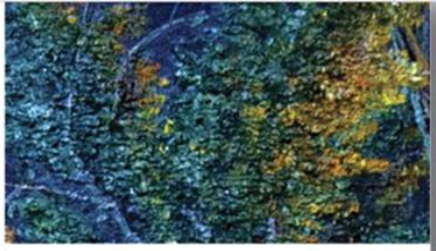


INTERNATIONAL SCIENCE REVIEWS

AIU

No. 4 (2) 2021

Natural Sciences and Technologies series

ISSN: 2707-4862

ASTANA INTERNATIONAL UNIVERSITY

INTERNATIONAL SCIENCE REVIEWS
Natural Sciences and Technologies series

Has been published since 2020

№4 (2) 2021

Nur-Sultan

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000
Tel.: (7172) 24-18-52 (ext. 316)
E-mail: natural-sciences@aiu.kz

International Sciense Reviews NST - 76153
International Science Reviews
Natural Sciences and Technologies series
Owner: Astana International University
Periodicity: quarterly
Circulation: 500 copies

CONTENT

DETECTING AND PREVENTING BLACK HOLE ATTACKS ON WIRELESS SENSOR NETWORKS

Mardenov Y. [1,2], Zhukabayeva T[1,2]., Abdildaeva A. [1], Sultangazieva A. [1]

Astana International University[1]
L.N. Gumilyov Eurasian National University[2]

Annotation. The protection of wireless sensor networks (WSN) is an urgent problem, since network nodes have low computing power, limited battery power and are located in unprotected places, and information is transmitted over wireless channels, any network disruption can lead to undesirable consequences. One of the common attacks against WSN is the Black hole attack. In this attack, the malicious host uses its routing technique to be able to advance in search of the fastest route to the host of the site or to the packet it wants to identify. This study analyzes the methods of protection in WSN against Black hole attacks. A method is shown of how a malicious node affects nodes in its transmission range.

Keywords: Black hole attack, WSN, attack detection.

I. Introduction

The latest advances in networking, semiconductor physics and materials science have enabled the widespread development and deployment of wireless sensor networks (WSS). BSS are formed by a large number of network nodes [1], called motes, - miniature autonomous devices capable of collecting information from the territory within a certain range and transmitting it to other devices. Each such device contains a data collection module (temperature, pressure, illumination, etc.) and an autonomous power source. Also, each motorcycle is equipped with a radio transceiver or other wireless communication device, that is, data is transmitted over the network via a radio channel. To accumulate all the collected information, the network contains a powerful node (sink, base station) connected to a stationary power source. Data is collected in this sink according to a specific routing algorithm. Combined into a wireless network, all nodes form a distributed self-organizing system for collecting and transmitting information. The advantages of systems based on sensor networks are the ability to deploy in hard-to-reach places, wireless communication, self-organization (the ability to redistribute routes in the event of failure of some nodes). Despite discoveries in the field of research in wireless sensor networks (WSN), there are already a large number of current problems in which these networks can be applied. [2] WSN security is one of the important ones. Inadequate physical protection makes them susceptible to interception, compromise and hacking. As a result, any encrypted data contained on these networks can be used by intruders to carry out attacks from the network, compromising the confidentiality of information. In addition, since there is a transmission in communication systems "over the air" by means of radio waves, it is possible

to carry out a wide class of attacks, starting with passive listening and ending with active [3], for example, Sybil,

Hello flood, Wormhole, DOS, Black hole attacks, etc. Old security mechanisms are not suitable due to lack of processing power, limited memory and power [4]. This article discusses the Black hole attack; as a result of this type of attack, more than 90% of the information transmitted to the sink can be lost [5].

II. Black hole attack

Black hole attacks are one such attack in WSN. This attack is carried out by an external attacker on a subset of sensor nodes in the network [6]. This is an active type of attack where an attacking node claims to have the shortest route to any desired node on the network, even if it does not have any route to it; therefore, all packets will go through it, and this allows the black hole node to forward or drop packets during data transfer. Regular nodes trust any response to the requests they send, and the black hole node takes advantage of this and continues to answer any request, claiming that it has the shortest path to the desired node. Usually, nodes begin the discovery phase to find a path to a destination node. The source node sends the request to the destination node, any node that receives this request checks to see if it has a new path to the destination node. When the black hole node receives this request, it immediately sends a response to the broadcaster, claiming it has the freshest and shortest path to the destination node. The originating node considers it to be the answer because there is no mechanism to verify that the request is from a normal node or from a black hole node. The source node starts forwarding packets to the black hole node in the hope of delivering those packets to the destination node, then the black hole node starts to discard those forwarded packets. [7]

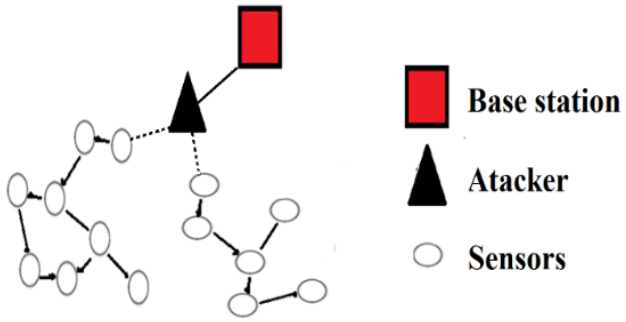


Figure-1 Black hole attack in the WSN

The attack can be organized in two ways [8].

- The first method is for an attacker to place a new node in the network area, with the help of which an attack is later organized. Impacts of this kind are relatively easy to detect and localize using standard FSS mechanisms.
- The second method is more dangerous when one of the legal nodes that are already participating in information exchange is hacked.

The attacker-controlled node removes all packets transmitted to it by other nodes for transit. In addition, a hacked node v0 can propagate information through the network that it is the closest node to the sink s, as a result of which the self-organizing network, which is the SSN, changes routing, and the other nodes that are closer to v0 than to s transmit their packets for onward transmission to s.

In [10] the developed scheme depends on the use of a fake identifier to decorate a black hole node. The originating node starts by sending a decoy request that contains an identifier that is not on the network. The black hole node will respond to this decoy RREQ due to its normal behavior, which responds to any RREQ on the network, reassuring that it has a better path. The developed scheme is implemented in DSR, so they modified the RREQ and RREP headers to identify the node of the black hole in the path. A warning is sent to neighboring nodes when a black hole node is detected. The origin node continues to check if there is a drop below a certain threshold; Then he starts bullying again. The limitations of this scheme are that it increases the size of control packets (RREQ and RREP), which leads to increased overhead in addition to black hole alerts, which can be used by an intelligent black hole to isolate nodes into the network.

In [11], they developed a technique that relies on the use of a cooperative decoy detection scheme (CBDS). In CBDS, black hole detection is divided into three phases: decoy, backtrace, and reactive defense. During the decoy phase, the source node chooses one of its neighbors at random and sends a decoy request using its identifier. During the backtracking phase, a list of suspicious nodes is generated from the RREP of the RREQ decoy, then neighbors enter random mode to determine if there is an attacker node in the path. For every black hole node found on the network, a black hole alarm is sent to neighboring nodes. In the reactive protection phase, the source node checks if the PDR is below a certain threshold, then it starts the decoy phase again. The limitation of this method is that the nodes enter promiscuous mode, which is not acceptable for all nodes. Since some nodes do not want any unauthorized user to listen to their own broadcasts, being in random mode will also encourage passive attacks. An intelligent black hole node can use the black hole alarm function and start transmitting false black hole signals to isolate network nodes.

In [12], they analyzed the black hole attack and explained that the route from a malicious node must increase the sequence number of the destination for a specific target in order to resolve the source node. The authors analyze and propose a statistical baseline anomaly detection approach to detect a black hole attack, and on the destination side they receive RREP (Route Replys) according to the destination sequence number

In [13], the black hole attack is isolated by propagating a message about the separation of the attack. This helps to improve the Packet Delivery Ratio (PDR) with minimal latency. Simulations are performed based on parameters such as black hole attack detection rate (BHADR), black hole attack detection time (BHADT), false positive rate (FPR), PDR and latency. The relationship between nodes is identified based on independent probability distribution functions and a mutual probability function.

III. The proposed algorithm

This project is a simulation of black hole attack detection in wireless sensor networks that uses a routing protocol for low power lossy devices as the network layer.

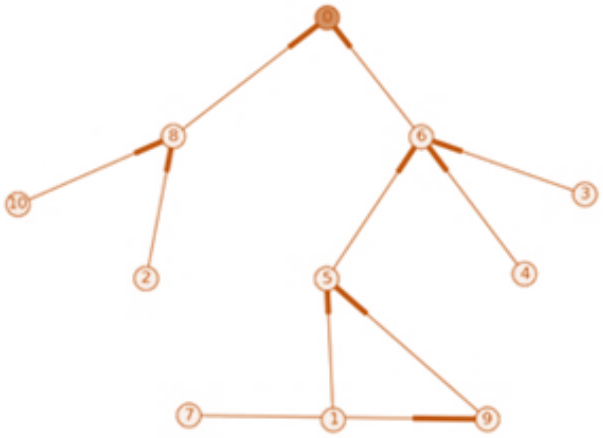


Figure-2 Wireless Sensor Network

This algorithm demonstrates that this type of attack can significantly affect the WSN through significant energy depletion.

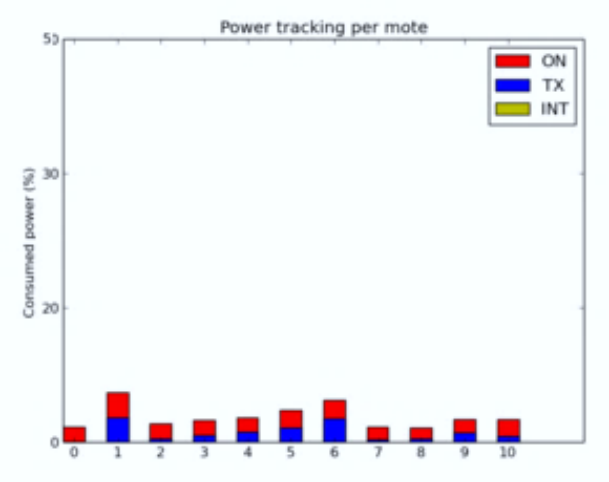


Figure-3 Tracking without active attack

Upon entering the WSN, thanks to the Contiki configuration constants set in the building block, the malicious node immediately starts sending DIS messages to its neighbors, then triggers DIO messages and resets the manual mode timers.

Figure-4 Black hole attack on WSN

As you can see, the malicious node (11) affects the nodes in its transmission range. We can now illustrate the effectiveness of the attack using this information to compare the power consumption in a simulation without (Figure-1) and with a malicious node (Figure-3).

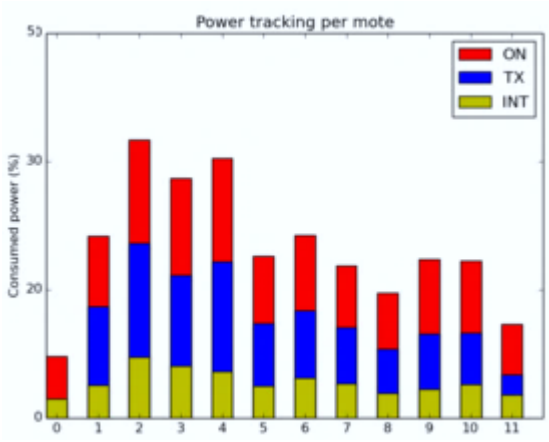


Figure-5 Tracking a Black Hole Attack

As you can easily see, nodes in the range of a malicious sensor are particularly susceptible to attacks in terms of turn on and receive times. However, these nodes are not affected by TX timing. This is because after receiving the DIS, the discarded nodes immediately send DIO due to the multicast nature of the DIS sent. Also, a way to perform a flood attack could be to unicast DIS to neighbors, activate DIO immediately in response, but not reset the manual timer.

Output

A black hole attack on a WSN can attract all kinds of traffic to a compromised host. Which leads to the launch of other attacks such as wormhole, eavesdropping. The consequences of which lead to the exhaustion of all network resources, dropping packets, modifying routing information

A mechanism for detecting the intrusion of black hole attacks is proposed. The approach is based on the exchange of control packets between sensor nodes and a base station. The simulation effects show that the recommended methodology has improved performance in IDS in terms of safety and energy consumption. As future work, sensory nodes can be modeled as black hole nodes along with a channel, and an efficient mechanism can be developed.

References

[1]. Umashankar Ghugar, Dr.Jayaram Pradhan, A Study on Black Hole Attack in Wireless Sensor Networks. Copyright, International Journal of Advance Computing Technique and Applications (IJACTA), ISSN : 2321-4546, Vol 5, Issue 1 2017

[2]. Miriam Carlos-Mancilla, Ernesto López-Mellado, and Mario Siller. Wireless Sensor Networks Formation: Approaches and Techniques. Hindawi Publishing Corporation Journal of Sensors. Volume 2016, Article ID 2081902, 18 pages. http://dx.doi.org/10.1155/2016/2081902

[3]. [4] A. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, editors, SPC, volume 3934 of Lecture Notes in Computer Science, pages 104{118. Springer, 2006

[4]. Ефименко, М. С. Проблемы применения и безопасности в беспроводных сенсорных сетях / М. С. Ефименко, С. И. Клымив. — Текст : непосредственный // Актуальные вопросы технических наук : материалы V Междунар. науч. конф. (г. Санкт-Петербург, февраль 2019 г.). — Санкт-Петербург : Свое издательство, 2019. — С. 24-26. — URL: https://moluch.ru/conf/tech/archive/324/14789/ (дата обращения: 10.06.2020).

[5]. Dokurer S., Erten Y., Acar C. Performance analysis of ad-hoc networks under black hole attacks. Proc. of IEEE Int. Conf. SoutheastCon 2007. 2007, pp. 148–153.

[6]. Ms.B.R.Baviskar, Mr.V.N.Patil. BLACK HOLE ATTACKS MITIGATION AND PREVENTION IN WIRELESS SENSOR NETWORK. International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163. Volume 1 Issue 4 (May 2014) http://ijirae.com

[7]. Adwan Yasin and Mahmoud Abu Zant. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 9812135, 10 pages. https://doi.org/10.1155/2018/9812135

[8]. В.В. Шахов, А.Н. Юргенсон, О.Д. Соколова. МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ АТАКИ BLACK HOLE НА БЕСПРОВОДНЫЕ СЕТИ. Программные продукты и системы / Software & Systems 1 (30) 2017. Т. 30. № 1. С. 34–39

[9]. C. Karlof, D.Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures, Special Issue on Sensor Network Applications and Protocols”, vol 1 (2-3), 2003,pp.1293 –1303

[10]. P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao, and J.-L. Chen, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs," in Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity, ICACT 2011, pp. 755–760, Seoul, Republic of Korea, February 2011.

[11]. P. L. Chelani and S. T. Bagde, "Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme," in Proceedings of the 2016 International Conference on Communication and Electronics Systems, ICCES 2016, Coimbatore, India, October 2016.

[12]. R.H.Jhaveri, S.J.Patel, D. Jinwala, "A novel approach for Greyhole and blackhole attacks in mobile ad hoc networks", Second International Conference on Advanced Computing and Communication Technologies, IEEE Computer Society, 2012, pp. 556–560.

[13]. John Clement Sunder A* and A. Shanmugam, "Black Hole Attack Detection in Healthcare Wireless Sensor Networks Using Independent Component Analysis Machine Learnining Technique", Current Signal Transduction Therapy (2018) 13: 1. https://doi.org/10.2174/1574362413666180705123733

МЕТОДЫ ОЦЕНИВАНИЯ ВНЕДРЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ БИЗНЕС-ПРОЦЕССАМИ ПРЕДПРИЯТИЯ

Серік Фараби[1*], Тасболатұлы Нұрболат[2]

[1]Студент магистратуры специальности «IT менеджмент», [2]PhD

[1,2]Международный Университет Астана, Нур-Султан, Республика Казахстан,

*+7(775)-115-75-10, serik.farabi@mail.ru

Аннотация.

В текущей статье описана следующая проблема, как рутиная работа, существующая абсолютно во всех должностях начиная со специалиста заканчивая вплоть до топ-менеджеров крупных компаний. в бизнес-процессах предприятия. Для решения поставленного вопроса рассматриваются автоматизированная система управления. В качестве примера была выбрана Роботизированная автоматизация процессов (RPA). Данная система является технологической имитацией человека-работника с целью быстрой и экономичной автоматизации структурированных и рутинных задач. Основываясь на послледние исследования выявляются следующие преимущества платформенной системы RPA: производительность работы, уменьшение расходов, быстрота и уменьшения количества ошибок. В статье приведены несколько методов для опредения необходимости внедрения автоматизированной системы управления бизнес-процессов, также знакомит с анализом критериев для определения возможности автоматизации бизнес-процессов. В добавок выделяется и описывается вероятность применения метода нечеткой логики в целях повышения эффективности автоматизации.

Ключевые слова: *автоматизированная система управления бизнес-процессов, RPA, Robotic Process Automation, метод нечеткой логики.*

Введение

Рутиная работа – основная часть многих бизнес-процессов имеющий однообразные и повторяющиеся действия. Под таким видом понимается не

только трудовая деятельность рабочего в архиве или менеджера по заключению договоров по типовой форме. С рутиными обязательствами часто сталкиваются и руководители.

Для уменьшения от такого вида работы можно обратиться к внедрению ИТ-проектов, однако планирование внедрения ИТ-проектов в больших случаях находится одним из сложных вопросов для многих компаний. Несмотря на многочисленных существующих методик и практик, оценка трудозатрат и эффективность внедрения с точностью в 100%, под силу только профессиональным проект-менеджерам имеющий немалый опыт работы. Для новых компаний планирующие внедрение такого рода автоматизации придется столкнутся с рядами рисков [1].

RPA (Robotic Process Automation или роботизация бизнеспроцессов) – это технология, позволяющая автоматизировать рутинные, повторяющиеся бизнес-процессы, позволяя сотрудникам сосредоточиться на более важных и сложных задачах. RPA применяется для процессов с четко прописанным алгоритмом действий. «Боты» способны полностью имитировать действия пользователя, и работать с сайтами, почтой, текстовыми документами, а также с различными системами.

В настоящее время RPA используется, как правило, для менее сложных, высокоструктурированных и часто встречающихся процессов. Хотя большинство RPA вендоров предлагают интеграцию с искусственным интеллектом, данные решения будут востребованы только в будущем [2].

Многие компании только начинают открывать для себя такую технологию как RPA. И здесь появляется вопрос о том, какие же процессы можно автоматизировать, а также о том, насколько это выгодно. Если бизнес-процессов для автоматизации в компании несколько, то необходимо проанализировать каждый процесс и

выделить процессы, которые наиболее подходят для автоматизации и принесут компании наибольший эффект.

Преимущества и недостатки внедрение роботизированных процессов

Потенциальные преимущества RPA многочисленны. Компаниям обещают огромную экономию средств и повышение качества. RPA также ассоциируется со словом «быстрый»: быстрая разработка, быстрое внедрение и быстрая окупаемость. Однако опыт доказывает, что это не всегда так. Не все компании, внедрившие RPA, могут заявить об успешном окончании проекта и о достижении поставленных целей. Некоторые клиенты сообщают, что ожидали от роботизации бизнес-процессов большего. Опрос клиентов показывает, что в 86% случаев внедрение RPA привело к ожидаемому повышению производительности или даже превысило ожидания. Однако, автоматизация не оправдывает ожидания по экономии средств в 40%, в частности, потому что разработка и внедрение требуют больше времени, чем ожидалось. Таким образом, можно сделать вывод о том, что к подготовке и планированию RPA проектов следует относится внимательнее, включая во внимание факторы, которые могут привести к задержке проекта [2].

Следует отметить, что при роботизированной автоматизации бизнес-процессов можно выделить общие выгоды, недостатки и затраты. К основным выгодам внедрения роботизации можно отнести повышение эффективности процессов при сокращении времени на их выполнение, улучшение качества работы. Для многих клиентов важным фактором является возможность работы 24/7, что позволяет выполнять некоторые процессы ночью. Автоматизация также несёт в себе иные преимущества. К примеру, сводит количество ошибок к нулю, исключая человеческий фактор. В некоторых случаях подобные ошибки могут обойтись компании очень дорого. Еще один важный плюс – это сокращение общих затрат на выполнение бизнес-процесса, а именно, сокращение количества сотрудников, участвующих в бизнес-процессе, или освобождение рабочего времени сотрудников для выполнения других заданий.

Однако, следует учесть и затраты, которые понесет клиент, решив внедрить RPA. К таким затратам следует отнести затраты на разработку и внедрение RPA. «Ботов» необходимо установить, протестировать, а при необходимости, внести изменения. Далее, в течение определенного периода времени, необходимо проверять и анализировать его работу. На это также должны быть запланированы ресурсы. Еще один тип затрат, который ожидает клиентов – это затраты на лицензию RPA-платформы.

Такая подписка может оплачиваться каждый месяц или каждый год, в зависимости от поставщика и типа лицензии.

Помимо затрат, есть и другие минусы, которые следует учитывать перед началом реализации RPA проекта. Проблема безопасности является одной из самых сложных и спорных на данный момент. Открытым остается вопрос о конфиденциальных данных, таких как учетные записи. Следующий вопрос, на который предстоит ответить – это вопрос о том, кто будет ответственен за ошибку, допущенную роботом. Сопротивление персонала или руководства – также является весомым минусом при внедрении роботизированной автоматизации. Для успешного внедрения РПА необходим грамотный анализ бизнес-процесса, который возможно провести только при поддержке персонала и руководства компании. Для этого необходимо, чтобы каждый понимал цели автоматизации и способствовал развитию данного проекта [3].

Анализ целесообразности внедрения роботизированных проектов

Залогом успешной автоматизации является грамотный анализ бизнес-процесса. Посредством данного анализа необходимо не только определить, насколько данный процесс подходит под критерии автоматизации, но и выяснить, насколько целесообразно данный процесс автоматизировать.

Основными критериями для автоматизации служат:

- четкий алгоритм работы;
- есть явный триггер процесса;
- интерфейс программы не подвергается меняться;
- структурированные данные; – большие объемы транзакций.

Опираясь на эти критерии следует понимать, что, если мы можем автоматизировать процесс с использованием РПА, совершенно не значит, что мы должны это делать. Если автоматизация возможна с использованием программирования и API-запросов, и при этом никакие другие факторы не противоречат этому, то такая автоматизация должна быть предпочтительнее, чем применение RPA [2].

Процессы, для выполнения которых необходим контроль человека, пока не популярны для автоматизированной роботизации. Ситуации, для которых требуется принятие решения, должны обрабатываться роботом, интегрированным с системами искусственного интеллекта. На сегодняшний день это возможно только при наличии большого объема структурированных данных. Такая автоматизация требует еще больших затрат, а также не всегда возможна, так как не все компании обладают возможностью собрать нужный объем данных. Поэтому основным направлением роботизации на сегодняшний день остаются рутинные, четко структурированные процессы.

Многие компании пытаются выделить для себя негласные принципы и правила автоматизации, основанные на их собственном опыте. Так, например, компания Forrester предлагает «правило 5» [4]:

- не более 5 решений
- не более 5 приложений – не более 500 кликов.

К сожалению, на данный момент не существует единого подхода для определения того, какие же процессы должны быть автоматизированы.

Классическим примером оценки эффективности автоматизации является количество времени, которое удастся сохранить благодаря роботам. Обобщая результаты пилотов на глобальные процессы, которые предполагается автоматизировать, можно подсчитать примерное количество часов, которое получится сэкономить (обычно цифры колеблются от 30% до 70%). После того, как эта цифра будет получена, можно использовать информацию о сотрудниках (включая их оклад), процессы которых будут автоматизированы, и подсчитать среднечасовую экономию. Крайне важно, чтобы в эту цифру также включалась информация о будущих возможных курсах по обучению персонала, повышениям, затратам на поддержку рабочего места и т. п.

Комплексная оценка внедрения роботизированных процессов

Проведение комплексной оценки внедрения RPA необходимо в том случае, когда в компании планируется автоматизировать не один, а несколько бизнес-процессов. В данном случае перед ИТ-отделом часто возникает вопрос о том, какие из процессов необходимо автоматизировать, а какие процессы оставить без изменений. Одним из методов такой оценки может служить распределение

бизнес-процессов на четыре категории: нецелесообразно, скорее нецелесообразно, скорее целесообразно, целесообразно.

Для реализации необходимо провести оценку каждого бизнес-процесса по четырем параметрам:

- FTE – число задействованных в процессе сотрудников (fulltimeemployee);
- ST – число сотрудников, поддерживающих RPA-процесс (supportteam);
- CF – фактор сложности процесса (complexityfactor);
- VF – фактор волатильности (изменчивости) процесса (volatilityfactor).

Измерив каждый показатель, можно разместить любой процесс на системе координат, где по оси ординат будет сложность и волатильность, а по оси абсцисс – число задействованных в процессе сотрудников и число сотрудников, поддерживающих RPA проект. Систему координат с проставленными на ней процессами можно разделить на четыре квадранта критериев-рейтингов:

- P1 – безусловно целесообразно;
- P2 – скорее целесообразно; – P3 – скорее нецелесообразно; – P4 – нецелесообразно.

Рисунок. Рисунок. Представление распределения бизнес-процессов

Данный метод позволяет лишь визуально определить, какие процессы наиболее подходят для автоматизации. Однако, он не учитывает, сколько рабочего времени будет сэкономлено благодаря автоматизации. Также, используя описанный выше метод, нельзя сказать и о том, когда окупиться внедрение проектов.

Определение группы бизнес-процессов, наиболее подходящих для роботизированной автоматизации возможно с помощью применения метода

нечеткой логики, позволяющей не только ввести дополнительные критерии оценки, но и использовать для оценки лингвистические переменные [5]. Таким образом, можно ввести ранжирование процессов по сложности: высокая, средняя, низкая. Далее каждому параметру необходимо задать дополнительный вес с помощью мультипликатора, к примеру, от 1.1 до 1.3. Далее, необходимо вычислить коэффициент эффективности автоматизации для каждого проекта. Полученные коэффициенты можно использовать при планировании комплексного внедрения RPA.

Выбор инстумента для оптимизации внетрия РПА

Оценку эффективности внедрения технологий РПА предлагается проводить на основе теории нечеткой логики методом аддитивной свертки ряда критериев.

Важной особенностью применяемого метода является необходимость учета субъективных предпочтений экспертной группы при определении коэффициента эффективности автоматизации процессов. Эта особенность означает, что различные эксперты при одной и той же ситуации, при использовании одной и той же модели могут получить различный результат [5].

При построении метода установлено, что характерными чертами алгоритмов решения задачи выбора оптимальных решений методами нечеткой логики является наличие некоторого набора утверждений (правил), каждое из которых представляет собой совокупность событий (условий) и результатов (выводов). После постановки задачи в терминах правил, состоящих из условий и выводов, производится их специальная обработка. Идея обработки состоит в преобразовании (фаззификации) нечетких значений условий и выводов в количественную форму. Для этого используются различного рода функции принадлежности. Выбор типа функции зависит от решаемой задачи.

Анализ современных подходов к учету специфики неопределенности в процессах протекающих в сфере IT-технологий, а также существующих методик их описания показал:

особенностью метода нечеткой логики является наличие возможности оценки эффективности внедрения относительно

«идеальной IT-компании»; оценку результатов внедрения РПА определять на основе статичной и динамической составляющих по значению коэффициента эффективности.

Из вышеизложенного следует, что применение метода нечетких экспертных оценок может существенно повысить качество комплексного внедрения RPA

Заключение

Одним из методов анализа возможности внедрения RPA для нескольких бизнес-процессов является распределение бизнес-процессов на основании четырех основных критериев: число задействованных в процессе сотрудников, число сотрудников, поддерживающих RPAпроцесс, фактор сложности процесса, фактор волатильности (изменчивости) процесса. Однако данный метод не дает информации о сэкономленном времени после внедрения RPA, а значит, нельзя сделать вывод о том, насколько быстро окупиться имплементация. Другой метод, позволяющий оценить эффективность внедрения RPA – метод оценки бизнес-процессов на основании нечеткой логики. Данный метод позволяет вычислить коэффициент эффективности автоматизации и использовать эти данные при планировании комплексного внедрения RPA. Таким образом, применение метода нечеткой логики повысит эффективность вложения денег компанией и поможет оптимизировать расходы на персонал.

Список литературы

1. Aguirre, S. Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study. Workshop on Engineering Applications. / S. Aguirre, A. Rodriguez. – Berlin: Springer Verlag. 2017. – P. 65-71.
2. Alejandro Rodriguez. Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study [Электронный ресурс] – Режим доступа : https://www.forbes.com/sites/cognitiveworld/2018/12/02/the-big-rpa-bubble/?sh=51c5a33368d9
3. Shetty, S. Gartner Says Worldwide Spending on Robotic Process Automation Software to Reach $680 Million in 2018 [Press release].
[Электронный ресурс] : статья. – Режим доступа :

https://www.gartner.com/en/newsroom/press-releases/2018-11-13-gartnersays-worldwide-spending-on-robotic-process-automation-software-to-reach680-million-in-2018. .html

4. Leslie, J. Ten Golder Rules fro RPA Success.[Электронный ресурс] : статья – Режим доступа : https://www.forrester.com/report/Ten+Golden+Rules+For+RPA+Success/-/ERES143771.

5. Матвеев, М.Г Обработка экспертной информации в задачах принятия решений в условиях нечеткой неопределенности / М.Г. Матвеев, Е.В. Гринева // Вестник Воронежского государственного технического университета. 2012 т.8 №8, – С.11-14.

УДК 004

МӘТІНДІ ТОНАЛДЫЛЫҚҚА АНЫҚТАУ ӘДІСТЕРІНЕ ТАЛДАУ

Леспекова А.А[1], Муканова А.С[2].
azizalespekova1998@gmail.com, assel.mukanova@aiu.edu.kz

[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Кәсіпорындардағы компьютерлік жүйелер мен желілерді әкімшілендіру, бақылау және қорғау мамандығының 2-курс магистранты, Нұр-Сұлтан қаласы, Қазақстан.
[2]Астана халықаралық университеті

Аңдатпа. Мақалада мәтіннің тоналдылығын анықтау үшін қолданылатын бірнеше тәсілдерге талдау жүргізілді. Олардың артықшылықтары мен кемшіліктері көрсетілген. Сонымен қатар машиналық оқыту әдісі мен лексикаға негізделген әдістердің жұмыс жасау принциптері қарастырылды. Лексикаға негізделген әдіске бағытталған программаның жұмыс істеу мүмкіндіктері көрсетілді.

Түйін сөздер: тоналдылық, лемматизация, корпус, мәтін, талдау алгоритмдері

КІРІСПЕ

Мәтіннің тоналдылығын талдау (sentiment analysis) - табиғи тілді өңдеу (natural language processing, NLP) әдістерінің бірі, оның мақсаты мәтіннен эмоционалды мазмұнды алу болып табылады. Жасанды интеллекттің бұл бағыты табиғи тілде мәтін түрінде болатын әртүрлі ақпаратты алуға мүмкіндік береді.

Мәтіннің тоналдылығы немесе тоны — бұл автордың кейбір оқиғаларға, кейіпкерлерге, объектілерге немесе тікелей аудиторияға деген эмоционалды қатынасының көрінісі. Бұл мәтіннің эмоционалды компоненті. Бұл сипаттама өте маңызды. Өйткені, эмоцияларсыз мәтін тартымсыз және монотонды болады Тоналдылық бір өлшемді немесе көп өлшемді эмоционалды кеңістікке жіктелуі мүмкін. Бір өлшемді кеңістікте тек бір шкала болады, онда бірнеше мәндер болуы мүмкін. Көп өлшемді кеңістікте бірнеше ортогональды өлшемдер бар, негізгі эмоцияларды (қуаныш, бақыт, қорқыныш) жатқызамыз. Осылайша, тоналдылықты талдауды кейбір көңіл-күй бағаларын тағайындау арқылы жүзеге асырылатын сапалы деректерді сандық сипаттау әдісі ретінде қарастыруға болады.

Тоналдылықты талдаудың мақсаты - мәтіндегі пікірлерді табу және олардың қасиеттерін анықтау. Аудитория мүшелерінің ойлау тәсілін зерттеу және өнімнің жағдайын қарама-қарсы тұрғыдан зерттеу мүмкіндігі.

Тоналдылықты анықтау үшін (Taboada, 2011жылы) [7] пікір терминдерін көңіл-күй сөздігімен салыстыратын лексикаға негізделген әдісті ұсынды. Ол жұмыста көңіл-күйді қаншалықты оң немесе теріс екенін бағалайды.Пікірлер сөздіктегі сөздер объективті.

(Hu, 2004жылы) [5] Сөздікке негізделген тәсілдің негізгі стратегиясы ұсынылған болатын. Онда белгілі бағдармен пікір білдіретін сөздердің шағын жиынтығы қолмен жинақталады.

Жарнама контекстінде (Qiu, 2010) [6] Сезімдерге қатысты сөйлемдерді анықтау үшін сөздікке негізделген әдісті қолданды. Олар жарнаманың өзектілігі мен пайдаланушылармен жұмыс істеу ыңғайлылығын арттыратын жарнамалық тәсілді ұсынды. Олар тақырыптық сөздерді шығару мәселесін шешуге және синтаксистік талдау мен көңіл-күй сөздіктерін қолдана отырып, жарнаманың кілт сөздерін алу кезінде тұтынушылардың көзқарасын анықтауға арналған ережеге негізделген стратегияны ұсынды. Олар автомобиль веб-форумдарына өз үлестерін қосты.

(Mandal Das, 2018) [8] Автор екі тілдің, ағылшын және бенгал тілдерінің көңіл-күйін анықтау үшін фильмдердің шолу мәліметтерімен жүргізілген әртүрлі эксперименттердің нәтижелерін талдады. Олар әр түрлі Машиналық оқыту алгоритмдерін сынақтан өткізді кодпен араласқан және ең жоғары дәлдікке қол жеткізген деректер *59,00% аңғал Байес* моделін (NB) және 72,50% тірек векторлық машина модельдеріндегі (SVM) нәтижені алды. Олар мынадай тұжырымға келеді: оқу және тест деректері бірдей болған кезде SVM жоғарғы нәтижені көрсетеді, ал NB оқыту және тестілеу деректері әртүрлі болған кезде жақсы жұмыс істейді.

НЕГІЗГІ БӨЛІМ

Мәтінді тоналдылыққа талдау алгоритмдері. Ережеге негізделген тәсіл табиғи тілді өңдеудің негізгі процедурасын қамтиды . Ол келесі мәтіндік әрекеттерді қамтиды:

- Стемминг
- Токенизация
- Тотау сөздер
- Талдау Лексиканы талдау (тиісті контекстке байланысты)

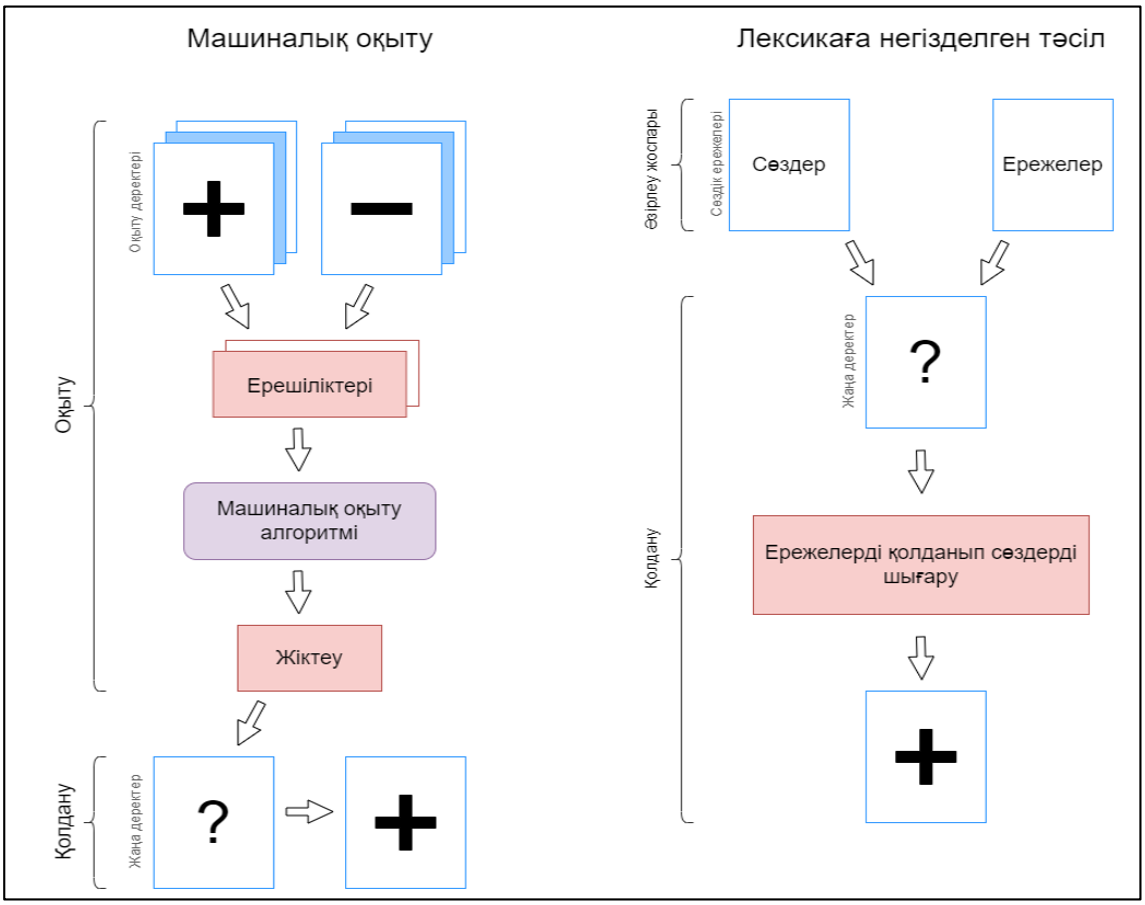
Мәтінді алдын-ала өңдеу мәтінді тоналдылыққа талдаудың бірінші кезеңі болып табылады. Бұл "шулы" мәтіннен тиісті ақпаратты бөліп көрсету үшін қажет. Мәтінді алдын-ала өңдеу барлық сөздерді бір регистрге келтіруді, тыныс белгілерін жоюды, тоқтату сөздерін жоюды, токенизацияны, сөздерді қалыпқа келтіруді және

қажет болған жағдайда басқа операцияларды қамтиды. Мәтінді талдау кезінде барлық сөздерді қалыпқа келтіру ұсынылады. Яғни. сөзді оның бастапқы түрінде ұсыну. Қалыпқа келтіруді екі жолмен жүргізуге болады: лемматизация және стемминг.

Лемматизация-сөзді оның бастапқы формасына (лемма) түрлендіру. Лемматизация морфологиялық сөздікке негізделген. Егер сөз сөздікте болмаса, онда сөзді өзгерту және оған лемма алу жолдары туралы гипотеза жасалады.

Стемминг-сөздің негізін алу, ал сөздердің соңы, жұрнақтары, префикстері алынып тасталады. Осылайша, мәтіндегі барлық сөздер бір нысанға келтіріледі. Стемминг негізделген морфологиялық ережелердің және сөздіктің болуын талап етпейді.

Оның жұмыс жасау принципі: Сөздердің екі тізімі бар. Олардың біреуіне тек оң, екіншісіне теріс кіреді. Алгоритм мәтінді қарайды, өлшемдерге сәйкес келетін сөздерді табады. Осыдан кейін алгоритм мәтінде қандай сөз басым екенін есептейді. Егер оң сөздер көп болса, онда мәтіннің оң полярлығы бар деп саналады(1-сурет). Төменгі суретті машиналық оқыту әдісі мен лексикаға негізделген тәсілдердің жұмыс жасау принциптері көрсетілген. Машиналық оқыту әдісінде тоналдылық автоматты түрде машиналық оқыту алгоритмі бойынша анықталады. Лексикаға негізделген тәсілде сөздерді реттеп отыратын мұғалім қажет болады. Ережеге негізделген алгоритмдердің мәні-олар қандай да бір нәтиже берсе де, оларды шынымен пайдалы ететін икемділік пен дәлдік жетіспейді. Мысалы, ережеге негізделген тәсіл контекстті ескермейді. Алайда, оны клиенттерге қызмет көрсету үшін пайдалы болуы мүмкін хабарламалардың үнін анықтау үшін жалпы мақсатта пайдалануға болады.



Сурет 1. Тоналдылыққа талдау әдістерінің жұмыс жасау архитектурасы

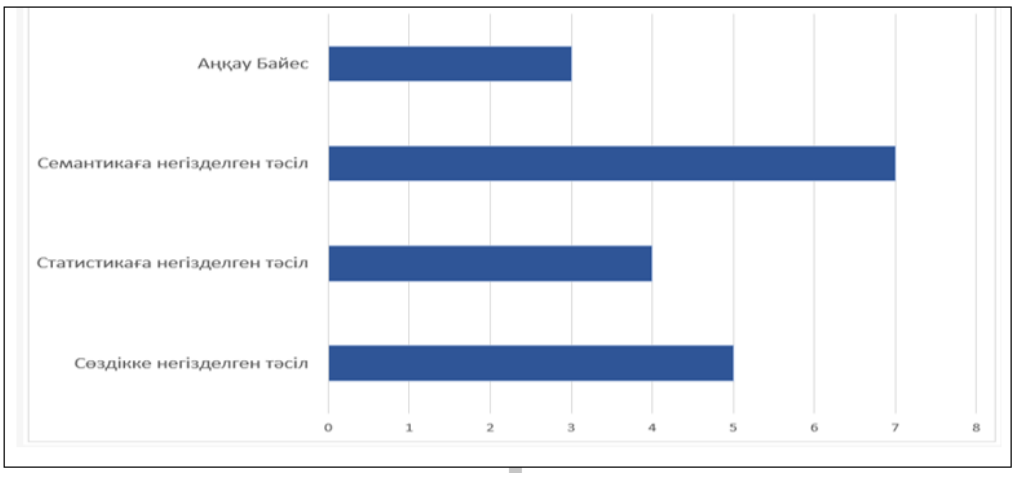
Тоналдылықты талдаудың қарапайым түрі "жақсы" және "жаман" сөздер сөздігінің көмегімен жүзеге асырылады. Сөйлемдегі әр сөз мағынасына қарай сандық сипатқа ие бола алады: әдетте +1 оң тоналдылық жағдайында, ал -1 – теріс тоналдылық жағдайында. Содан кейін біз сөйлемнің жалпы тоналдылығын білу үшін барлық сөздердің бағаларын қорытындылаймыз. Әлбетте, бұл тәсіл көптеген шектеулерге ие болады. Контекст пен жақын сөздерді елемеуі мүмкін. Мысалы, біздің қарапайым модельде "жақсы емес" деген сөзді 0 тоналды бағалаумен жіктеуге болады, өйткені "жоқ" -1 баллға ие, ал "жақсы" +1 баллға ие. Адам "жақсы емес" сөзін "жақсы"сөзінің болуына қарамастан теріс деп жіктеуі мүмкін, сондықтан да анықталмаған жағдайда 0 балл шкаласымен есептейміз.

Лексикаға негізделген тәсілдер жоғары сапалы көңіл-күй лексикасын қажет етеді, ал машиналық оқыту тәсілдері тиімді лингвистикалық функцияларды қажет етеді. Көңіл-күй лексикасы әртүрлі көңіл-күй полярлықтары бар көптеген сөздерден тұрады. Лексикаға негізделген тәсілдерге сөздікке негізделген тәсілдер,

корпус және қолмен жасалатын тәсілдер кіреді, бірақ көптеген зерттеушілер корпусқа негізделген әдістерге көбірек көңіл бөледі.

Сөздікке негізделген тәсіл. Ол полярлығы қолмен жинақталған бастапқы сөздердің аз санынан басталады. Содан кейін сентименталды сөздердің саны WordNet, SentiWordNe және тезаурус сияқты танымал лексикондарға негізделіп көбейеді. Бұл әдіс лингвистикалық талдауды қолдана отырып, алдын-ала құрастырылған тоналды сөздіктер мен ережелер бойынша мәтіндегі эмоционалды лексиканы іздеуге негізделген.

Корпустық тәсіл сентименталды сөздердің аз санынан басталуы мүмкін, содан кейін кейбір нақты ережелерге немесе формулаларға сәйкес үлкен корпус арасында сентименталды сөздердің саны артады. Корпус тәсілдері контекстке бағытталып оның мазмұнын таба алады, ал сөздікке негізделген тәсілдер мұндай сөздерді таба алмайды. Корпустың көптеген тәсілдері деректерге негізделген көңіл-күй лексикасын құру әдістеріне негізделген. Ол белгілі бір пәндік аймаққа тән көңіл-күй лексикондарын құруда артықшылықтарға ие. Корпусқа негізделген тәсілдерді нақты әдістер тұрғысынан статистикаға негізделген тәсілдер мен семантикаға негізделген тәсілдер деп бөлуге болады.



Сурет 2. Мәтінді тоналдылыққа таңдау әдістерінің қолданылу жиілігі

Статистикаға негізделген тәсілдің негізгі идеясы—көңіл -күй сөздері арасындағы қатынасты көрсететін тиісті статистикалық ережелерді әзірлеу. Бұл бастапқы көңіл-күй сөздерінің аз ғана бөлігінен басталады, ал статистикаға негізделген кейбір басқа тәсілдер бастапқы көңіл-күй сөздерін қажет етпейді. Статистикалық ережелер зерттеушілердің назарын аударды және олар бақылау, талдау және жалпылау арқылы статистикаға негізделген көптеген тиімді ережелерді анықтады. Мәтінді талдау үшін біз келесі алгоритмді қолдана аламыз: алдымен мәтіндегі әр сөзге сөздіктен оның тоналдық мәнін тіркейміз (егер ол

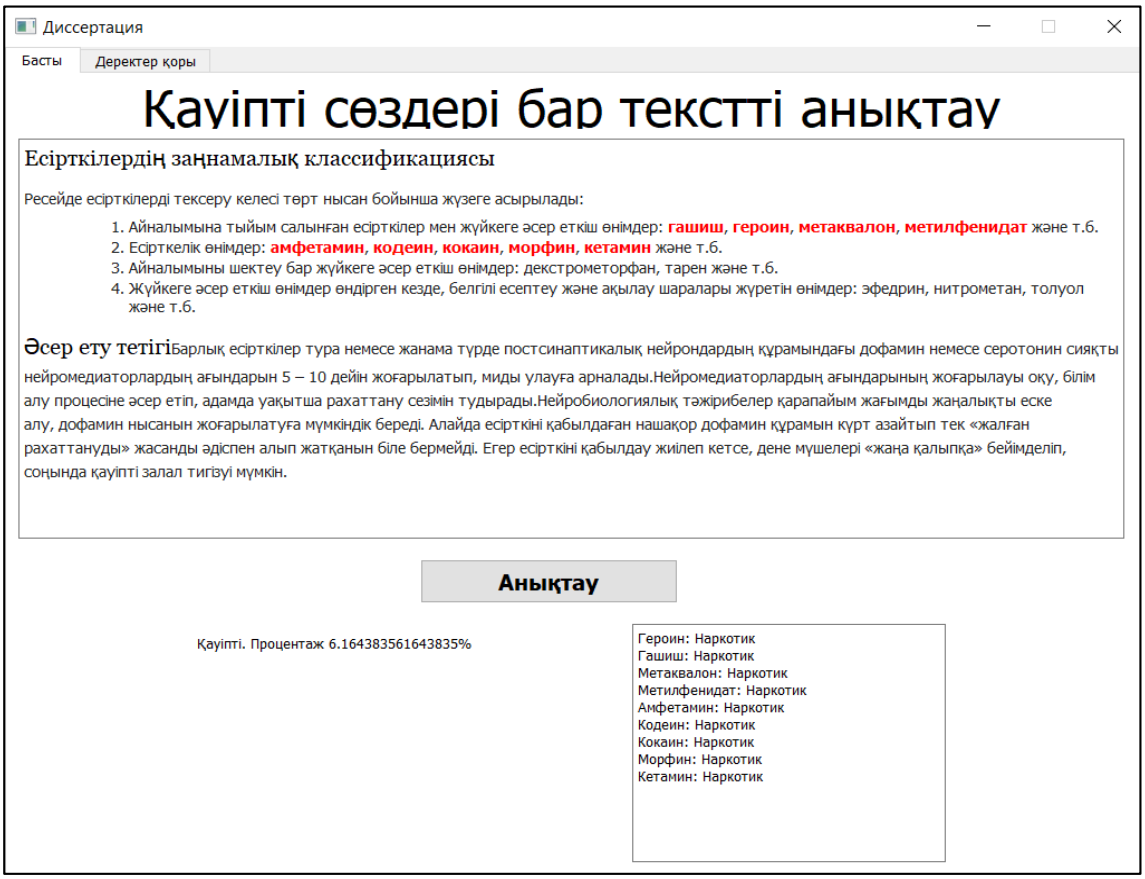
сөздікте болса), содан кейін әр жеке сөйлемнің тоналдық мәндерін қосу арқылы бүкіл мәтіннің жалпы тоналдылығын есептейміз. Қарапайым арифметикалық ортасын есептей қоямыз.

Семантикаға негізделген тәсіл сентименталды сөздердің мағыналарын белгілі бір принциптерге сәйкес анықтайды. Семантикалық мағынасы ұқсас сөздер көңіл-күйді ұқсас бағалауға ие болады. Семантикаға негізделген тәсілдің негізгі идеясы-көңіл-күйдің бастапқы сөздері, эмотикондар немесе көңіл-күйдің белгілі бір полярлығын білдіретін кез-келген басқа белгілер сияқты парадигмалық сөздерді анықтау. Әр сөзді дұрыс есептеу формуласын қолдана отырып, сөз парадигмасы арқылы өлшеуге болады. Бұл жағдайда көңіл-күйдің қарқындылығын көрсететін көңіл-күйді бағалау тиісті көңіл-күй сөзіне тағайындалады. Сонымен қатар, бұл тәсілді итеративті түрде жүзеге асыруға болады, яғни көңіл-күй лексикасының ауқымы біртіндеп артып келеді. 2004 жылы көңіл-күйдің тұқымдық сөздері мен бағалау факторы - "жақсы" және "жаман"деп аталатын *сын есімдер арасындағы* семантикалық қашықтықты есептейтін тәсілді ұсынды. Семантикалық қашықтық WordNet-пен есептеледі, ал соңғы нәтижелер бұл тәсіл әдеттегі сұраушыға қарағанда нақты мәселелер үшін жеткілікті жұмыс істейтінін көрсетеді.

Категориялар	Әдістер	Артықшылықтары	Кемшіліктері
Лексикалық тәсіл	Сөздікке негізделген тәсіл	Сөздік қоры тез жасалады және оның сапасы жоғары	Ол алдыңғы лексиканы немесе синонимдерді қажет етеді және оны қамту шектеулі
	Статистикаға негізделген тәсіл	Статистикаға негізделгендіктен оның қамтуы үлкен. Сонымен қатар, лексикондар әртүрлі салаларға жарайды	Лексиканың сапасы қол лексикондарына қарағанда нашар. Параметрлерден тым шекті мәндерді анықтау оңай емес
	Семантикаға негізделген тәсіл	Ол семантикалық ақпаратты енгізу арқылы жоғары қол жетімділікке және сапаға ие	Кейбір жағдайларда бұл ұзақ уақыт алуы мүмкін және оның параметрлері тәжірибеге сәйкес беріледі
Дәстүрлі машиналық оқыту тәсілі	Аңқау Байес	Онымен модель құру оңай және ол тұрақты жіктеу дәлдігіне ие	Әр түрлі тәуелсіз деген болжам нақты жағдайларда орындалмауы мүмкін

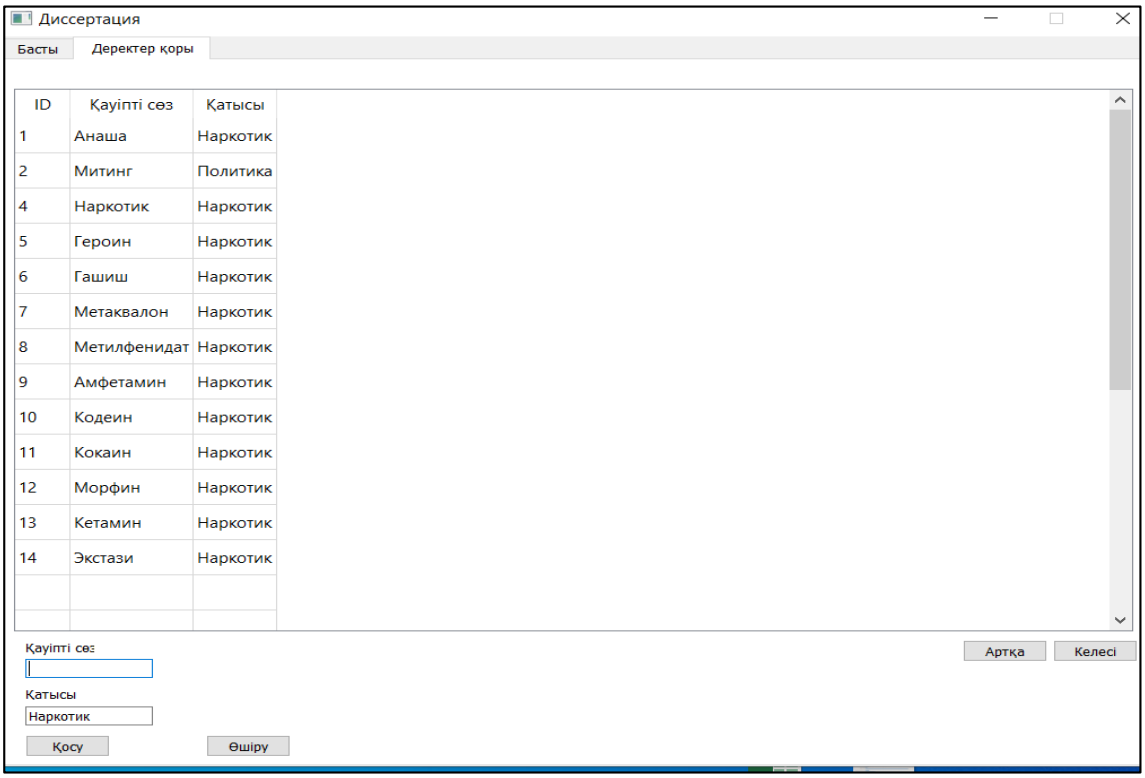
Сурет 3. Мәтінду тоналдылыққа талдау әдістемесінің қысқаша мазмұны

Жоғарыда көрсеткен әдістерді талдай отырып, мәтіннің тоналдылығын анықтай отырып, тыйым салынған сөздерді анықтауға бағытталған программа жүзеге асырылды. Программада мәтінді тоналдылыққа талдаудың лексикаға негізделген әдісі қолданылады және алдағы уақытта толықтырылады. Ол екі беттен тұрады. Бірінші бетте енгізілген мәтіннен корпуста бар сөздер белгіленеді. Мұнда анықтау батырмасы арқылы мәтінде кезіккен қауіпті барлық сөздерді және олардың қандай категорияға жататынын көрсетеді.



Сурет 4. Мәтіннен кауіпті сөздердің анықтау

Екінші бетте мәтін корпусымен жұмыс жасалады. Мұнда біз қауіпті сөздерді категорияларға бөліп,қоса аламыз. Алдағы уақытта бұл жұмыс өңделіп толықтырылады.



Сурет 5. Корпустағы сөздер жиыны

ҚОРЫТЫНДЫ

Бұл жұмыста мәтіннің тоналдылығын анықтаудың бірнеше тәсілдеріне талдау жүргізілді. Артықшылықтары мен кемшіліктері көрсетіліп өтілді.

Сонымен қатар машиналық оқыту әдісі мен лексикаға негізделген әдістердің жұмыс жасау принциптері қарастырылды. Тақырып бойынша жүргізілген жұмыстар сипатталды. Таңдалған әдістердің ішінде ең оңтайлысы корпуска негізделген әдіс. Лексикаға негізделген әдіске бағытталған программаның жұмыс істеу мүмкіндіктері көрсетілді.

ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Б. Лю и Л. Чжан, «Пікірлерді зерттеуге және көңіл-күйді талдауға шолу» 2012жыл, 412-425бет.
2. Кумбрия Эрик, "Аффективті есептеу және көңіл-күйді талдау", IEEE Intelligent Systems. 2016жыл, 102-107 бет.
3. Поляков Е. В., Восков Л. С., Абрамов П. С., Поляков С. В. Қысқа мәтіннің көңіл-күйін талдау мәселелерін шешуге жалпыланған көзқарасты зерттеу,

табиғи тілді өңдеу тапсырмаларындағы хабарламалар. Ақпараттық-басқару жүйелері, 12-14бет. 2020ж.
4. Ениколопов С. Н., Кузнецова Ю. М., Смирнов И. В., Станкевич М. А., Чудова Н. В. мәтінді автоматты түрде талдау құралын жасау әлеуметтік-гуманитарлық зерттеулер. 1 бөлім. Әдістемелік және әдіснамалық аспектілер. Жасанды интеллект және шешім қабылдау, 2019жыл, 28-38 бет.
5. Hu, M., Liu, B., & Street, S. M. (2004). Пайдалы қазбаларды өндіру және клиенттердің пікірлерін жалпылау.
6. Кю, Г., Он, Х., Чжан, Ф., Ши, Ю., Бу, Дж., и Чен, с.((2010). Қолданба деректері бар сараптамалық жүйелер : Көңіл-күйге негізделген наразылыққа бағытталған жарнаманы талдау Q, қосымшалары бар сараптамалық жүйелер, 37 (9), 6182-6191. https://doi.org/10.1016/j.eswa.2010.02.109
7. Табоада, М., Брук, Дж., және Фолл, к. (2011). Лексикаға негізделген көңіл-күйді талдау әдістері. 2010 жылғы қыркүйек
8. Mandal, S., & Das, D. (2018). Көңіл-күйді анықтау үшін жіктеуіштер мен кодпен араласқан факторлардың рөлін талдау.

АНАЛИЗ МЕТОДОВ ОПРЕДЕЛЕНИЯ ТОНАЛЬНОСТИ ТЕКСТА

Аннотация. В статье проведен анализ нескольких подходов, используемых для определения тональности текста. Показаны их достоинства и недостатки. Также были рассмотрены принципы работы метода машинного обучения и методов, основанных на лексике. Продемонстрированы возможности функционирования программ, ориентированных на лексический метод.

Ключевые слова: тональность, лемматизация, корпус, текст, алгоритмы анализа

Сведения об авторе:

Леспекова А. А[1], Муканова А. С[2].
[1]Евразийский национальный университет имени Л.Н. Гумилева, магистрант 2 курса, г. Нур-Султан, Казахстан.
[2]Международный университет Астана

ANALYSIS OF METHODS FOR DETERMINING THE TONALITY OF THE TEXT

Annotation. The article analyzes several approaches used to determine the tonality of the text. Their advantages and disadvantages are shown. The principles of the machine

learning method and methods based on vocabulary were also considered. The possibilities of functioning of programs focused on the lexical method are demonstrated.

Keywords: tonality, lemmatization, corpus, text, analysis algorithms

About the author:

[1]Lespekova A. A , [2]Mukanova A. S.
[1]L.N. Gumilyov Eurasian National University, 2nd year master's student, Nursultan, Kazakhstan.
[2]Astana International University

ИССЛЕДОВАНИЕ И АНАЛИЗ МЕТОДОЛОГИЙ УПРАВЛЕНИЯ IT-ПРОЕКТАМИ В ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ

МажитА., Муканова А.С.

Международный университет Астана

Аннотация. Данная работа посвящена отображению темы различных методологий управления IT проектами в телекоммуникационной области. Проектное управление – метод управления масштабными задачами в условиях временных и ресурсных ограничений для достижения заявленных результатов и поставленных целей. За все время существования проектного управления было создано немало эффективных подходов, методик и стандартов, которые можно взять на вооружение. О самых популярных из них мы и расскажем в данной статье.

Разработанные подходы сильно отличаются друг от друга. Они различаются по областям применения, детализированности, самодостаточности и формализации. Цель данной статьи — дать наиболее широкий обзор существующих в управлении проектами подходов и провести анализ какие из методологий больше всего подходят для телекоммуникационной отрасли.

Цели. Понять и предоставить результаты о том какие методологии больше всего подходят для реализации IT проектов. Ознакомить в целом с общими понятиями что такое IT-проектный менеджмент и для чего используют методологии. Комплексный анализ выбора наилучших методологий для работников телекоммуникационной отрасли. Предложение по использованию различных методологий.

Новизна исследования. Новизна исследования в том, что в данной статье исследовано 5 методологий, из которых каждый человек в праве выбрать наилучший вариант для своего IT-проекта.

Методологии. В ходе анализа были предложены 5 различных методологий в IT-проектном управлении: классический проектный менеджмент, Agile, Scrum, Lean, Kanban. Данные методологии берут свои истории с XX века и по сей день используются многими компаниями не только в IT сфере. Многие из них достаточно известные.

Классический проектный менеджмент - основной принцип этого подхода: чтобы решить задачу, ее нужно разбить на последовательные этапы. Этот метод применим для проектов, где ограничена последовательность задач.

В классическом менеджменте есть 5 основных этапов:

1. **Инициализация.** На этом этапе команда проводит «мозговой штурм», определяет требования к проекту и вид конечного продукта.
2. **Планирование.** Команда ставит цели, уточняет, какие должны быть результаты проекта. Определяется бюджет, формируется календарный план и оцениваются риски. На этом этапе также выявляются спонсоры и прочие заинтересованные стороны. Если этап планирования будет грамотно проведен, руководитель всегда будет в курсе количества ресурсов для работы.
3. **Разработка.** Эта стадия характерна для технологичных проектов. Для некоторых проектов она может быть совмещена со стадией планирования. Суть разработки в определении технических способов достижения цели. Например, языка программирования.
4. **Реализация и тестирование.** На этой фазе происходит работа по проекту на основе разработанного плана. Создается содержание плана и проводится контроль по выбранным метрикам. Затем проводится тестирование продукта, чтобы выявить и исправить недостатки. В первую очередь учитываются требования заказчика.
5. **Мониторинг и завершение проекта.** На этой фазе готовый продукт передается заказчику. Также возможны улучшения и изменения продукта по согласованию с заказчиком.

Следующая методология – **Agile** (agile software development, от англ. agile – проворный) – это семейство «гибких» подходов к разработке программного обеспечения. Такие подходы также иногда называют фреймворками или agile-методологиями.

Agile возник в IT-среде, но затем распространился и в другие сферы – от промышленной инженерии до искусственного интеллекта.

Смысл Agile сформулирован в Agile-манифесте разработки ПО: «Люди и взаимодействие важнее процессов и инструментов. Работающий продукт важнее исчерпывающей документации. Сотрудничество с заказчиком важнее согласования условий контракта. Готовность к изменениям важнее следования первоначальному плану».

Третья методология – **Scrum. Scrum – это «подход структуры».** Над каждым проектом работает универсальная команда специалистов, к которой присоединяется еще два человека: владелец продукта и scrum-мастер. Первый соединяет команду с заказчиком и следит за развитием проекта; это не

формальный руководитель команды, а скорее куратор. Второй помогает первому организовать бизнес-процесс: проводит общие собрания, решает бытовые проблемы, мотивирует команду и следит за соблюдением scrum-подхода.

Scrum-подход делит рабочий процесс на равные спринты – обычно это периоды от недели до месяца, в зависимости от проекта и команды. Перед спринтом формулируются задачи на данный спринт, в конце – обсуждаются результаты, а команда начинает новый спринт. Спринты очень удобно сравнивать между собой, что позволяет управлять эффективностью работы.

Четвертой возможной методологией является **Lean** — это набор принципов для оптимизации работы предприятия. Как она помогла Toyota? С помощью Lean Toyota довела все рабочие процессы до четкой стандартизации, а все лишнее — потери на предприятии — убрала. Такой подход в японской компании назывался «бережливое производство», то есть улучшение продуктивности на всех этапах производства без высоких затрат. В Lean процессы работы сосредоточены на конечной ценности компании (проданном товаре) и удалении тех действий, которые не создают дополнительной ценности. Чтобы провести тест и определить, что важно, а что нет, поставьте вопрос: «Помогает ли это действие быстрее прийти к конечной ценности?». Результат работы с Lean — сэкономленное время, которое позволит обработать большее количество заказов.

Последняя методология, которую мы разберем **Kanban – это «подход баланса».** Его задача – сбалансировать разных специалистов внутри команды и избежать ситуации, когда дизайнеры работают сутками, а разработчики жалуются на отсутствие новых задач.

Вся команда едина – в kanban нет ролей владельца продукта и scrum-мастера. Бизнес-процесс делится не на универсальные спринты, а на стадии выполнения конкретных задач: «Планируется», «Разрабатывается», «Тестируется», «Завершено» и др.

Главный показатель эффективности в kanban – это среднее время прохождения задачи по доске. Задача прошла быстро – команда работала продуктивно и слаженно. Задача затянулась – надо думать, на каком этапе и почему возникли задержки и чью работу надо оптимизировать.

В книге Пучков И. И. «**Управление IT-проектами**» было сказано следующее: «Есть различные способы, с помощью которых можно подходить к управлению проектами, и за последние 60 лет было разработано множество «методологий»,

«рамок» и «процессов». Некоторые из них имеют свое происхождение в академических исследованиях, в то время как другие выросли из собственных методов, разработанных организациями, которые имеют высокую проектную направленность, например управленческие консультации.

Agile (гибкие) методы определяют новую роль менеджера проекта по сравнению с традиционной. Вместо тщательного планирования деятельности в рамках проекта, менеджер проекта управляет короткими циклами разработки. Разработаны гибкие методы управления проектами для обработки изменяющегося вклада участников проекта в определение результатов проекта; это дополняется свободной структурой и формализацией рабочих задач, и сосредоточением внимания на быстрых и малых результатах. Согласно этому подходу гибкие методологии обеспечивают согласование результатов проекта с заинтересованными сторонами. ИТ-менеджеры проекта постоянно получают данные относительно действий и поведения участников проекта. Тем не менее, исследования показывают, что существует существенный разрыв между тем, как проблемы проявляются в проекте, и тем, что является актуальной проблемой. При этом руководители проектов, ориентируясь исключительно на решении возникающих проблемы и не пытаясь проследить причины, лежащие в основе проблем, рискуют направить усилия на устранении симптомов, а не на решение реальной проблемы.»

В статье про «**Топ-7 методов управления проектами: Agile, Scrum, Kanban, PRINCE2 и другие**» сказано следующее: «Управление проектами – это управление и организация всего, что нужно для достижения цели – вовремя и в рамках бюджета, конечно же. Будь до разработка нового программного обеспечения, проведение маркетинговой компании или высадка человека на Марс – проектное управление позволяет добиться успеха.

Все проекты разные. Не существует идеальной системы управления проектами, подходящей для каждого из видов проектов. Также не существует системы, которая бы подходила каждому руководителю и была удобна для всех членов команды. Однако за время существования проектного управления было создано немало эффективных подходов, методик и стандартов, которые можно взять на вооружение. О самых популярных из них мы сегодня и поговорим.

Разработанные подходы сильно отличаются друг от друга. Они различаются по областям применения, детализированности, самодостаточности и формализации.»

Задачи исследования. Провести опрос у сотрудников телекоммуникационной отрасли о том какие методологии они привыкли использовать**.** Проанализировать полученные данные и вывести свои варианты решения. Также после ознакомления с различными методологиями сотрудник телекоммуникационной отрасли вправе выбрать наиболее подходящую методология для своего проекта.

Результаты. Мною был проведен опросник среди коллег компании Kcell (проектные менеджеры, разработчики, дизайнеры, тестировщики). Результат опросника показал, что работникам телекоммуникационной отрасли удобнее работать с такими методологиями как: Agile, Scrum, Kanban. Также в своей презентации я построил подробный график с методологиями.

Выводы. Сделан вывод о том, что при начинании любого IT-проекта в первую очередь нужно понять для каких целей инициируется проект, какие у него сроки и количество участников команды. Выбор методологии лежит на плечах проектного менеджера и важно понимать, что нету плохой методологии. У каждой методологии свое применение, я лишь отобразил какие из них наиболее удобны в использовании. В мире используются различные методология помимо тех, что я указал. Те методологии, что я раскрыл часто встречающиеся в IT рынке.

Список литературы

1. Скотт Беркун. Книга «Сделано: Проектный менеджмент на практике».
2. Джефф Сазерленд. Книга «Scrum: Революционный метод управления проектами».
3. Пучков И. И. Книга «Управление IT-проектами».