального подхода. Показано, что при наличии большого набора средств ограничений, объединенных существующей технологией функционирования системы ОИБ, системно-концептуальный подход в целом предпочтительнее.

Ключевые слова: информационная безопасность, системный подход, системный анализ, дерево целей, метод В.Н. Сагатовского.

* Корреспондирующий автор
Адреса электронной почты: popov@astu.org (Г.А. Попов), simsim58@mail.ru (С.Ж. Симаворян), oppm@mail.ru (А.Р. Симонян), elenaulitina@mail.ru (Е.И. Улитина)



Published in the Slovak Republic
Modeling of Artificial Intelligence
Has been issued since 2014.
E-ISSN: 2413-7200
2019, 6(1): 13-18

DOI: 10.13187/mai.2019.1.13
www.ejournal11.com

Machine Learning Algorithm for Detecting Outliers and Anomalies

Maxim Vasilenko [a, *], Andrey Kopyrin [a]

[a] Sochi State University, Russian Federation

Abstract

The detection of anomalies in the time series is an important topic in modern data science.

Existing solutions for detecting anomalies mainly look for deviations in parameter values. Consequently, their ability to detect anomalies and deviations in a priori unknown processes is limited, since it is difficult to determine their numerical characteristics. To solve this problem, the authors propose using machine learning technology to detect anomalies along with soft calculations based on fuzzy logic.

Modern artificial neural networks usually use a large number of neurons operating in parallel and arranged in layers, but due to the disappearing gradient problem, a large recurrent neural network will not be effectively trained.

It is proposed to use a network with Long Short-Term Memory (LSTM), since regular back propagation of an error is effective for teaching LSTM to store values for very long time intervals.

It is concluded that when analyzing time series, the LSTM network will efficiently process unstructured statistical information, which makes it suitable for use for big data analysis.

Keywords: anomaly search, neural networks, LSTM.

1. Введение

С быстрым развитием информационных технологий, вопрос анализа больших объемов экономических и технических данных также получает все больше и больше внимания. Исследования по обнаружению аномалий во временных рядах являются важной темой в современной науке об аналитике данных – data science.

Различные методологии обнаружения аномалий устанавливают расхождение модели в соответствии с реальным поведением объекта и проводят обнаружение выбросов на основе того, отличаются ли фактическое значение от моделируемого.

Однако с ростом объема анализируемых данных, а также несбалансированное распределение нормального и аномального поведения объекта, возникают проблемы низкой достоверности и скорости обнаружения выбросов.

Существующие решения обнаружения аномалий в основном ищут отклонения в значениях параметров, которые фиксируют свойства известных (или предполагаемых известными) процессов, а это означает, что они используют так называемые числовые признаки. Следовательно, их возможности по обнаружению аномалий и отклонений в априорно неизвестных процессов ограничены, так как трудно определить их числовые характеристики. Для решения данной проблемы, авторы предлагают использовать

* Corresponding author
E-mail addresses: renxi@yandex.ru (M. Vasilenko), kopyrin_a@mail.ru (A. Kopyrin)

технологию машинного обучения для обнаружения аномалий наряду с мягкими вычислениями на основе нечеткой логики.

В данной работе предложено обоснование выбора алгоритма обучения нейронной сети для выявления аномалий в темпоральных данных.

2. Обсуждение

Нейронные сети представляют собой набор алгоритмов, которые очень похожи на мозг человека и предназначены для распознавания паттернов. Они интерпретируют сенсорные данные через машинное восприятие, маркировку или кластеризацию необработанного ввода (Haykin, 1994). Они могут распознавать числовые шаблоны, содержащиеся в векторах, в которые должны быть переведены все реальные данные (изображения, звук, текст или временные ряды). Искусственные нейронные сети состоят из большого количества сильно взаимосвязанных элементов (нейронов), работающих вместе для решения поставленной задачи.

Согласно универсальной теореме аппроксимации (Горбань, 1998), простая нейронная сеть с n-нным количеством нейронов в 1 скрытом слое может аппроксимировать любую непрерывную функцию. Регулируя веса и смещения нейронов, сеть может принимать любые входные данные и аппроксимировать их, чтобы соответствовать примерно такому же поведению, что и у целевой функции. Обязательным условием является непрерывность целевой функции, если функция не является непрерывной, то нейронная сеть с одним скрытым слоем не сможет точно приблизиться к целевой функции, что, в прочем, может быть решено добавлением дополнительных слоев.

Современное машинное обучение акцентировано на использовании глубоких, многослойных сетей (в отличие от сетей с одним скрытым слоем). Основным преимуществом таких сетей является тот факт, что они могут эффективно выводить композиции функций. Это позволяет приближать сложные математические модели и выделять закономерности.

В современных искусственных нейронных сетях обычно используется большое количество нейронов, работающих параллельно и расположенных по слоям. Первый слой получает необработанную входную информацию – аналог зрительных нервов при визуальной обработке человеческим мозгом. Каждый последующий уровень получает выходные данные от предшествующего уровня, а не от необработанного ввода – таким же образом нейроны, находящиеся дальше от входа, получают сигналы от тех, кто ближе к нему. Последний уровень производит вывод системы.

Рекуррентная нейронная сеть (РНС) – это обобщение нейронной сети с прямой связью, имеющей внутреннюю память (Осипов, 2010; Haykin, 1994). Такая сеть является рекуррентной по своей природе, поскольку она выполняет одну и ту же функцию для каждого ввода данных, в то время как вывод текущего ввода зависит от предыдущих вычислений. После создания вывода он копируется и отправляется обратно в рекуррентную сеть. Для принятия решения она учитывает текущий ввод и вывод, который был получен из предыдущего ввода. В других типах нейронных сетей все входы независимы друг от друга, в РНС все входы связаны друг с другом. Этот факт, а также присутствие в нейронах кратковременной памяти позволяет производить контекстно-ориентированный анализ данных – в отличие от нейронных сетей с прямой связью, РНС могут использовать свою «память» для обработки последовательностей входных данных, таких как временные ряды, статистическая информация, с учетом их контекста.

Определим X как вектор входных данных, и H как вектор промежуточных результатов вычислений в рекуррентной сети. Таким образом: вначале сеть берет X(0) из последовательности ввода, а затем выводит H(0), которое вместе с X(1) является входом для следующей итерации. Итак, H(0) и X(1) – это вход для следующего шага. В этом случае передача H(n) подобна использованию т.н. «входа смещения» в прямонаправленных сетях (feedforward, персептроны). Отличие в том, что вход смещения подразумевает смещение на постоянную константу (обычно, 1 при диапазоне входных значений от 0 до 1). Аналогично, H(1) и X(2) являются входом для следующего шага и так далее. Таким образом, РНС учитывает контекст во время обучения.

Но применение рекуррентных нейронных сетей затруднено одной серьезной проблемой – проблемой исчезающего градиента (Созыкин, 2017).

Проблема исчезающего градиента состоит в том, что при добавлении в нейронные сети большого количества слоев, использующих определенные функции активации (обычно, сигмоид или гиперболический тангенс), градиенты функции потерь приближаются к нулю, что затрудняет обучение сети. Это происходит из-за того, что некоторые функции активации, такие как сигмоида, делят большое пространство входных значений на маленькое входное пространство между 0 и 1 или -1 и 1. Поэтому, большое изменение на входе, например, сигмоидной функции, вызовет небольшое изменение на выходе. Для небольших сетей с несколькими скрытыми слоями, которые используют такие функции активации, это не является проблемой, но в случае с крупными сетями производная функции в данной точке становится весьма небольшой, что снижает эффективность метода градиентного спуска при обучении сети.

Метод градиентного спуска заключается в нахождении градиентов нейронных сетей, обнаруживаемых с помощью метода обратного распространения (Федосин и др., 2010). Проще говоря, обратное распространение находит производные сети, перемещаясь слой за слоем от конечного слоя к начальному. Производные каждого уровня умножаются по сети, чтобы вычислить производные начальных слоев. Однако, когда n скрытых слоев используют функции активации, подобные сигмоидальной функции, n маленьких производных перемножаются вместе. Таким образом, градиент уменьшается по мере того, как обратное распространение доходит до начальных слоев.

Небольшой градиент означает, что веса и смещения начальных слоев не будут эффективно обновляться с каждой эпохой обучения. Поскольку эти начальные слои часто имеют решающее значение для распознавания основных элементов входных данных, это может привести к общей неточности всей сети.

Иными словами – большая РНС не будет эффективно обучаться.

Для решения этой проблемы были изобретены сети с долгой краткосрочной памятью (Long Short-Term Memory, LSTM), которые представляют собой модифицированную версию рекуррентной нейронной сети, которая облегчает запоминание прошлых данных в памяти (Hochreiter, Schmidhuber, 1997; Sainath, 2015). В таких сетях не стоит проблема исчезающего градиента. LSTM хорошо подходит для классификации, обработки и прогнозирования временных рядов с учетом временных задержек неизвестной длительности. Сети LSTM, как и обычные РНС, обучаются с использованием обратного распространения. В такой сети присутствуют три «шлюза»:

1. Шлюз утраты – определяет, какую информацию нужно отбросить из памяти нейрона. «Лишняя» информация определяется сигмоидной функцией, которая просматривает предыдущее состояние H(n-1) и текущий вход сети X(n) и выводит число от 0 до 1, на которое затем домножается H(n-1) перед сложением с числом в входном шлюзе.
2. Входной шлюз - определяет, какое значение из ввода следует использовать для изменения памяти нейрона. Сигмоидная функция работает как своего рода фильтр с порогом срабатывания на 0.1, определяя какие значения стоит запоминать, затем гиперболический тангенс определяет вес переданных значений, назначая им уровень важности в диапазоне от -1 до 1.
3. Выходной шлюз – вход и память блока используются для определения выхода. Сигмоидная функция определяет какие значения пропустить через порог срабатывания и tanh дает вес для значений, которые передаются, определяя их уровень важности в диапазоне от -1 до 1 и умножая на выход сигмоиды.

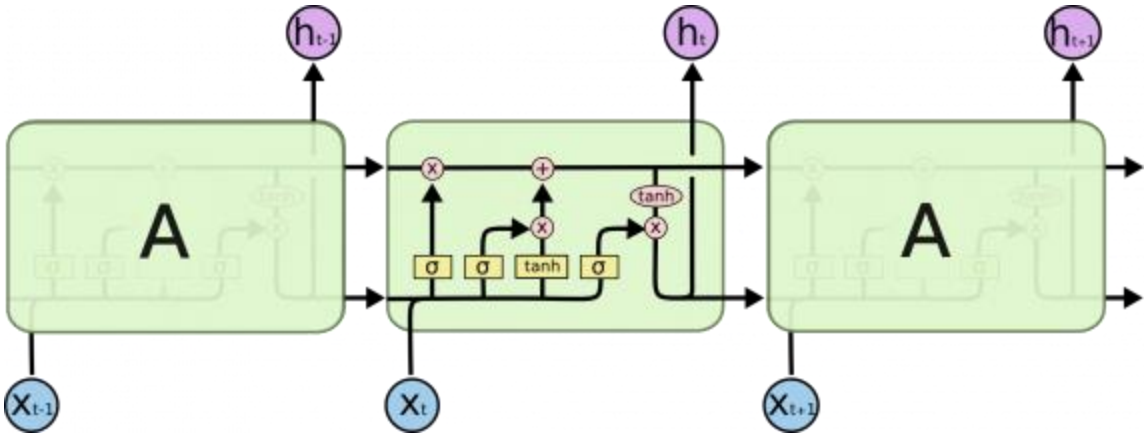


Рис. 1. Структура шлюзов нейрона в сети LSTM
Источник: Google Images

Фактически, механизм работы памяти такого нейрона можно описать по принципу «Забудь старое, если новое было лучше». Этот принцип устраняет проблемы при использовании метода градиентного спуска, поскольку, когда значение ошибки распространяется в направлении, противоположном выходному слою сети, ошибка блокируется в памяти нейрона, который непрерывно возвращает её обратно каждому шлюзу, пока они не обучатся отбрасывать значение.

Таким образом, регулярное обратное распространение ошибки эффективно для обучения LSTM запоминанию значений в течение очень длинных временных интервалов.

Так же возможно применение эволюционного/генетического алгоритма при обучении, в случае, когда обычный метод тренировки сети зашел в тупик.

Из вышесказанного следует, что при анализе временных рядов сеть LSTM будет эффективно обрабатывать неструктурированную статистическую информацию, что делает ее пригодной к использованию для анализа больших данных. Сети LSTM применялись в подобных задачах, например в труде Malhotra (Malhotra et al., 2015).

3. Результаты

Представлен краткий обзор применения нейронных сетей в рамках задач поиска аномалий. Сформулирован обобщенный алгоритм работы рекуррентных сетей, указана проблема исчезающего градиента. Обосновано использование в качестве алгоритма обучения нейронной сети по поиску аномалий сети Long Short-Term Memory.

4. Заключение

Данная работа посвящена рассмотрению алгоритмов обучения нейронных сетей, которые могут быть использованы для детектирования аномалий в потоках данных, а также обзору существующих методов и подходов к их поиску. Было проведено сравнение рекуррентной архитектуры и парадигмы обучения с LSTM-парадигмой, приведены краткие описания алгоритмов.

5. Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта No 19-01-00370.

Литература

Горбань, 1998 – *Горбань А.Н.* Обобщенная аппроксимационная теорема и вычислительные возможности нейронных сетей // *Сибирский журнал вычислительной математики*. 1998. Т. 1. № 1. С. 11-24.

Осипов, 2010 – *Осипов В.Ю.* Рекуррентная нейронная сеть с управляемыми синапсами // *Информационные технологии*. 2010. № 7. С. 43-47.

Созыкин, 2017 – *Созыкин А.В.* Обзор методов обучения глубоких нейронных сетей // *Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика*. 2017. Т. 6. № 3.

Федосин и др., 2010 – *Федосин С.А., Ладяев Д.А., Марьина О.А.* Анализ и сравнение методов обучения нейронных сетей // *Вестник Мордовского университета*. 2010. № 4.

Haykin, 1994 – *Haykin, S.* Neural networks: a comprehensive foundation. Prentice Hall PTRб 1994.

Hochreiter, Schmidhuber, 1997 – *Hochreiter S., Schmidhuber J.* Long short-term memory // *Neural computation*. 1997. Т. 9. №. 8. Pp. 1735-1780.

Malhotra et al., 2015 – *Malhotra P. et al.* Long short term memory networks for anomaly detection in time series / *Proceedings. Presses universitaires de Louvain*, 2015. P. 89.

Sainath, 2015 – *Sainath T.N. et al.* Convolutional, long short-term memory, fully connected deep neural networks / *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2015. Pp. 4580-4584.

References

Fedosin i dr., 2010 – *Fedosin, S.A., Ladyaev, D.A., Mar'ina, O.A.* (2010). Analiz i sravnenie metodov obucheniya neironnykh setei [Analysis and comparison of training methods for neural networks]. *Vestnik Mordovskogo universiteta*. № 4. [in Russian]

Gorban', 1998 – *Gorban', A.N.* (1998). Obobshchennaya approksimatsionnaya teorema i vychislitel'nye vozmozhnosti neironnykh setei [Generalized approximation theorem and computational capabilities of neural networks]. *Sibirskii zhurnal vychislitel'noi matematiki*. T. 1. № 1. Pp. 11-24. [in Russian]

Haykin, 1994 – *Haykin, S.* (1994). Neural networks: a comprehensive foundation. Prentice Hall PTR.

Hochreiter, Schmidhuber, 1997 – *Hochreiter, S., Schmidhuber, J.* (1997). Long short-term memory. *Neural computation*. T. 9. №. 8. Pp. 1735-1780.

Malhotra et al., 2015 – *Malhotra, P. et al.* (2015). Long short term memory networks for anomaly detection in time series. *Proceedings. Presses universitaires de Louvain*. P. 89.

Osipov, 2010 – *Osipov, V.Yu.* (2010). Rekurrentnaya neironnaya set' s upravlyaemymi sinapsami [Recursive neural network with controlled synapses]. *Informatsionnye tekhnologii*. № 7. Pp. 43-47. [in Russian]

Sainath, 2015 – *Sainath, T.N. et al.* (2015). Convolutional, long short-term memory, fully connected deep neural networks. *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. Pp. 4580-4584.

Sozykin, 2017 – *Sozykin, A.V.* (2017). Obzor metodov obucheniya glubokikh neironnykh setei [A review of teaching methods for deep neural networks]. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Vychislitel'naya matematika i informatika*. T. 6. № 3. [in Russian]

Алгоритм машинного обучения для детектирования выбросов и аномалий

Максим Сергеевич Василенко [a, *], Андрей Сергеевич Копырин [a]

[a] Сочинский государственный университет, Российская Федерация

Аннотация. Исследования по обнаружению аномалий во временных рядах являются важной темой в современной науке об аналитике данных – data science.

Существующие решения обнаружения аномалий в основном ищут отклонения в значениях параметров, которые фиксируют свойства известных (или предполагаемых известными) процессов, а это означает, что они используют так называемые числовые признаки. Следовательно, их возможности по обнаружению аномалий и отклонений в

[*] Корреспондирующий автор
Адреса электронной почты: renxi@yandex.ru (М.С. Василенко), kopyrin_a@mail.ru (А.С. Копырин)

априорно неизвестных процессов ограничены, так как трудно определить их числовые характеристики. Для решения данной проблемы, авторы предлагают использовать технологию машинного обучения для обнаружения аномалий наряду с мягкими вычислениями на основе нечеткой логики.

В современных искусственных нейронных сетях обычно используется большое количество нейронов, работающих параллельно и расположенных по слоям, но из-за проблемы исчезающего градиента большая рекуррентная нейронная сеть (РНС) не будет эффективно обучаться.

Предлагается использование сети с долгой краткосрочной памятью (Long Short-Term Memory, LSTM), так как, регулярное обратное распространение ошибки эффективно для обучения LSTM запоминанию значений в течение очень длинных временных интервалов.

Сделан вывод о том, что при анализе временных рядов сеть LSTM будет эффективно обрабатывать неструктурированную статистическую информацию, что делает ее пригодной к использованию для анализа больших данных.

Ключевые слова: поиск аномалий, нейронные сети, LSTM.