С. ДЕМИРЕЛ АТЫНДАҒЫ УНИВЕРСИТЕТТІҢ ХАБАРШЫСЫ: ЖАРАТЫЛЫСТАНУ ЖӘНЕ ТЕХНИКАЛЫҚ ҒЫЛЫМДАР

SULEYMAN DEMIREL UNIVERSITY BULLETIN: NATURAL AND TECHNICAL SCIENCES

ҚАҢТАР-МАУСЫМ
JANUARY-JUNE

Қаскелең – Kaskelen, 2020

МАЗМҰНЫ

ЖАРАТЫЛЫСТАНУ ЖӘНЕ ТЕХНИКАЛЫҚ ҒЫЛЫМДАР

CONTENTS

NATURAL AND TECHNICAL SCIENCES

ЖАРАТЫЛЫСТАНУ ЖӘНЕ ТЕХНИКАЛЫҚ ҒЫЛЫМДАР
_____

NATURAL AND TECHNICAL SCIENCES

IRSTI 06.58.45

A. Zhumekeshov[1], A. Bogdanchikov[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

FORECASTING OIL PRODUCTION USING LSTM NETWORKS CONFINED TO DECLINE

Abstract. Natural resources are limited and very important in our industrial life and development. Oil is considered as the black gold and it is included in hundreds of industrial fields. Therefore, forecasting future oil production performance is an important aspect for oil industry. In this study, we proposed improvements to the existing deep learning model in order to overcome limitations associated with the original model. For evaluation purpose, proposed and original deep learning models were applied on a real case oil production data. The empirical results show that the proposed adjustments to the existing deep learning model achieves better forecasting accuracy.

Keywords: Oil Production Forecast, Long-Short Term Memory, Decline Curve Analysis.

***

Аңдатпа. Табиғи ресурстар шектеулі және біздің өндірістік өмірімізде және дамуымызда өте маңызды. Мұнай қара алтын болып саналады және ол жүздеген өнеркәсіпте паидалынады. Сондықтан мұнай өндірісінің болашақтағы көрсеткіштерін болжау мұнай саласы үшін маңызды аспект болып табылады. Осы зерттеуде біз түпнұсқа модельмен байланысты шектеулерді еңсеру үшін қолданыстағы терең оқыту моделін жетілдіруді ұсындық. Мұнай өндірісінің нақты деректерінде бағалау

мақсатында ұсынылған және түпнұсқалық терең оқыту модельдері қолданылды. Эмпирикалық нәтижелер қолданыстағы терең оқыту моделіне ұсынылған түзетулер болжамның дәлдігіне жететінін көрсетеді.

Түйін сөздер: Мұнай өндірісінің болжамы, ұзақ мерзімді жад, өндірістің төмендеу қисығын талдау.

<center>***</center>

Аннотация. Природные ресурсы ограничены и очень важны в нашей промышленной жизни и развитии. Нефть считается черным золотом и используется в сотнях промышленных областях. Поэтому прогнозирование будущих показателей добычи нефти является важным аспектом для нефтяной промышленности. В этом исследовании мы предложили усовершенствования существующей модели глубокого обучения, чтобы преодолеть ограничения, связанные с исходной моделью. Для целей оценки предложенные и оригинальные модели глубокого обучения были применены на реальных данных добычи нефти. Эмпирические результаты показывают, что предлагаемые корректировки существующей модели глубокого обучения обеспечивают лучшую точность прогнозирования.

Ключевые слова: Прогноз добычи нефти, долгая краткосрочная память, анализ кривой падения добычи.

Introduction

Until the middle of the XIX century oil was produced in small quantities, mainly from shallow wells near its natural outlets to the surface of the earth. Since the second half of the XIX century demand for oil began to increase due to the widespread use of steam engines and the development of other industries, which posed complex problem of future oil production pattern. Historical and most common approach in solving this problem is Decline Curve Analysis (DCA) [1]. By identifying decline rate, DCA extrapolates past production in order to estimate expected production in the future. The main limitation of this tool is the linear statistical approach, which generally produce a poor fit on historical production data. Hence, in order to improve fitting curve, more accurate nonlinear model is required.

In the last couple of decades, deep learning models have been widely used with non-stationary data prediction, like economics, weather, stock price, and retail sales. Similarly, several studies in predicting oil production using deep learning algorithms such as Long Short-Term Memory (LSTM) were completed. However, despite its performance, deep learning models are still in infancy stage and requires further analysis in using during oil production prediction.

In this paper, we analyzed application of the existing deep learning model [2] on a real case oil field data from the western part of Kazakhstan, and compared to the proposed model which is a combination of traditional DCA and deep learning models. Empirical results showed that latter model outperformed its counterparts.

Related Works

In [3] it was demonstrated that using increased depths of LSTM networks improve overall performance of time series forecasting. Encouraged by these results authors in [2] developed Deep LSTM (DLSTM) network with stacked three LSTM blocks one after another in Petroleum Production Forecasting (Figure 1: Architecture of DLSTM recurrent network). The paper empirically shows that proposed model outperforms some other algorithms such as ARIMA, NEA, RNN, DGRU in describing the nonlinear relationship of petroleum time series data.
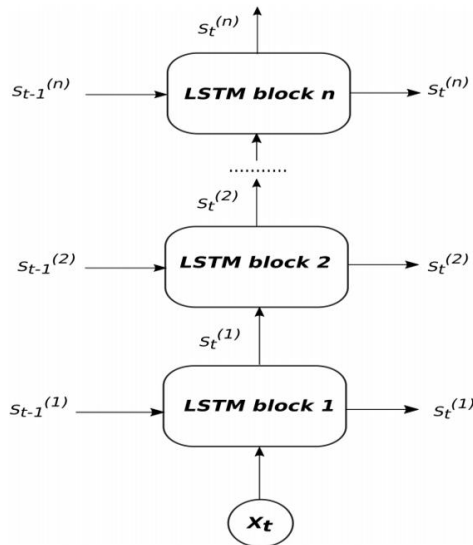
Figure 1: Architecture of DLSTM recurrent network

However, two major concerns of this model should be noticed. First one is an evaluation of a model accuracy using testing data set (original data is split into train and test sets). Authors created data batches using certain time lag period and predicted next time series data using the last batch from the dataset (Figure 2: Included evaluation approach). This is not the best approach in validating the model, since the assumption of using unseen data during the testing stage is not valid anymore. The second drawback of the proposed model is the fact that known trend of any oil production data, which is decline over the

time, is not captured in the model. This can result in unrealistic output over the long-term forecasting (Figure 3: DLSTM output results).
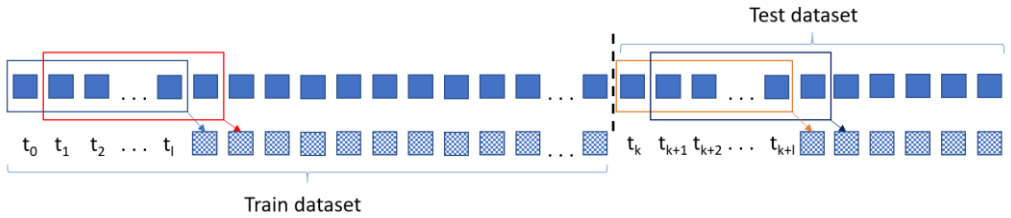
Figure 2: Included evaluation approach
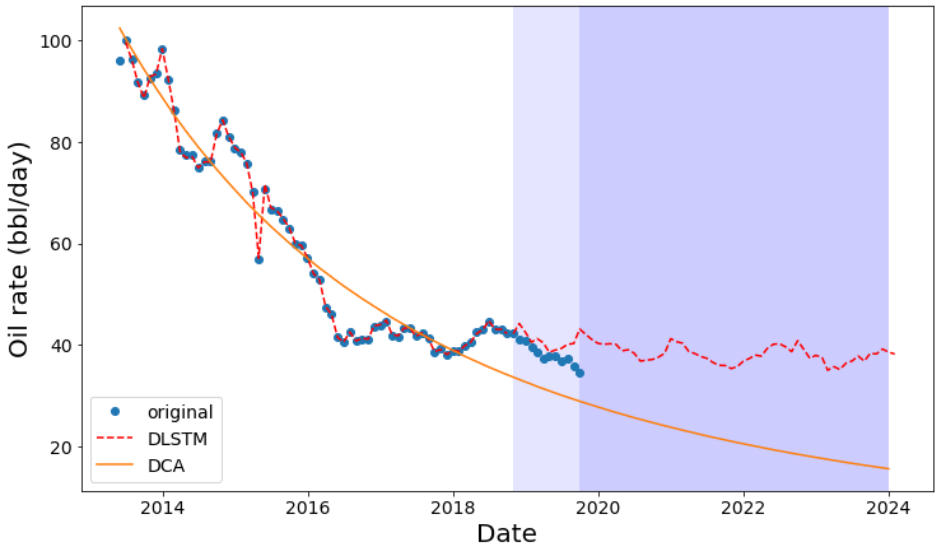
Figure 3: DLSTM output results

Proposed Model

The main reason why DLSTM Model fails in following decline trend is the fact that during removing the trend of historical production curve difference of consecutive data was applied. This approach does not constrain the general curve to decline over the time. In the proposed model, constrain to decline is achieved by taking the difference between production data and general exponential decline, and only then apply DLSTM model. Therefore, deviation of historical production data from general decline curve is modelled.

In addition to that, for making fair evaluation model accuracy was estimated using mismatch between unseen test data and pure predicted output as shown in the Figure 4: Proposed evaluation approach below.
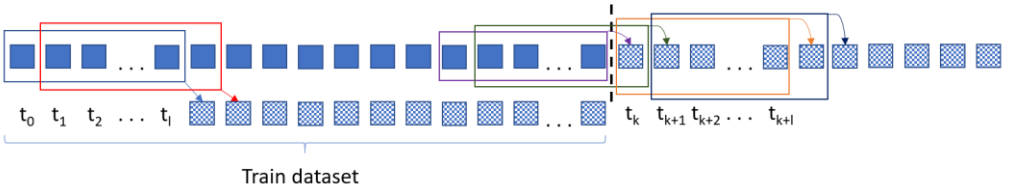
Figure 4: Proposed evaluation approach

Experimental Results

After de-trending historical production data using overall decline and applying DLSTM model explained in [2], it is possible to achieve better fit to the test datasets. At the same time, future predictions from DCA-DLSM model follow general trend of conventional decline pattern (Figure 5: Proposed DCA-DLSTM output results).
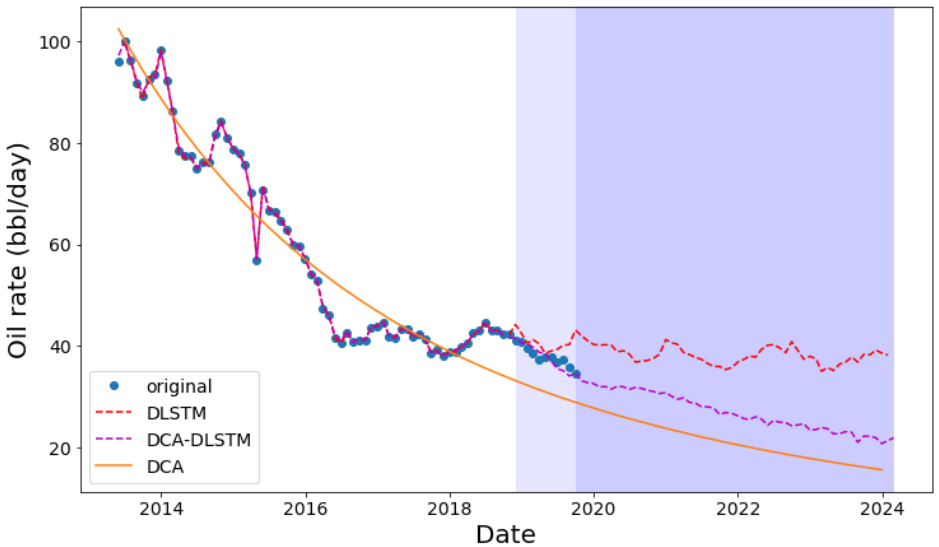
Figure 5: Proposed DCA-DLSTM output results

To control the learning process and evaluation accuracy of the proposed method, the root means square error (RMSE) was used. The RMSE is a frequently used measure of the differences between values (sample or population values) predicted by a model and the values observed [4]. It represents the square root of the second sample moment of the differences between predicted values and observed values or the quadratic mean of these differences.

$$E_{RMSE} = \sqrt{\frac{1}{n}\sum (y - \hat{y})^2}$$

Table 1: Forecasting accuracy

Forecasting Model	RMSE
DCA	5.8
DLSTM	3.65
DCA-DLSTM	**0.53**

As can be seen from the Table 1*: Forecasting accuracy*, in the assessment of oil production forecasting, the effectiveness of the DCA-DLSTM model is better than other algorithms.

Conclusion

In this paper we discussed existing experiments conducted using recurrent neural networks (DLSTM), which can capture the nonlinear relationship between the system's input and output labels. However, it is limited in controlling overall decline trend of the oil production time series data. Therefore, we developed better prediction model, which is based on combination of traditional DCA and described DLSTM. The results show that the accurate prediction and learning performance of proposed model outperformed its counterparts.

References

1 Production forecasting decline curve analysis, 2018. URL: https://petrowiki.org/Production_forecasting_decline_curve_analysis.

2 Sagheer, A., Kotb, M. Time Series Forecasting of Petroleum Production using Deep LSTM Recurrent Networks. *Neurocomputing,* 2018, pp. 203-213.

3 Hermans, M., Schrauwen, B. Training and Analysing Deep Recurrent Neural Networks. *26th International Conference on Neural Information Processing Systems,* (2013): pp. 1-9.

4 Root-mean-square deviation. URL: https://en.wikipedia.org/wiki/Root-mean-square_deviation.

5 Aizenberg, I., Sheremetev, L., Villa-Vargas, L. "Multilayer Neural Network with Multi-Valued Neurons in time series forecasting of oil production. *Neurocomputing*, 175 (2016): pp. 980-989.

7 Abdullayeva F., Imamverdiyev, Y. Development of Oil Production Forecasting Method based on Deep Learning. *International Academic Press*, 7 (2019): pp.826-839.

IRSTI 06.58.45

U. Sadyk[1], B. Cemal Adil[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

SUPERCONDUCTIVITY

Abstract. The aim of this article is to provide a general information about superconductors. Superconductivity is the weird phenomenon of zero electrical resistance that occurs when some materials are cooled below a critical temperature. To get cold enough liquid helium or nitrogen (often as low as -250 °C or -480 F) are used. This article primarily focuses on the history, the invention and the properties and the areas of usage of superconductors. The phenomena of superconductivity was first observed by Heike Kamerlingh Onnes in 1908 in Netherlands. Experimental physicists are now trying to find superconductors at room temperature. This article also intends to arouse curiosity among physics students.

Keywords: Superconductors, critical temperature, zero electrical resistance.

***

Аңдатпа. Осы мақаланың мақсаты суперөткізгіштер туралы жалпы ақпарат беру. Өткізгіштік дегеніміз - нөлдік электр кедергісінің таңқаларлық құбылысы, кейбір материалдар сыни температурадан төмен салқындаған кезде пайда болады. Салқын болу үшін сұйық гелий немесе азот қолданылады (көбінесе -250 ° C немесе -480 F). Бұл мақалада ең алдымен өткір өткізгіштердің тарихы, өнертабысы және қасиеттері мен қолдану салалары қарастырылған. Өткізгіштік құбылыстарын алғаш рет Хейк Камерлинг Оннес 1908 жылы Нидерландыда байқады. Эксперименттік физиктер қазір бөлме температурасында суперөткізгіштерді табуға тырысуда. Бұл мақала сонымен бірге физика пәні студенттерінің қызығушылығын тудырмақ.

Түйін сөздер: өткізгіштер, сыни температура, нөлдік электр кедергісі.

***

Аннотация. Целью данной статьи является предоставление общей информации о сверхпроводниках. Сверхпроводимость - это странное явление нулевого электрического сопротивления, которое возникает, когда некоторые материалы охлаждаются ниже критической температуры. Чтобы

получить достаточно холодный жидкий гелий или азот (часто до -250 ° С или -480 F). Эта статья в основном фокусируется на истории, изобретении, свойствах и областях использования сверхпроводников. Явление сверхпроводимости впервые наблюдал Хайке Камерлинг Оннес в 1908 году в Нидерландах. Физики-экспериментаторы сейчас пытаются найти сверхпроводники при комнатной температуре. Эта статья также намеревается вызвать любопытство среди студентов-физиков.

Ключевые слова: сверхпроводники, критическая температура, нулевое электрическое сопротивление.

Introduction

You plug the cable into the prize and run the device by passing the electrical current through the circuits. Sometimes you even work so hard, when it comes to your bill, it's like the world is crumbling.

In this article, we will examine the superconductors that shape the supreme electricity that shapes our lives. We will examine its history, where it is not used, its analysis and its physics. 103 years have an annual.

Superconductivity is the fact that the electrical resistance of some materials is zero below a certain temperature and they push the magnetic flux out. The history of superconductivity began when Dutch physicist Heike Kamerlingh Onnes discovered mercury superconductivity in 1911. Since then many other superconducting materials have been discovered and the theory of superconductivity has been developed. These issues remain active in the field of condensed matter physics.

Discovery of ultra-cold phenomenon (until 1908)

James Dewar started. Zygmunt Florenty Wroblewski conducted investigations of electrical properties at low temperatures, but his investigation was terminated due to the death of accident results. In 1864, Karol Olszewski and Wroblewski predicted the phenomenon of electricity as resistance levels dropped at ultra-cold temperatures. According to this case Olszewski and Wroblewski evidence was revealed in 1880.

Dewar and John Ambrose Fleming, pure metals can become excellent electromagnetic conductors at absolute zero (later, Dewar changed his mind, eliminating resistance, believing that a piece of conductivity would exist in his time). Walther Hermann Nernst developed the third law of thermodynamics and states that absolute zero is inaccessible. Carl von Linde and William Hampson are both commercial researchers. Linde's patent has been the turning point in a 20-year systematic investigation of proven cases in the regenerative reverse linkage region. Hampson's designs were also a regenerative method. History as a liquefaction method in Hampson-Linde [1].

Onnes bought a Linde machine for his research. On 21 March 1900, a US patent was issued to Nikola Tesla for the method of increasing the intensity of electrical emissions by lowering the temperature caused by low resistance, a phenomenon previously observed by Olszewski and Wroblewski. This patent describes the increased intensity and duration of electrical oscillations of a low temperature resonance circuit. Tesla is believed to intend to use Linde's machine to obtain refrigerant.

On July 10, 1908, Heike Kamerlingh Onnes was the first to produce liquefied helium at the University of Leiden, the Netherlands with a boiling point of 4.2 kelvin at atmospheric pressure.

0 degrees Kelvin = -273 degrees Celsius

0K = -273oC

Heike Kamerlingh Onnes and Jacob Clay re-examined Dewar's earlier experiments on lowering resistance at low temperatures. Onnes began his study with platinum and gold, then replaced them with mercury. Onnes' research on the resistance of solid mercury at cryogenic temperatures was achieved by the use of liquid helium as a coolant. On April 8, 1911, at 16:00, Onnes dropped the note "Kwik nagenoeg nul "which could be translated as mercury resistance is almost zero. Onnes observed that the resistance suddenly disappeared at a temperature of 4.19 K. Onnes discovered his research in 1911 in an article entitled "About the sudden speed at which mercury resistance disappears". In this article Onnes said that "resistivity amount is thousands of times lower in quantity than the best conductor at the usual temperature. Onnes then reversed the process and found that resistance to 4.2 K'da returned to matter. The following year, Onnes published more articles on this phenomenon. Initially, Onnes called this phenomenon "supra-conductivity" (1913), and only later, he adopted the term "superconductivity". Onnes received the Nobel Prize in Physics in 1913 for his research.

In 1912, Onnes conducted an experiment on the usability of superconductivity. Onnes gave an electric current to a superconducting ring and removed the battery that produced it. When Onnes measured the electric current, he found that his intensity did not disappear over time. The current was continuous due to the superconducting state of the conductive medium. In later years, superconductivity was also found in many other substances. In 1913, the

lead was found to be superconducting at 7 K, and in 1941, niobium nitride was found to be superconducting at 16 K.

Features

Superconducting materials have very important basic features that make it technologically prominent. First of all, they show zero resistance to electrically correct current (d.c.) and have a very high current carrying capacity compared to normal conductors.

These properties have an important place in the transport, storage, production of strong magnets, generators and the production of sensitive electrical devices.

Extremely low resistance at high frequencies, very low signal distribution and the ability to carry signals at speeds almost close to the speed of light are important for communication, military purposes (defense industry) and microwave technologies. The fact that they transmit electrical current without resistance / loss and show very low resistance even at high frequencies eliminates the problem of heating on circuit elements or wider circuits / devices.

For normal metals, T (K) = 0 $\rho = \rho 0$, while in superconductors, T superconducting materials have very important properties such as electrical properties in terms of magnetic properties. For example, their high sensitivity to magnetic field and their ability to give 1000 times more accurate results compared to conventional magnetic field detectors and similar measuring systems are extremely important applications for today's technology. Another important feature is that they easily exclude even high magnetic fields applied from outside.

Used areas

High energy physics

Since high magnetic flux density can be achieved by superconductors, magnetic resonance imaging (MRI) devices, commonly known as absorption, have been developed and a significant distance has been achieved in the field of medical diagnostics.

Superconducting cables

1000 KW and 10 GVA, such as the production of high-capacity power transmission cables, which have never been imaginable, have been realized. Since these cables are still very fragile, scientific research continues.

Railway transportation

MEGLAV trains moving through the strong magnetic field obtained by superconductors have been developed.

Particulate flashers

In the particle colliders used in particle physics experiments, strong magnets are required to keep subatomic particles moving at speeds close to the

speed of light connected to the center, but can be made only with superconductors. Advanced level experiments can be performed.

Electronic circuits

In almost all electronic circuits and especially integrated circuits, the problems caused by the resistances of the conductors used in the interconnections are an important cost factor.

From partıcle accelerator to an nanorobot

Here, an example of the contribution of superconductors to the development of experimental facilities in scientific research, which has an important place among the various application areas, should be given. Table 1 gives the temperature values required for some materials to be superconducting.

Table 1. Temperature values for superconducting

Material	T_c
Gallium	1.1K
Aluminum	1.2 K
Indium	3.4 K
Tin	3.7 K
Mercury	4.2 K
Lead	7.2 K
Niobium	9.3 K
La-Ba-Cu-oxide	17.9 K
Y-Ba-Cu-oxide	92 K
Tl-Ba-Cu-oxide	125 K

References

1 Superconductivity. URL: https://en.wikipedia.org/wiki/Superconductivity.
2 Temel özellikler. URL: http://cesur.ankara.edu.tr/superiletkenlik-hakkinda/temel-ozellikler/.
3 Ocak, E.M. – Süperiletkenlik nedir? URL: http://www.bilimgenc.tubitak.gov.tr/makale/superiletkenlik-nedir.

4   Arwen, A-süperiletkenlerin kullanım alanları nelerdir? URL: https://www.delinetciler.net/showthread.php?t=94090https://tr.wiki pedia.org/wiki/S%C3%BCperiletkenlik_tarihi - 2010/03/26.

M. Urmanov[1], M. Alimanova[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

TRAINING A SINGLE MACHINE LEARNING AGENT USING REINFORCEMENT LEARNING AND IMITATION LEARNING METHODS IN UNITY ENVIRONMENT

Abstract. This paper provides a research of Unity plugin that helps to develop Machine Learning Agents within Unity engine environment. This work introduces training a single Machine Learning Agent using both Reinforcement Learning and Imitation Learning methods, comparing the results and effectiveness.

Keywords: Computer Science, Game Development, Artificial Intelligence, Machine Learning, Unity.

***

Аңдатпа. Бұл мақала Unity үшін плагинді зерттеу ұсынады, ол қозғалтқыш ортасының ішінде машина оқыту агенттерін дамытуға көмектеседі. Бұл жұмыс екі әдісті пайдалана отырып, машиналық оқытудың жеке агентін оқыту, Нығайту және Имитацияны оқыту, нәтижелер мен тиімділікті салыстыруды ұсынады.

Түйін сөздер: Информатика, Ойын Дамыту, Жасанды Интеллект, Машинамен Оқыту, Unity.

***

Аннотация. Эта статья предоставляет исследование плагина для Unity, который помогает разрабатывать Агентов Машинного Обучения внутри среды движка Unity. Эта работа предоставляет тренировку единичного Агента Машинного Обучения, используя оба метода, Обучения с Подкреплением и Обучения Имитацией, сравнение результатов и эффективность.

Ключевые слова: Информатика, Разработка Игр, Искусственный Интеллект, Машинное Обучение, Unity.

Introduction

Since the making of computer games, the artificial intelligence development improvement issue, which would make games all the more fascinating to play, has consistently been important. Regularly artificial

intelligence was sub-par compared to players in abilities, so computer games turned out to be unreasonably straightforward for them. For this situation, the game developers, as a rule, turned to different stunts to change the powers of a human and a computer rival. In cases when we are discussing a racing simulation, at that point, the alleged "catchup" word is used. The attributes of a car controlled by a computer are artificially exaggerated. Subsequently, paying little heed to how handy the player is, the computer can play with him as an equivalent. Another case - RTS genre games, where the computer is helped by additional resources. But such solutions seem to be a cheat and reject the player. That is the reason online games are so mainstream, since playing with a genuine individual is significantly more interesting. In this manner, the issue is the amazingly low or absurd degree of insight of computer rivals, which is the second rate compared to the human. With the help of Machine Learning, it will take care of this issue and significantly grow the abilities of AI in games. One of the most popular researches on this subject is the paper of DeepMind Technologies workers. Using Q-Learning [1], they figured out how to actualize a calculation fit for playing straightforward Atari 2600 computer games without knowing anything about them, aside from the pixels on the screen [2]. In the event that more data is given to the neural system (such as, the directions of game objects), the use of AI grows. Getting data about the condition of the game world is a genuinely basic task if the neural network is designed for a game with AI, which suggests the presence of game sources, rather than the work with Atari games. In this work, the development and training ML agent, which is able to control character in a three-dimensional Unity environment, will be considered. The agent's tasks include maneuvering to avoid enemy traditional AI and getting to the aim area.
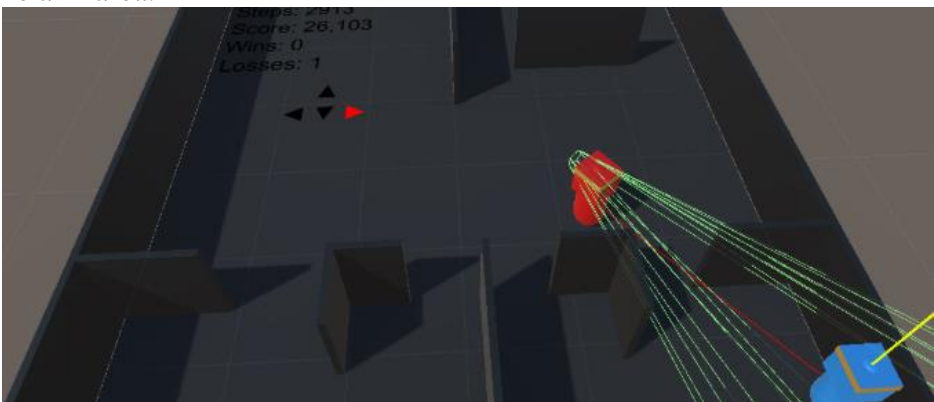
Fig. 1: The ML Agent is in the field of view and line of sight of the AI, and is being pursued.

Background

The Unity game engine was chosen as a tool for the development of a learning environment. To train agents The Unity Machine Learning Agents Toolkit (ML-Agents) [3] was used. For learning, two methods will be used one after another: Reinforcement Learning and Imitation Learning.

Reinforcement Learning

The principle thought of Reinforcement Learning is that the t-agent exists in a specific S-environment. Whenever the agent may process an action (or more than one action) from the arrangement of A-actions. Because of this action, the environment changes its state and the agent gets the r-reward[4]. In light of this cooperation with the environment, the agent must pick the ideal solution that boosts its reward. Reinforcement Learning is particularly useful for taking care of issues related to a decision between long-term and short-term profits. It has been effectively applied in different fields, for example, robotics, media communications, lift management. Likewise, Reinforcement Learning is a decent method to create AI in games. On account of games, the game character goes about as an agent and his general surroundings and his enemies go about as an environment. Each time the character plays out an action that approximates him to win, he gets a fortifying reward. For instance, the car agent on a dashing track gets a reward after some time if the separation to the finish line is decreased. This works in the same logic otherwise - when performing ineffective actions, the agent gets a punishment. All together for the agent to perform effective actions, it is fundamental for him to get a variety of data describing the condition of the environment. The measure of this data ought to be sufficient to guarantee that the operator gets all the vital data about the environment, yet not be unreasonably huge for the agent to train all the more effectively. Additionally, it is important to normalize the data, so the estimations of the signals showing up to the agent were inside the range of [0; 1] or [-1; 1]. There are examples of the input signal for a car like speed and position on the track. A list of action signals would be resulted out of the agent's work. Just as input signals, they require normalization. For example, the input signal for a car could be [0; 1] for the gas pedal and [-1; 1] for the steering.

Figure 2: The Reinforcement Learning cycle

Imitation Learning

Unlike Reinforcement Learning, which processes with a reward/punishment system, Imitation Learning uses a framework dependent on the cooperation between a Teacher agent that executes the task and a Student agent that imitates the teacher. This is helpful in cases where you don't need your AI to have machine-like flawlessness, yet you need your agent to act like a real human being [5]. Imitation Learning Support was introduced in ML-Agents v0.3 Beta. This tool component is a ground-breaking feature that facilitates the development of a complex AI using fewer resources. All things considered, the procedure of AI development proceeds like this: there are two agents, one is a Teacher and another is a Student. Another neural network, a real person or a deterministic algorithm may go as a Teacher. The most effective outcomes are accomplished if the Teacher is a human being. Next, the learning procedure starts. The Teacher plays for some time. The planning shifts relying upon the task difficulty. For easier tasks, it takes around 4-6 minutes. For complex tasks, it is required about 2 hours. The learning is that while the Teacher agent plays, and the Student watches his activities and tries to imitate its Teacher.

Hide and Escape Scenarios

In the first two versions of the environment scenario, the goal for the agent was to avoid being captured by the traditional AI. The reward was calculated by how many seconds the agent would manage to avoid the traditional AI. And in order to enhance learning speed, there were nine parallel environments with nine agents that trained simultaneously. After performing 3

million attempts in the first scenario progress of avoiding continuality occurred. But it was inconsistent and by the time there were still cases when the agent would be captured too fast. After testing some values of parameters in the curriculum, increasing buffer size twice, there were improvements in the learning, and results were more effective than in the first scenario, but still, it had flaws and inconsistent reward curve after the same 3 million attempts. Then a new approach of training was decided to perform. There was a problem that it never is possible to avoid the traditional AI indefinitely in a closed area like our environment. And even if the agent could eventually train to avoid indefinitely it meant that there was no win condition for the environment. It was decided that an agent should have an endpoint and the win condition. In this scenario, the reward was calculated by 10 minus how many seconds it took for the agent to reach the aim area. The expected result was achieved after the same 3 million attempts the agent could reach the aim area in less than a second [6].
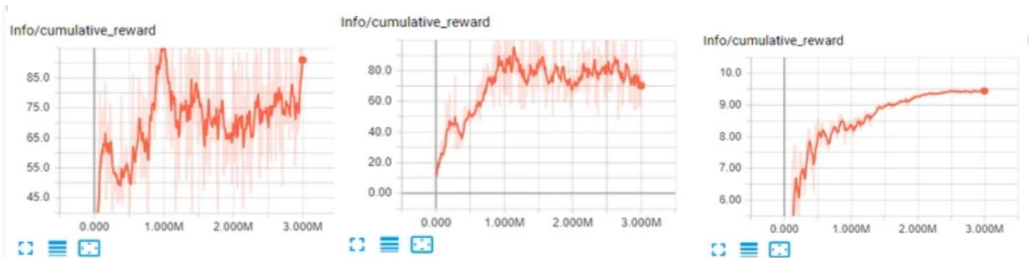
Figure 3: Reward graph of Hide, Hide2 and Escape scenarios

Human Escape Scenario

After we reached sufficient results by using Reinforcement Learning it was time for the next step which is applying Imitation Learning to training ML agent in the same environment. Although the controls for the environment were super simple it was very time consuming to record enough data for upcoming calculations. Also, a flaw occurred in the behavior of a human being since the aim area is randomly placed in the environment, including the character and traditional AI, after each attempt. It took some time for a real person to detect its aim area and the position of the character. While the agent would know the environment state in the first frame of the attempt. And because of this, the best result that the agent would achieve after applying Reinforcement Learning was a little less than 2 seconds, which is three times more than the result of Escape scenario. But in this scenario, the agent manages to behave like a real person and if this result is expected by the developers, then one second is not that important comparing to the realism.

Comparing the methods

Comparing two methods of learning is difficult since they achieve different results and behaviors. And the intersection results may only occur for early training which may be random and not satisfactory. It is obvious that Imitation Learning approach consumed more time to perform due to recording realtime human behavior which also consumes human resources more. If the developers seek the most effective results then Reinforcement Learning method will be more preferable. And if their intentions are to develop an AI that is close to human behavior, then Imitation Learning method is the best choice. However in both approaches there were some cases when even after 3 million steps of learning, the agent was able to reach the point only when the traditional AI is gone in a very long distance. And as the traditional AI patrols the environment randomly, there were cases, when the agent was waiting unnecessarily for a long time. That happened because the agent does not consider barriers in his path like walls and also he does not consider the direction of the traditional AI.

Conclusion

This study explores the opportunities and benefits of single use of Reinforcement Leaning and simultaneous use of Reinforcement Learning and Imitation Learning in artificial intelligence development for video games. Tools for creating the Learning Environment and learning AI agents have been considered. Practical recommendations, allowing to optimize the parameters and characteristics of the neural network and to conduct more effective training, were given. In the final result, a video game agent, which controls the character, effectively uses the available game mechanics and whose behavior is similar to a human, was created and trained. And also a video game agent who shows the most effective result was developed and trained.

References

1   Volodymyr, M., Puigdomenech, A.B., Mehdi, M., Graves, A., Timothy, P., Lillicrap, T.H., Silver, D., Kavukcuoglu, K. Asynchronous methods for deep reinforcement learning. arXiv preprint arXiv:1602.01783, 2016.

2   Bellemare, M.G., Naddaf, Y., Veness, J., Bowling, M. The Arcade Learning Environment: An evaluation platform for general agents. *J. Artif. Intell. Res.,* 47 (2013): pp. 253–279.

3   Juliani, A., Berges, V., Vckay, E., Gao, Y., Henry, H., Mattar, M., Lange, D. (2018). Unity: A General Platform for Intelligent Agents. arXiv preprint arXiv:1809.02627. URL: https://github.com/Unity-Technologies/ml-agents.

4   Gupta, A., Devin, C., Liu, Y.X., Abbeel, P., Levine, S. Learning invariant feature spaces to transfer skills with reinforcement learning. *In Int. Conf. on Learning Representations (ICLR),* (2017): pp. 1-14.

5   Englert, P., Paraschos, A., Peters, J., Deisenroth, M.P. Model-based Imitation Learning by Probabilistic Trajectory Matching. *Proceedings of the International Conference on Robotics and Automation,* (2013): pp.1-6.

6   Urmanov, M., Alimanova, M., Nurkey, A. Training Unity Machine Learning Agents using reinforcement learning method, *2019 15th International Conference on Electronics, Computer and Computation (ICECCO),* Abuja, Nigeria, (2019): pp. 1-4.

G. Assanbayeva[1], Sh. Kadyrov[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

PRINCIPAL COMPONENT ANALYSIS AND A MULTILINGUAL CONSTRUCT TO DETERMINE THE UNDERGRADUATE MAJOR SELECTION FACTORS

Abstract. In this article, we review mathematics behind well-known Principal Component Analysis from Linear Algebra implemented in various applied fields. As an application, we develop a construct to measure factors that affect college students in their major selection. This is a multilingual construct given in three languages, namely Kazakh, Russian, and English. To this end, we prepare a survey consisting of 27 Likert scale items in three languages and it is conducted among 314 undergraduate students in Kazakhstan. For dimensionality reduction, Principal Component Analysis is carried in python programming language which resulted in 9 major scales with only 22 elements. The overall reliability of the test is calculated to be 0,856. The nine scales are the effect of Uniform National Testing, state grant affect, personal interest affect, skills affect, occupation salary affect, teacher affect, external affect, university cost affect, parent's affect.

Keywords: Principal Component Analysis, Factor Analysis, Varimax rotation, Reliability, Major selection, Construct.

***

Аңдатпа. Бұл мақалада біз әртүрлі қолданбалы салаларда енгізілген сызықтық алгебрадан белгілі негізгі компонентті талдаудың артындағы математиканы қарастырамыз. Бағдарлама ретінде біз университет студенттеріне негізгі мамандық таңдау кезінде әсер ететін факторларды өлшейтін сауалнама жасаймыз. Бұл үш тілде, атап айтқанда қазақ, орыс және ағылшын тілдерінде берілген көптілді сауалнама. Осы мақсатта авторлар үш тілде 27 Likert шкаласынан тұратын сауалнама дайындады және ол Қазақстандағы 314 студенттер арасында өткізілді. Өлшемділікті төмендету үшін негізгі компоненттік талдау Python арқылы есептелінді, нәтижесінде 22 негізгі элементтерден тұратын 9 ірі компоненттер алынды. Тесттің жалпы сенімділігі 0,856 құрайды. Тоғыз шкалалар: ұлттық тестілеу нәтижесі әсері, мемлекеттік грант нәтижесі,жеке қызығушылық әсері,өз

қабілетінің әсері, мамандықтың жалақысы әсері, мұғалімнің әсері, сыртқы әсер, университеттің құнынының әсері,ата-ананың әсері.

Түйін сөздер: Негізгі компоненттік әдіс, факторлық әдіс, варимакс айналымы, сенімділік, мамандық таңдау, құрастыру.

<center>***</center>

Аннотация. В этой статье мы рассматриваем математику, лежащую в основе хорошо известного анализа главных компонентов из линейной алгебры, реализуемой в различных прикладных областях. В качестве приложения мы разрабатываем конструкцию для измерения факторов, влияющих на студентов университета в их главном выборе. Это многоязычная конструкция, представленная на трех языках, а именно на казахском, русском и английском. С этой целью авторы подготовили опрос, состоящий из 27 пунктов шкалы Лайкерта на трех языках, и он был проведен среди 314 студентов бакалавриата Казахстана. Для уменьшения размерности был проведен анализ главных компонент в python, который привел к 9 основным масштабам с только 22 элементами. Общая достоверность испытания, по расчетам, составляет 0,856. Девять шкал: влияние единого национального тестирования, влияние личного интереса, влияние государственного гранта, влияние заработной платы по профессии, влияние навыков, влияние преподавателя, влияние внешних факторов, влияние стоимости университета, влияние родителей.

Ключевые слова: анализ главных компонент, факторный анализ, Варимакс - вращение, достоверность, выбор специализации, построение.

1. Introduction

Linear algebra is a branch of mathematics that deals with system of linear equations, vector spaces, linear maps and their properties. Matrices are one of the building blocks of linear algebra. A numerical data consisting of m cases and n variable entries for each case can be thought of as $m \times n$ matrix. This representation enables us to carry various manipulations available to us from linear algebra and interpret the results. When n is large, it often becomes difficult to derive meaningful conclusions from the data. Principal Component Analysis (PCA) is one of the widely used techniques from linear algebra that helps with dimensionality reduction and makes it possible to extract hidden features of the data (Sanguansat, 2012). Even though this is a century old method invented by K. Pearson (Pearson, 1901), in its original form and in improved versions it is still being used nowadays for handling various large datasets. Some of the research areas where PCA is used include signal processing (Turan, et al., 2018),

genetics (Li, et al., 2019), quantitative finance (Avellaneda, et al., 2010), neuroscience (Subasi, et al., 2010), and questionnaire development (Brown, 2010).

Our goal in this article is to review mathematics behind this powerful tool and show how it can be applied in developing a construct that measures factors influencing students' major selection. There are various questionnaires are used in the literature to analyse factors related to major selection. Factors such as Interest in major, Peer pressure, Family pressure, Academic ability, Major's reputation, Job availability, Job salary, Major's prestige, Public sector job, Private sector job were analyzed in (Aldosary, et al., 1996) from 447 students of King Fahd university and Job availability, Salary, social status and prestige were found to be the main affecting factors in that order. Another study was carried with 111 participants to investigate college students' academic major declaration (Galotti, 1999). An exploratory factor analysis was carried by Sarwar et al, (2015) to analyse the variables affecting the specialization selection of 300 business graduates in Lahore resulting 6 main factors: academic factors, social capital factors, future prospect factors, human capital factors, market demand factors and finally job prospect factors. This 31-item construct is calculated to have high reliability of 0.845. Another study was carried (Fizer, 2013) at the University of Tennessee, Martin to determine the variables that influence agriculture students' choices in deciding their career path. The findings show that the main variable (22%) is family influence followed by a factor "a career that is personally rewarding" (21%).

In the next section, we provide the methodology used to develop our construct. More specifically, we will brief on the participants and the questionnaire conducted, and review the background information needed to understand PCA methodology. The section 3 contains the application of PCA to extract main factors via dimensionality reduction. The paper ends with discussion and conclusion section where we interpret our findings and highlight the possible future research directions.

2. Methodology
1.1. Participants and questionnaire

The main purpose of this study is an attempt to reduce the number of factors and define main aspects of the resulted construct. The survey is prepared by using various sources like (Singh Swapnika), (Sarwar, et al., 2015) and adapted to the context of Kazakhstan. An online survey questionnaire is consisting 27 questions. The survey is prepared languages,namely Kazakh, Russian, and English and send out to students from 16 universities within the country and

received 314 students participants. Students took as a sample through non probability convenience sampling technique.First part of questionnaire is directed to collect demographic data and items related to major selection were in the second part of the survey. Table 1 provides demographic information on participants. The number of respondents in the Kazakh language is 109,in Russian 93 and in English 112.

Table 1

Language	Age group	Gender	University GPA
Kazakh	16-18y	Male	3.5-4.0
34.7%	18.5%	45.9%	43.3%
Russian	19-21y	Female	2.5-3.4
29.6%	42.7%	54.1%	46.2%
English	22-24y		1.5-2.4
35.7%	25.1%		9.55%
	24-more		1.0-1.4
	13.7%		0,95%

Most respondents are between 19-21 years old students. They took 42.7% (134 students) from total. However, 24 years or older than 24 years are 13.7% from 314 students. Students of the engineering speciality took part in the survey by 21.3% (67students) and it is the highest frequency of respondents. Then comes students majoring in pedagogy and mathematics with 20% (63 students). The minimum size of the surveyed participants are attended by journalists and fine and applied art. They took only 1% (3 students from each).

Figure 1. Major distribution of participants
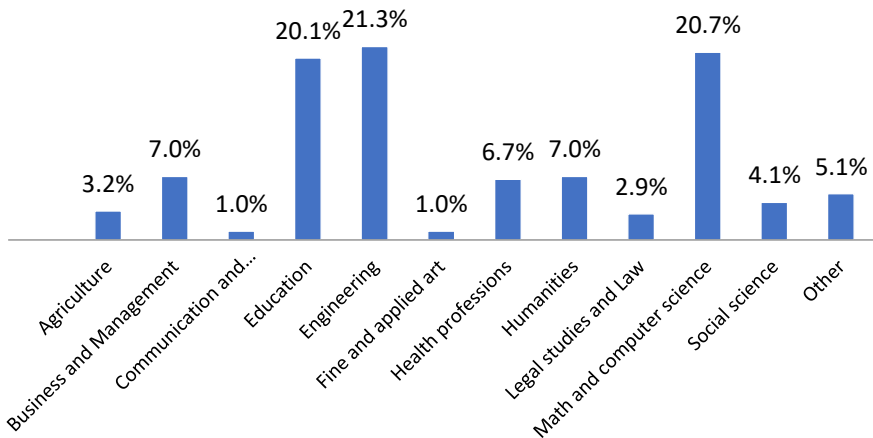
Figure 2 provides information about the number of students surveyed by more than 16 universities. The majority of respondents are students of SDU university.Number of participants from SDU is 197.In the second is KazNu with 28 participants, and the NU with 22. Small number of students from different universities are counted as a one group with 26% from total.

Figure 2.University
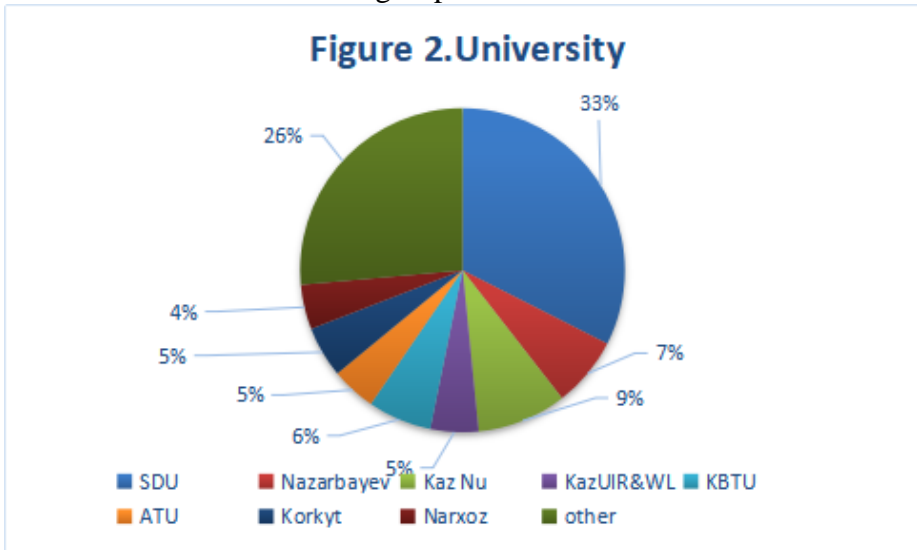
1.2. Instruments

Participants answered to questions by online form. Responses are evaluated using the Likert Scale. Items are graded from 1 to 5 points. Accordingly, 1-'strongly disagree', 2-'disagree', 3-'neutral',4-'agree',5-'strongly disagree'. The answers are translated into Kazakh and Russian languages accordingly with this grading system.

In order to check the internal consistency of scale items, Chronbach alpha reliability analysis is performed.

For dimensionality reduction factor analysis through Principal Component Analysis is implemented with Varimax rotation. The Kaiser-Meyer Olkin sampling Adequacy index is a figure showing the proportion of variation in your variables that could be caused by underlying factors.

Scree plot is used to plot eigenvalues of a data and to determine the number of factors of principal components. By using the rotation methods such as VARIMAX, we have additional tools which make easier the interpretation of the factors, and which can thus improve the relevance of the results.

1.3. Principal Component Analysis

Principal component analysis (PCA) is a technique that is useful for the compression and classification of data variables. The goal is to reduce the

dimensionality of a data set (sample) by grouping the intercorrelated variables , possibly obtaining smaller than the original set of variables, that nonetheless retains most of the sample's information. A PCA is an application of linear algebra where one rotates and shifts the coordinate axes to obtain more suitable representation of data helpful for feature extraction one that presents important information. PCA requires a small background of linear algebra. So, we now discuss some basic concepts of linear algebra, in particular algebra (Lindsay, 2002) used to apply in PCA.

  Basic Linear Algebra Review:

Eigenvectors and eigenvalues are important properties of matrices that are fundamental to PCA.

Definition 1. Let A be an $n \times n$ real matrix. A complex number λ is called an *eigenvalue* of a matrix A if there exists an n *dimensional* non-zero complex vector $\vec{x}$, called an *eigenvector,* such that

$$A\vec{x} = \lambda\vec{x}.$$

To determine eigenvalues one needs to solve the characteristic equation:

$$D(\lambda) = \det(A - \lambda I)$$

By solving the equation for λ, we will have eigenvalues $\lambda_1, \lambda_2...$ .By substituting $\lambda's$ into the vector equation, we can obtain eigenvectors.

Eigenvectors belonging to different eigenvalues are easily seen to be linearly independent. If a matrix is symmetric then in fact distinct eigenvectors are mutually orthogonal. We now make these notions more clearer. Orthogonality is important because it means that you can express the data in terms of these perpendicular eigenvectors, instead of expressing them in terms of the x and y axes. We will be doing this later (Lindsay, 2002).

Definition 2 : A $m \times n$ matrix $A = [a_1, a_2......a_n]$ is said to be orthogonal:

$$a_i^T a_j = \left\{ \begin{array}{l} 1 \quad if\ i = j \\ 0\ otherwise \end{array} \right.$$

where each $a_i, i = 1,2,3...,n$ is a column vector of m rows.

Theorem 1: The inverse of an orthogonal matrix is it's transpose (Shlens, 2014).

Definition 3 : A $m \times m$ square matrix A is said to be symmetric if $A_{ij} = A_{ji}$, i.e., row index and column index are interchangeable: $A^T = A$.

Theorem 2: For any $m \times n$ matrix of real numbers A ,m x m matrix $A^T A$ and the n x n matrix AA^T are symmetric (Shlens, 2014).

Proof :

Let's take the transposes of AA^T .We apply properties of transpose operation. Then:

$$(AA^T)^T = A^{TT} A^T = AA^T$$

We repeat this analysis for $A^T A$:

$$(A^T A)^T = A^T A^{TT} = A^T A$$

Definition 4: A matrix A is said to be diagonalizable if there exists some E such that $A = EDE^T$, where D is a diagonal matrix and E is some special matrix that diagonalizes A. Additionally, if E is orthogonal, then A is said to be orthogonally diagonalizable .

Theorem 3: A matrix is symmetric if it is orthogonally diagonalizable (Shlens, 2014).

Proof: Suppose *A* is orthogonally diagonalizable. Let us compute A^T.

$$A^T = (EDE^T)^T = E^{TT} D^T E^T = EDE^T = A.$$

Hence, if A is orthogonally diagonalizable, it must also be symmetric

Theorem 4: If A is symmetric (meaning $A^T = A$), then A is orthogonally diagonalizable and has only real eigenvalues. In other words, there exist real numbers $\lambda_1 ... \lambda_n$(the eigenvalues) and orthogonal, non-zero real vectors $\overrightarrow{v_1} ... ... \overrightarrow{v_n}$(the eigenvectors) such that for each $i = 1,2......n$. (Jauregui, 2012):

$$A\overrightarrow{v_i} = \lambda_i \overrightarrow{v_i}$$

Let A be a square n × n symmetric matrix with associated eigenvectors $\{e_i\}_{i=1}^n$

$$\text{and } E = [e_1............e_n].$$

Then:

Theorem 5: A symmetric matrix *A* is diagonalized by a matrix of its orthonormal eigenvectors (Shlens, 2014).

Proof: This theorem asserts that there exists a diagonal matrix *D* such that $A = EDE^T$. Let *A* be any matrix, not necessarily symmetric, and let it have independent eigenvectors e_i (i.e. no degeneracy).

$$AE = [Ae_1............Ae_n] = [\lambda_1 e_1.........\lambda_n n] = ED.$$

Since $AE = ED$, it follows that $A = EDE^{-1}$.

Calculation of PCA:

Step 1. Get some data

Suppose we take *n* individuals, and on each of them we measure the same *m* variables. In this case, we say that we have *n* samples of m-dimensional data. For the $i-th$ individual, record the m measurements as a vector $\overrightarrow{x_i}$ belonging to R^m (Jauregui, 2012).

Step 2. Subtract the mean

Using notation from Step 1, we can store the mean of all m variables as a single vector in R^m:

$$\bar{\mu} = \frac{1}{n}(\vec{x_1} + \cdots + \vec{x_n})$$

For PCA to work properly, you should standardize the dataset.The mean subtracted is the average across each dimension. It is common 're-centering' the data so that the mean is zero. It is working by subtracting mean $\bar{\mu}$ from each sample vector $\vec{x_i}$. Let A be the *m* x *n* matrix whose *i-th* column is $\vec{x_i} - \bar{\mu}$ (Jauregui, 2012):

$$A = [\vec{x_1} - \bar{\mu}]...[\vec{x_i} - \bar{\mu}]$$

Then define covariance matrix.

Step 3. Calculate the covariance matrix

In mathematics and statistics, covariance is a measure of the relationship between two random variables.Covariance is a measure of how changes in one variable are associated with changes in a second variable. Covariance is always measured between 2 dimensions. If you calculate the covariance between one dimension and itself, you get the variance. So, if you had a 3-dimensional data set (x, y, z) , then you could measure the $m \times n$ covariance between the *x* and *y* dimensions, the *x* and *z* dimensions, and the *y* and *z* dimensions. In fact, for an n-dimensional data set, you can calculate $\frac{n!}{(n-2)!2}$ different covariance values (Lindsay, 2002). Formula for covariance matrix *S* (which will be *m* x *m*) (Jauregui, 2012).:

$$S = \frac{1}{n-1}AA^T$$

By Theorem 2 , our S is symmetric. Since S is a symmetric matrix, it can be orthogonally diagonalized by Theorem 3. This connection between statistics and linear algebra is the beginning of PCA. The other point is that since $\text{cov}(a,b) = \text{cov}(b,a)$, the matrix is symmetrical about the main diagonal (Lindsay, 2002).

Step 4. Calculate the eigenvectors and eigenvalues of the covariance matrix

Since the covariance matrix is square and symmetric, we can calculate by Theorem 4 the eigenvectors and eigenvalues for this matrix. This is very important for PCA.Apply the Theorem 4 , and let $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$ be the eigenvalues of S (in decreasing order) with corresponding $eig_1 ... ... eig_n$ orthonormal eigenvectors by theorem 5. These eigenvectors are called the *principal components* of the data set (Jauregui, 2012).

Step 5. Choosing components and forming a feature vector

If you originally have *n* dimensions in your data, and so you calculate *n* eigenvectors and eigenvalues, and then you choose only the first *p* eigenvectors, then the final data set has only *p* dimensions. What needs to be done now is you

need to form a feature vector, which is just a fancy name for a matrix of vectors. This is constructed by taking the eigenvectors that you want to keep from the list of eigenvectors, and forming a matrix with these eigenvectors in the columns (Lindsay, 2002). .

$$Feature\ vector = (eig_1, eig_2, eig_3, \dots eig_n)$$

Step 6. Deriving the new data set

This the final step in PCA, and is also the easiest. Once we have chosen the components (eigenvectors) that we wish to keep in our data and formed a feature vector, we simply take the transpose of the vector and multiply it on the left of the original data set, transposed.

$$Final\ data = Row\ feature\ vector\ \times Row\ data\ adjust$$

where *Row Feature vector* is the matrix with the eigenvectors in the columns transposed so that the eigenvectors are now in the rows, with the most significant eigenvector at the top, and *Row data adjust* is the mean-adjusted data (centered data by Step 2) transposed, i.e. the data items are in each column, with each row holding a separate dimension (Lindsay, 2002).

Final data will give us the original data solely in terms of the vectors we chose. Our original data set had two axes, x and y, so our data was in terms of them. It is possible to express data in terms of any two axes that you like.If these axes are perpendicular, then the expression is the most efficient. This was why it was important that eigenvectors are always perpendicular to each other. We have changed our data from being in terms of the axes *x* and *y,* and now they are in terms of our 2 eigenvectors. In the case of when the new data set has reduced dimensionality,we have left some of the eigenvectors out, the new data is only in terms of the vectors that we decided to keep (Lindsay, 2002).

Step 7. Getting the old data back

Recall that the final transform which can be turned around so that, to get the original data back:

$$RowDataAdjust = RowFeatureVector^{-1} \times FinalData$$

However, when we take all the eigenvectors in our feature vector, it turns out that the inverse of our feature vector is actually equal to the transpose of our feature vector by Theorem 1. This makes the return trip to our data easier, because the equation becomes:

$$RowDataAdjust = RowFeatureVector^{T} \times FinalData$$

However, to get the actual original data back, we need to add on the mean of that original data. So, for completeness (Lindsay, 2002),

$$RowDataAdjust = (RowFeatureVector^{T} \times FinalData) + OriginalMean$$

3. Analysis and Results

In applying the Kaiser-Meyer-Olkin's (KMO) overall measure of sampling adequacy (MSA), a score of 0.850 is recorded which is in the acceptable range based on a KMO overall MSA greater than 0.60 being considered acceptable, (Tabachnick.B.G., 2013).Kaiser-Meyer-Olkin (KMO) Barlett's test of sphericity threshold is high and a high significant chi-square ($\chi^2 = 2102.9$ (1 d. p.), $p < 0.0001$).

Chronbach's Alpha reliability was performed ,to check consistency of the scale items.Particular sample with the value of 0.856 Chronbach's Alpha shows a high level of internal consistency for our scale.

PCA finds principal components in descending order of variations explained. The first components account for more variations than the later ones. The 1st principal component accounts for the maximum amount of variations possible in data, and the 2nd principal component extracts the maximum possible variations in data after excluding what was explained by the 1st component. Extractions can be done until all the by the last principal variations are accounted for components. So, we decided to consider (Kaiser, 1960) the first 6 factors which resulted in 27 Items. From the Table 2 Total Variance Explained it is clear that the 49,97% of the variance is explained by the first six components.

Table 2.Total variance explained

PC#	Eigenvalue	% of Variance Exp	Cumulative %
1	5.951	22.04%	22.04%
2	2.485	9.20%	31.24%
3	1.472	5.45%	36.69%
4	1.327	4.92%	41.61%
5	1.217	4.51%	46.12%
6	1.041	3.86%	49.97%

A scree plot and a bar chart for the cumulated percentage of variance are drawn in the same graph as shown on Figure 3 (Mulhern, et al., 1998).

Figure 3.
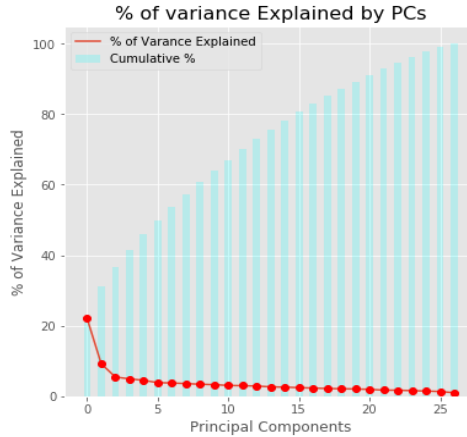
The next analysis (Table 3) shows how factor loadings. Among the principal c omponents (PCs), at the beginning only the first 6 are selected. The loadings m atrix in output shows the relationship between old variables with new principal components by calculating the coordinate of the old variables along the PC (pri ncipal component) axes:

Table 3.Component matrix

	PC1	**PC2**	**PC3**	**PC4**	**PC5**	**PC6**
1	0.182	-0.025	-0.127	0.184	0.137	0.53
2	0.376	-0.399	-0.33	-0.049	0.445	-0.084
3	0.426	-0.295	0.314	0.195	0.256	0.143
4	0.319	0.36	-0.148	0.396	0.291	-0.2
5	0.413	-0.259	0.382	0.175	0.059	-0.241
6	0.458	-0.108	0.459	0.173	0.243	0.138
7	0.432	0.214	0.059	-0.253	0.134	0.071
8	0.442	0.244	-0.471	0.029	0.216	-0.287
9	0.505	0.173	0.029	0.226	0.341	0.072
10	0.561	0.101	-0.132	0.011	0.218	0.118
11	0.553	-0.341	-0.197	-0.248	0.042	0.011
12	0.475	-0.176	-0.27	-0.092	-0.169	0.297
13	0.254	0.497	-0.161	0.15	-0.028	0.308
14	0.609	-0.253	-0.028	-0.22	0.024	-0.213
15	0.434	-0.034	-0.187	0.351	-0.429	0.214
16	0.07	0.66	0.308	-0.216	0.052	0.123

17	0.548	0.138	-0.014	-0.209	-0.223	-0.126
18	0.726	0.13	-0.019	-0.173	-0.196	0.022
19	0.695	0.088	-0.032	-0.197	-0.246	-0.005
20	0.478	0.432	-0.262	0.027	-0.061	-0.227
21	0.134	0.48	0.009	0.153	0.04	0.004
22	0.339	-0.086	0.02	0.561	-0.388	-0.079
23	0.553	-0.189	0.314	0.042	-0.08	-0.084
24	0.606	-0.228	0.117	-0.215	-0.089	0.077
25	0.525	-0.408	-0.06	-0.004	0.004	0.156
26	0.542	0.156	0.267	0.163	-0.137	-0.297
27	0.295	0.492	0.318	-0.289	0.054	0.138

PCA often needs rotation for easier interpretation. The current we used the most popular method called Varimax rotation. Varimax orthogonal rotation tries to maximize variance of the squared loadings in each factor so that each factor has only a few variables with large loadings and many other variables with low loadings (Singh Swapnika), Only loadings greater than |0.40| are considered. Results of Varimax rotation is shown on Table 4. From rotated component matrix, we eliminated questions 7,10,13,21,26 (Appendix 1) with lowest loadings. We obtained components with a Chronbach's alpha greater than 0,6.Components 1,2,3 are satisfied to condition. We considered each elements in components 4,5,6 separately, because these components reliability scale less than 0,6.

Table 4. Rotated Component Matrix

	Component					
	1	**2**	**3**	**4**	**5**	**6**
19.Alumni's presentations influenced my choice	0,682					
18.Presentations of currently enrolled students made a great impact in my choice	0,670					
11.My relatives affected my choice	0,647					
14.I wanted to follow my parents' footsteps	0,628					

24.Opinions of my peers affected my selection	0,617			
17.I was influenced by various advertisement sources (e.g. news, social media, etc)	0,559			
12.University location can be considered as a factor which affected my choice	0,538			
25.Current situation in my family affected my selection	0,489			
6.I was encouraged by a teacher because I was good at my main subjects.		0,692		
3.My high school career advisor influenced my choice		0,647		
5.My religious convictions influenced the selection of my choice		0,612		
23.My high school teacher asked me to specialize in this field as it has high demands nowadays		0,509		
8.Upon graduation good salary affected my choice			0,702	
4.The job's accessibility affected my choice			0,689	
20.Prestige of profession affected my selection			0,565	
9.My academic performance at High School affected my choice			0,460	
16.My personal interest was the strongest factor when choosing a major				0,758

27.My skills were major effect in my choice	0,675	
2.I was influenced by my parents in my choice	-0,481	
22.My UNT result was important when I selected my major		0,707
15.The major which I had selected provided more state grants than others		0,635
1.University costs played a major role in my choice		0,608

Factor 1: External Influences
   External influence factor has 8 items .As a result, external factors play an important role in choosing a profession for a child. It has loadings from 0.682 to 0.489. All these factors are more related to external influences like influence of peers and relatives, and situation of family, also advertisement of specializations. Reliability scale is 0,810(Chronbach alpha).
Factor 2: Teacher influences
Second component gave information that students can influence by school teachers. Reliability scale is 0,638.It is given with loadings 0.692 to 0.509. That is why,parents should make sure that the teacher is a person of good level. Always be in close contact with the teacher.It has 4 items
Factor 3: Influence of occupation salary
The third is important component and it covers job accessibility and prestige of major, also salary. Also, it has 4 items. The child thinks that studying for a prestigious and popular specialty will be received on the highest salary. Influence of occupation salary factor is given with loadings ranging from 0.702 to 0,565.Chronbach's alpha is 0,624.
Since the Chronbach alpha of the other 3 components is very low,we considered each element as a separate factor.Components between 4 and 9 covers only one factor of the study that is:

Factor 4: Personal interest influences

Factor 5: Personal skill influences

Factor 6: Parent's affect

Factor 7: National test affect

Factor 8: State grant affect factor

Factor 9: University cost affect factor

Hence we might conclude that factors between 4 and 9 on a very strong level can influence ones career decision all on its own.

4. *Discussion and Conclusion*

  The factors found in this article show results similar to (Sarwar, et al., 2015) ,despite the fact that two studies used samples from different study fields and different countries (Kazakhstan, Pakistan). The similarities include the factors such as personal interest affect, skills affect, occupation salary affect, teacher affect, external affect, parent's affect. However, due to the fact that the educational system of the two countries are completely different,   (Sarwar, et al., 2015) did not considered some of the facts like UNT results, state grant, cost of the university. Another study which can prove reliability of our study is (William J.Crampton, 2006). They did not work with dimensionality reduction, but defined important factors which influences to choice.
  One shortcoming of the study is that majority of participants were from ony city, Almaty. However, we note that Almaty is the largest city in Kazakhstan with many major universities.In order to improve the generalizability the study should be replicated at other universities from different cities. The biggest disadvantage of the our survey is that one third of participants are SDU students. That can change a lot of results. Also, reliability scale of component 2,3 are somewhat low.The results may be improved by increasing number of students participating in the survey and ensuring that there are different universities and majors. In the future work, we can make hypotheses testing between factors and demographic data and determine own concepts. Also, in the future research could look into the relationship between factors on the one hand and students' satisfaction with the choice made and the study success in the bachelor program on the other hand. Also, the way in which data was collected limited the study. Subjects were allowed to sign up to participate in the study and take it online at their own convenience. Administering this type of survey could be more successful if done in person. If any questions arose on the influence listed, having

a researcher available to answer questions or clarify the factor listed could provide more accurate data which in turn would lead to more accurate results. Academic consideration factor was not provided in our work. It includes course description, instructors.

The purpose of study was to identify main factors that influence the selection of major field. Principal factor analyses method conducted to reduce number of factors and we decreased factors from 27 to 9.The result of analysis gave 9 main factors. Also, this article shows all the steps needed for PCA along with Python code beyond varimax rotation. Therefore, this would help anyone who wants to run PCA at a deeper level. Teachers and parents can use the results of this study to focus their efforts on supporting students facing the decision about a major. The five-scale translated questionnaires are proved in the Appendix.

References

1   Aldosary, A.S, Assaf, S.A. Analysis of factors influencing the selection of college majors by newly admitted students. *Higher Education Policy,* 3 (9), (2009): pp. 215-220.
2   Alkhateeb H.M. Internal consistency reliability and construct validity of an Arabic translation of the shortened form of the Fennema-Sherman mathematics attitudes scales.*Psychological reports,* 94 (2004): pp. 565-571.
3   Allport G.W. *Attitudes A Handbook of Social Psychology.* Clark University Press, (1935): pp. 219-222.
4   Avellaneda, M , Lee, J.H. Statistical arbitrage in the US equities market. *Quantitative Finance*,10 (2010) :pp. 761-782.
5   Brown, J.D, How are PCA and EFA used in language test and questionnaire development? *Statistics*, 14 (2010): pp. 167-170.
6   Code, W., Merchant, S., Maciejewski, W., Thomas, M., Lo, J. The Mathematics Attitudes and Perceptions Survey: an instrument to assess expert-like views and dispositions among undergraduate mathematics students. *International Journal of Mathematical Education in Science and Technology*, *47* (6), (2016): pp. 917-937.
7   Dutton W.H. Measuring attitudes toward arithmetic. *The Elementary School Journal,* 1 (55), (1954): pp. 24-31.
8   Fennema, E., Julia, A. Sherman. "Fennema-Sherman mathematics attitudes scales: Instruments designed to measure attitudes toward the learning of mathematics by females and males". *Journal for research in Mathematics Education,* 7 (5), (1976): pp. 324-326.

9   Fizer, D. Factors affecting career choices of college students enrolled in agriculture. *A research paper presented for the Master of Science in Agriculture and Natural Science degree at The University of Tennessee, Martin* (2013): pp. 51-54.

10 Galotti, K.M. Making a" major" real-life decision: College students choosing an academic major. *Journal of Educational Psychology,* 91 (2), (1999): pp. 379-382.

11 Hyde, J. Sh., et al. Gender comparisons of mathematics attitudes and affect: A meta-analysis. *Psychology of women quarterly,* 14 (3), (1990): pp. 299-324.

12 Jauregui, J. Principal component analysis with linear algebra. *Philadelphia: Penn Arts & Sciences,* (2012).

13 Kaiser, H.F. The application of electronic computers to factor analysis. *Educational and psychological measurement,* 20 (1), (1960): pp. 141-151.

14 Leong, K.E., Nathan, A. College Students Attitude and Mathematics Achievement Using Web Based Homework. *Eurasia Journal of Mathematics, Science & Technology Education,* 10 (6), (2014): pp. 75-78.

15 Li, Han, P., Ralph, L. PCA shows how the effect of population structure differs along the genome. *Genetics,* 211 (1), (2019): pp. 289-304.

16 Liau, A., Kassim, M., Tet, M., Liau, L. Reliability and validity of a Malay translation of the Fennema-Sherman Mathematics Attitudes Scales. *The Mathematics Educator,* 2 (10), (2007): pp. 71-84.

17 Lim S.Y., Chapman, E. Development of a short form of the attitudes toward mathematics inventory. *Educational Studies in Mathematics,* (2013) , 1 (82): pp. 145-164.

18 Lin S.H., Huang Y.C. Development and application of a Chinese version of the short attitudes toward mathematics inventory. *International Journal of Science and Mathematics Education.* (2016), 1 (14): pp. 193-216.

19 Smith, L.I. *A tutorial on principal components analysis*. 2002.

20 Agrey, L., Naltan, L. Determinant factors contributing to student choice in selecting a university. *Journal of Education and Human Development* 3 (2), (2014): pp.391-404.

21 Ma, X., Nand, K. Assessing the relationship between attitude toward mathematics and achievement in mathematics: A meta-analysis. *Journal for research in mathematics education* (1997): pp. 26-47.

22 Melancon, J.G., Bruce Th., Shirley B. Measurement integrity of scores from the Fennema-Sherman Mathematics Attitudes Scales: The attitudes

of public school teachers. *Educational and Psychological Measurement,* 54 (1), (1994): pp. 187-192.

23 Michaels, L.A., Robert, A.F. Construction and validation of an instrument measuring certain attitudes toward mathematics. *Educational and Psychological Measurement,* 37 (4), (1977): pp. 1043-1049.

24 Moenikia, M., Adel Zahed-Babelan. A study of simple and multiple relations between mathematics attitude, academic motivation and intelligence quotient with mathematics achievement. *Procedia-Social and Behavioral Sciences,* 2 (2), (2010): pp. 1537-1542.

25 Mulhern, F., Gordon, R. Development of a shortened form of the Fennema-Sherman Mathematics Attitudes Scales. *Educational and psychological Measurement,* 58 (2), (1998): pp. 295-306.

26 Pearson, K. On lines and planes of closest fit to systems of points in space. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science,* 2 (11), (1901): pp. 559-572.

27 Pierce, R., Stacey, K., Barkatsas, A. A scale for monitoring students' attitudes to learning mathematics with technology. *Computers & Education,* 48 (2), (2007): pp. 285-300.

28 Richardson, F.C., Richard, M.S. The mathematics anxiety rating scale: psychometric data. *Journal of counseling Psychology,* 19 (6), (1972): pp. 551-554.

29 Sandman, R.S. The Mathematics Attitude Inventory: Instrument and User's Manual. *Journal for research in Mathematics Education,* 11 (2), (1980): pp.148-49.

30 Sanguansat, P. Principal component analysis. *BoD–Books on Demand,* (2012): pp. 1-23.

31 Sarwar, A., Rizwana, M. Factors affecting selection of specialization by business graduates. *Science International*, 27 (1), (2015): pp. 47-50.

32 Schofield, H.L. Sex, grade level, and the relationship between mathematics attitude and achievement in children. *The Journal of Educational Research,* 75 (5), (1982): pp. 280-284.

33 Shlens, J. A Tutorial on principal Component Analysis, (2014): pp. 1-12.

34 Swapnika, S., Kapse, M., Sonwalkar, J. Factors Which Affect the Career and Subject Preference of the Female. *Jounal of Women's Entrepreneurship and Education.* 1 (2), (2011): pp.89-107.

35 Subasi, A., Gursoy, M.I. EEG signal classification using PCA, ICA, LDA and support vector machines. *Expert systems with applications*, 12 (37), (2010): pp. 8659-8666.

36 Tabachnick, B.G., Linda S.F., Jodie, B.U. *Using multivariate statistics*. Boston, MA: Pearson, (2007): pp. 476-480.

37 Tapia M., Marsh G.E. An instrument to measure mathematics attitudes. *Academic Exchange Quarterly*, 2 (8), (2004): pp.16.

38 Turan, C., Kadyrov, S., Burissova, D. An Improved Face Recognition Algorithm Based on Sparse Representation. *2018 International Conference on Computing and Network Communications,* (2018): pp. 32-35.

39 White, A.L., Mathematical attitudes, beliefs and achievement in primary pre-service mathematics teacher education. *Mathematics teacher education and development*, 7 (2005): pp. 33-52.

40 Wigfield, A., Judith, L.M. Math anxiety in elementary and secondary school students. *Journal of educational Psychology,* 2 (80), (1988): pp. 210-216.

41 William, J.C., Kent, W.A., Schambach, T. *Factors influencing major selection by college of business students.* Information system, Illions State University, 7 (2016): pp. 226-229.

Appendix

	English	Russian	Kazakh
1	University costs played a major role	Плата за обучение в университете сыграла большую роль в моем выборе	Менің таңдауымда университеттің оқу ақысы үлкен рөл атқарды
2	I was influenced by my parents	На меня повлияли мои родители в моем выборе	Менің таңдауыма ата-анам әсер етті
3	My high school career advisor influenced my choice	Консультант по карьере в моей школе повлиял на мой выбор	Менің таңдауыма мектебімдегі мамандық таңдау бойынша кеңесші әсер етті
4	The job's accessibility affected my choice	Доступность работы повлияла на мой выбор	Жұмыстың қолжетімділігі таңдауыма әсер етті

5	My religious convictions influenced the selection of my major	Мои религиозные убеждения повлияли на мой выбор	Менің діни сенімдерім таңдауыма әсер етті
6	I was encouraged by a teacher because I was good at my main subjects.	На меня повлиял учитель, потому что я был хорош в своих основных предметах.	Маған мектеп мұғалімі әсер етті, себебі мен негізгі пәндерден жақсы болдым.
7	My Life Experiences have affected me (eg. You want to be a doctor, because a doctor saved someone's life in your family)	Мой собственный жизненный опыт повлиял на мой выбор (напр. Я хочу быть врачом, потому что врач спас чью-то жизнь в моей семье)	Менің өмірлік тәжірибем таңдауыма әсер етті (мысалы, Мен дәрігер болғым келеді, өйткені дәрігер менің отбасымдағы біреудің өмірін сақтап қалды)
8	Upon graduation good salary affected my choice	Наличие хорошей зарплаты после окончания учебы повлияло на мой выбор	Оқуды аяқтағаннан кейін жақсы жалақы алу мүмкіндігі таңдауыма әсер етті
9	My academic performance in High School affected the selection	Моя успеваемость в средней школе повлияла на мой выбор	Менің орта мектептегі үлгерімім таңдауыма әсер етті
10	Duration of schooling (e.g. the major will require further training like a master's degree)	Продолжительность обучения повлияла на мой выбор (например, профессия потребует дальнейшего обучения, как степень магистра).	Оқу ұзақтығы таңдауыма әсер етті (мысалы, мамандық магистр дәрежесі секілді одан әрі оқуды талап етеді

11	Extended family members affected my selection	Мои родственники повлияли на мой выбор	Менің туыстарым таңдауыма әсер етті
12	University location can be considered as a factor which affected my selection	Расположение университета можно рассматривать как фактор, повлиявший на мой выбор	Университеттің орналасуын таңдауыма әсер еткен фактор ретінде қарастыруға болады
13	Reputation of the university was important for me	Репутация университета была важна для меня в моем выборе	Таңдауым үшін университеттің беделі маңызды болды
14	I wanted to follow my parents footsteps	Я хотела пойти по стопам родителей	Мен ата- анамның ізімен жүргім келді
15	The major which I had selected provided more state grants than others	Профессия, которую я выбрал, давала больше государственных грантов, чем другие	Басқаларға қарағанда мен таңдаған мамандық бойынша көбірек мемлекеттік гранттар берілді
16	My personal interest was the strongest factor when choosing a major	Мой личный интерес был самым сильным фактором при выборе специальности	Менің жеке қызығушылығым мамандықты таңдауда ең үлкен фактор болды
17	Academic assessment of the major that I had selected based from printed or online information	На меня повлияли различные источники рекламы (например, новости, социальные сети и т. д)	Маған түрлі жарнама көздері әсер етті (мысалы, жаңалықтар, әлеуметтік желілер және т. б.)

18	Presentations of currently enrolled students made a great impact	Презентации зачисленных студентов оказали большое влияние на мой выбор	Қазіргі таңда сол мамандық бойынша оқып жатқан студенттерінің презентациялары таңдауыма үлкен әсер етті.
19	Alumni's presentations influenced my choice	Презентации выпускников повлияли на мой выбор	Түлектердің презентациялары таңдауыма әсер етті
20	Prestige of profession affected my selection	Престиж профессии повлиял на мой выбор	Мамандықтың беделі таңдауыма әсер етті
21	I assumed that professionals in this field can help develop my country	Я считаю, что профессионалы в этой области могут помочь развитию моей страны	Менің ойымша, осы саладағы мамандар еліміздің дамуына көмектесе алады
22	My school graduation exam result was important when I selected my major	Мой результат ЕНТ был важен, когда я выбирал свою специальность	Мамандығымды таңдағанда ҰБТ-ның нәтижесі маңызды болды
23	My high school teacher asked me to specialize in this field as it has high demands nowadays	Мой учитель средней школы попросил меня специализироваться в этой области, поскольку она имеет высокие требования в настоящее время	Менің орта мектеп мұғалімім маған осы саланы меңгеруге кеңес берді, себебі ол қазіргі уақытта жоғары сұраныста бар сала
24	Opinion of my peers affected my selection	Мнения моих сверстников повлияли на мой выбор	Менің құрдастарымның пікірлері таңдауыма әсер етті

25	Current situation in my family affected my selection	Текущая ситуация в моей семье повлияла на мой выбор	Менің отбасымның сол уақыттағы жағдайы таңдауыма әсер етті
26	Famous personalities who had the same specialization in that field affected my major selection	Знаменитые личности, которые имели ту же специализацию в этой области, повлияли на мой основной выбор	Осы салада мамандаған танымал тұлғалар негізгі таңдауыма әсер етті
27	My skills were major effect in my choice	Мои навыки оказали большое влияние на мой выбор	Менің қабілеттерім таңдауыма үлкен әсер етті

IRSTI 28.23.01

S. Dauylov[1], A. Bogdanchikov[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

INTRODUCE PREDICTIVE ANALYTICS USING THE NEXT BEST ACTION (NBA) MODELS INTO THE BANKING SYSTEM

Abstract. NBA - is an approach in which each client is initially considered purely individual. It has a close correlation with Predictive analysis. Predictive or prognostic analytics is a set of techniques and methods for analyzing data to build a forecast of future events. The banking system is currently using the method to obtained certain business results from its customers and has increased loyalty, increased income, found new growth points, etc. The classical model of marketing was rather different, it repelled from its existing product line and its parameters. But new models repels from customer's inclination to purchase a particular product. The aim of this project is to investigate the field of deposit accounts of the banking system by using NBA approach and to show the benefits and possible outcomes. This approach was tested on various aspects of the banking system and showed a number of solutions which can predict the probability of a customer to create a term deposit account.

Keywords: Next Best Action, Predictive analysis, mplementation, Banking System, Term Deposit, Predictive analysis.

∗∗∗

Аңдатпа. NBA - бұл әр клиент бастапқыда жеке тұлға болып саналатын тәсіл. Болжамдық талдаумен тығыз байланыс бар. Болжалды немесе болжамдық аналитика - бұл болашақ оқиғалардың болжамын құру үшін мәліметтерді талдау әдістері мен әдістерінің жиынтығы. Қазіргі уақытта банк жүйесі өз клиенттерінен белгілі бір бизнес нәтижелерін алу әдісін қолданады және адалдықты арттырды, кірісті ұлғайтты, жаңа өсу нүктелерін тапты және т.с. маркетингтің классикалық моделі мүлдем өзгеше болды, ол өзінің қолданыстағы өнімі мен параметрлерінен өзгеше болды. Бірақ жаңа модельдер тұтынушының белгілі бір өнімді сатып алуға деген бейімділігінен арылтады. Бұл жобаның мақсаты - НБА тәсілін қолдана отырып, банктік жүйенің депозиттік шоттары саласын зерттеу және оның артықшылықтары мен мүмкін нәтижелерін көрсету. Бұл тәсіл

банктік жүйенің әртүрлі аспектілері бойынша сыналды және клиенттің мерзімді депозиттік шотты құру ықтималдығын болжайтын бірқатар шешімдерді көрсетті.

Түйін сөздер: Next Best Action, болжамды талдау, енгізу, банк жүйесі, мерзімді салым, болжамды талдау.

<div align="center">***</div>

Аннотация. NBA - это подход, при котором каждый клиент изначально считается сугубо индивидуальным. Это имеет тесную связь с прогнозным анализом. Прогнозирующая или прогностическая аналитика - это набор методов и методов анализа данных для составления прогноза будущих событий. Банковская система в настоящее время использует метод для получения определенных бизнес-результатов от своих клиентов и имеет повышенную лояльность, увеличенный доход, найденные новые точки роста и т.д. Классическая модель маркетинга была несколько иной, она отталкивалась от существующей линейки продуктов и ее параметров. Но новые модели отталкивают от склонности покупателя покупать конкретный товар. Целью данного проекта является исследование области депозитных счетов банковской системы с использованием подхода НБА и демонстрация преимуществ и возможных результатов. Этот подход был опробован в различных аспектах банковской системы и показал ряд решений, которые могут предсказать вероятность того, что клиент создаст срочный депозитный счет.

Ключевые слова: Next Best Action, прогнозный анализ, внедрение, банковская система, срочный депозит, прогнозные анализы.

Introduction

The theme of emotion and customer experience has been worrying bankers for quite some time. The tightening of regulations and requirements prompted banks to look for new sources of competitive advantage, in the US for example, 92% of millennials claim to have a lack of confidence in the traditional banking system and increasingly use new services. Customer experience is an indirect characteristic that translates into financial results of a bank through customer loyalty, a desire to continue to serve all of them at the same bank even in conditions of high consumer awareness and low switching costs to other financial companies. 78% of bank managers around the world surveyed by the IBM Institute for Business Value argue that customer engagement and understanding customer's needs are key conditions for the best customer experience and successful creation of new products and services.

Aim and objectives of the research

As a successful, the whole process of the research, find the dataset which will contain attributes of Bank System. Then preprocessing data, which means replace empty fields or putting default value. A good result will be comparison several prediction methods. Also it will be nice if each step can contain a pretty graph. In the future go to practice with a big amount of data and using a stack of technologies from Big Data tools.

Background of literature review

At the beginning of the research, have been found a couple of interesting scientific papers which are a little be related to our topic, also some solutions that are ready for use. There are several finished offers, from free to paid.

One of the companies in New Zealand used a lot of data for improving credit scoring models. They construct a baseline model based solely on the existing scoring features obtained from the loan application form, and a second baseline model based solely on the new bank statement-derived features. A combined feature model is then created by augmenting the application form features with the new bank statement derived features [1].

Microsoft offers Veripark's [2] Next Best Action (N.B.A.) is a leading customer-centric technology that considers all the possible actions during a customer interaction and recommends the next best one thereby increasing the likelihood of positive response.

RapidMiner [3] is a software platform for analytics teams that unites data prep, machine learning, and predictive model deployment, also one of the solutions is Next Best Action. Their slogan is "One platform, does everything", they mean visual workflow, team collaboration, model management, deployment and work with technologies like Hadoop and Spark.

Cloud Sense [4] platform has a good interface, tutorials and before using it, you can see the demo version. For an organization that uses Salesforce, a most popular CRM system, CloudSense easily can be integrated.

Pega [5] they're a software solution called Pegasystems. Good company with a couple of success cases. In the platform, they have Customer Decision Hub, Intelligent Guided Selling, Contextual Next-Best-Action Marketing Intelligent Guidance for Customer Service.

NGData [6] offers the solution of Next Best Action as a whole marketing system. This decision is an excellent solution for the organization that works with clients and they need a CRM System.

Jacada [7] prefer a flexible system for working with their platform. Also, they have a nice intelligent chatbot. Their Agent Desktop is prime real-estate in the bid to win and keep customers.

Also, early in this year, there was a good article [8], about how Sberbank works with BigData and what kind of tools they are using. Their tools and methods can be as good for a start.

Methods and materials

The main tool to support this project was the Jupyter notebook, which consists of various libraries for applying of the machine learning approach. Data was collected from the open-sourced repository "UCI: Machine Learning Repository" [9]. In this database were used 45211 instances and 21 attributes.

I.   Attribute Information - to some of them was presented detailed graphs for better representation (Figure 1).
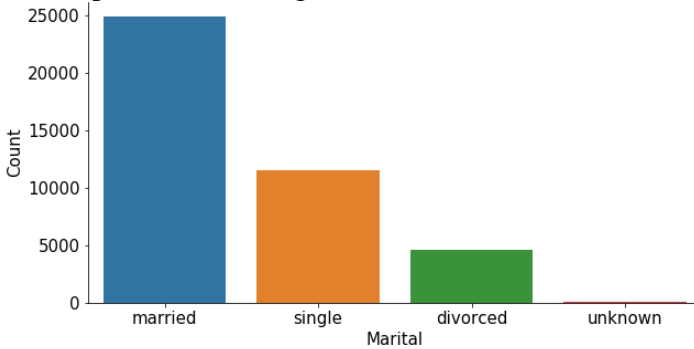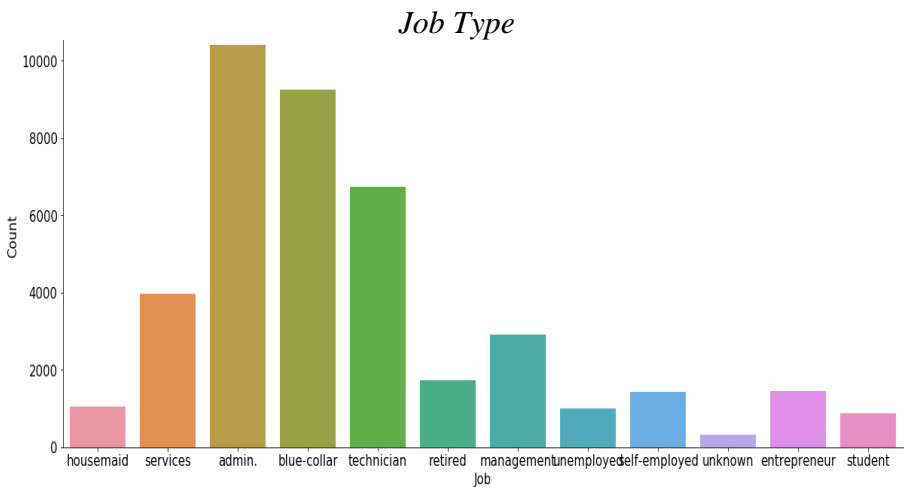

Figure 1. Attributes Information Marital Status

II.   Implementation

Stage 1: Import of Library and Data

Stage 2: Preprocessing of data

Stage 3: Development of Predictive Model

After preprocessing data development of the model can finally start. Data was divided into standard proportions: train - 0.8, test - 0.2. Here will be comparing several types of machine learning classifiers:

1. K Nearest Neighbors Classifier [10]

An object is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its k nearest neighbors (k is a positive integer, typically small). If k = 1, then the object is simply assigned to the class of that single nearest neighbor. K = will be choosing just brute-forcing neighbors from 1 to 25, and getting categories where the accuracy of prediction was tested. Thereby was selected an optimal number of neighbors.

2. Random Forest Classifier [11]

Random Forest Classifier is an ensemble algorithm. Ensembled algorithms are those which combine more than one algorithms of the same or different kind for classifying objects. Random forest classifier creates a set of decision trees from a randomly selected subset of the training set. It then aggregates the votes from different decision trees to decide the final class of the test object. Basic parameters to Random Forest Classifier can be a total number of trees to be generated and decision tree related parameters like minimum split criteria etc.

3. Naive Bayes Classification [12]

Naive Bayes classifier calculates the probabilities for every factor (here in case of email example would be Alice and Bob for given input feature). Then it selects the outcome with the highest probability.

Data and results

In this study were tested three types of classifiers. Random Forest classifier showed 90.0% of accuracy, NaiveBayes has shown 85.0% and highest among them is K Neighbors Classifier with remarkable 90.4% of accuracy. During the study 22 neighbors were selected due to their high accuracy. In comparison to more traditional methods of product-based marketing, this model allows finding potential customers with high accuracy due to a predictive selection of them (Figure 2).
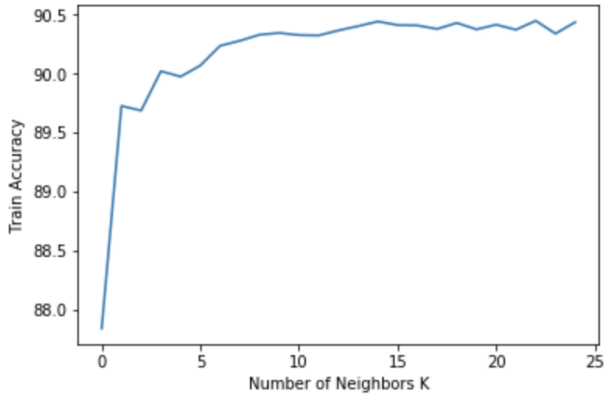
The optimal number of neighbors is 22 with 90.4%

Figure 2. Selection of best numbers of neighbors

Discussion

In this paper, the NBA approach was presented and implemented into the banking system cases. The proposed approach correlates between Marketing and Data Science, to develop new models of working with clients. The performance of the NBA method in comparison to more traditional methods has shown remarkably well. In the future this might be used as the main model of working with clients. This is significantly increasing the popularization of Data Science among young developers and creates better ground for further investigation.

Conclusion

In this paper, the NBA approach was presented and implemented into the banking system cases. The proposed approach correlates between Marketing and Data Science, to develop new models of working with clients. The performance of the NBA method in comparison to more traditional methods has shown remarkably well. In the future this might be used as the main model of working with clients. This is significantly increasing the popularization of Data Science among young developers and creates better ground for further investigation.

References

1   Rory, P.B., Zhang, W., Asif Naeem, M. Improving a Credit Scoring Model by Incorporating Bank Statement Derived Features. Oct 30, 2016. Arxiv.org. Last modified on March 1, 2017. URL: https://arxiv.org/abs/1611.00252v2
2   Veripark. Veripark.com. Last accessed on Feb 27, 2020. URL: https://www.veripark.com/products/veriloan.

3 RapidMiner. Rapidminer.com. Last accessed on Feb 27, 2020. URL: https://rapidminer.com/solutions/next-best-action/.

4 CloudSense. Cloudsense.com. Last accessed on Feb 27, 2020. URL:-https://www.cloudsense.com/platform/genius-next-best-action/.

5 Pega. Pega.com. Last accessed on Feb 27, 2020. URL:-https://www.pega.com/technology/next-best-action.

6 NGData. Ngdata.com. Last accessed on Feb 27, 2020. URL: https://www.ngdata.com/solutions.

7 Jacada. Jacada.com. Last accessed Feb 27, 2020. - URL: https://www.jacada.com/solutions/agent-next-best-action.

8 Чирухин О. Спецпроекты в Сбербанк-Технологиях. Habr.com. Jan 30, 2018. Last accessed on Feb 27, 2020. URL: https://habr.com/company/jugru/blog/347854/

9 Moro, S., Cortez, P., Rita, P. A Data-Driven Approach to Predict the Success of Bank Telemarketing. Decision Support Systems, Elsevier. Archive.ics.uci.edu. June 2014. Last accessed on Feb 27, 2020. URL: https://archive.ics.uci.edu/ml/datasets/Bank+Marketing.

10 Harrison, O. Machine Learning Basics with the K-Nearest Neighbors Algorithm. Towardsdatascience.com. Sep 11, 2018. Last accessed on Feb 27, 2020. URL: https://towardsdatascience.com/machine-learning-basics-with-the-k-nearest-neighbors-algorithm-6a6e71d01761.

11 Yiu, T. Understanding Random Forest. Towardsdatascience.com. June 12, 2019. Last accessed on Feb 27, 2020. URL: https://towardsdatascience.com/understanding-random-forest-58381e0602d2.

12 Gandhi, R. Naive Bayes Classifier. Towardsdatascience.com. May 5, 2018. Last accessed on Feb 27, 2020. URL: https://towardsdatascience.com/naive-bayes-classifier-81d512f50a7c.

IRSTI 28.23.01

K. Kaiyp[1] , M. Alimanova[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

IMPROVING INDICATORS OF DIGITAL MARKETING USING ARTIFICIAL INTELLIGENCE

Abstract. In recent years, artificial intelligence (AI) has become a growing trend in various fields: medicine, education and the automotive industry. AI also reached a business, namely the marketing department of various businesses. The goal of the article is to research how deeply AI is used in digital marketing. The authors asked two research questions - which areas of AI are used in marketing and what are the positive effects of chat bots on a business. To answer these questions, the authors conducted a study of secondary data with examples of AI used for marketing purposes. An analysis of the collected examples shows that AI is widely implemented in the field of marketing, although applications are at the operational level. This may be the result of the careful implementation of the new technology, still at the level of experimentation with it. The uncertainty of the results of the implementation of AI can also affect caution when applying these innovations in practice. The collected examples proved that AI affects all aspects of the marketing structure, affecting both consumer value and the organization of marketing and business management. This document is important for the business, especially the idea of introducing artificial intelligence into marketing, developing innovation, and ideas on how to incorporate new skills into the marketing team needed for new technology.

Keywords: artificial intelligence, machine learning, big data, digital marketing, marketing strategy.

***

Аңдатпа. Соңғы жылдары жасанды интеллект (ЖИ) әртүрлі салаларда: медицина, білім және автомобиль өнеркәсібінде өсіп келе жатқан үрдіске айналды. ЖИ сонымен қатар бір бизнеске, атап айтқанда әртүрлі бизнестің маркетинг бөліміне жетті. Мақаланың мақсаты - сандық маркетингте ЖИ қаншалықты терең қолданылатындығын зерттеу. Авторлар екі зерттеу сұрақтарын қойды - маркетингте ЖИ-дің қай бағыттары қолданылады және бизнеске чат боттардың оң әсері қандай? Осы сұрақтарға жауап беру үшін авторлар маркетингтік мақсаттарда пайдаланылған ЖИ мысалдары бар қайталама деректерді зерттеу жүргізді.

Жиналған мысалдарды талдау ЖИ маркетинг саласында кеңінен қолданылатынын көрсетеді, дегенмен қолданбалар операциялық деңгейде. Бұл жаңа технологияны тәжірибе деңгейінде әлі де мұқият іске асырудың нәтижесі болуы мүмкін. ЖИ енгізу нәтижелерінің белгісіздігі де осы жаңалықтарды тәжірибеде қолдану кезінде сақ болуға әсер етуі мүмкін. Жиналған мысалдар ЖИ тұтынушылық құндылыққа да, маркетинг пен бизнесті басқаруға да әсер ететін маркетинг құрылымының барлық аспектілеріне әсер ететіндігін дәлелдеді. Бұл құжат бизнес үшін маңызды, әсіресе маркетингке жасанды интеллект енгізу, инновацияны дамыту, жаңа технологияға қажет маркетингтік топқа жаңа дағдыларды қалай енгізу туралы идеялар.

Түйін сөздер: жасанды интеллект, машиналық оқыту, үлкен мәліметтер, сандық маркетинг, маркетинг стратегиясы.

<center>***</center>

Аннотация. В последние годы искусственный интеллект (ИИ) стал развивающейся тенденцией в различных областях: медицина, образование и автомобилестроение. ИИ также достиг бизнеса, а именно отдела маркетинга различных бизнесов. Целью статьи является исследование того, насколько глубоко ИИ применяется в цифровом маркетинге. Авторы задали два вопроса исследования - какие области ИИ используются в маркетинге и какие положительные последствия чат боты дают бизнесу. Чтобы ответить на эти вопросы, авторы провели исследование вторичных данных с примерами ИИ, использованными в маркетинговых целях. Анализ собранных примеров показывает, что ИИ широко внедряется в области маркетинга, хотя приложения находятся на операционном уровне. Это может быть следствием тщательного внедрения новой технологии, все еще на уровне экспериментов с ней. Неопределенность результатов внедрения ИИ также может повлиять на осторожность при применении этих нововведений на практике. Собранные примеры доказали, что ИИ влияет на все аспекты структуры маркетинга, влияя как на потребительскую ценность, так и на организацию маркетинга и управлению бизнесом. Этот документ имеет значение для бизнеса, особенно идеи по внедрению искусственного интеллекта в маркетинг, разработке инноваций и идеи о том, как включить новые навыки в команду маркетинга, необходимые для новой технологии.

Ключевые слова: искусственный интеллект, машинное обучение, большие данные, цифровой маркетинг, маркетинговая стратегия.

Introduction

The essence of marketing has not changed, but the way of communication has changed marketing. It changes every day. That is where the big shift happened. The art of storytelling is plentiful, but the key to this is how we tell the story and the means by which we tell the story. The big changes that will happen in marketing, as well as in business, are artificial intelligence and machine learning. - Sanjiv Mehta, CEO and MD of Hindustan Unilever Ltd.

It is not so difficult to say that in the future marketing will increasingly use AI. Even today, the components of an artificial intelligence-based approach are pretty much in place. Modern marketing is becoming more quantitative, targeted and tied to business results. Ads and promotions are increasingly being adapted to individual consumers in real time. Companies use several channels to access customers, but they are increasingly using digital content. The company's marketers still work with agencies, many of which have developed their own analytical capabilities. - Thomas H. Davenport.

Main part

AI has so far attracted the attention of engineers, IT experts and analysts, but now it goes beyond its traditional fields of activity, making an increasingly noticeable footprint in the field of management and marketing. The ever-growing volume of consumer data available online, in big data systems or mobile devices, makes AI an important marketing ally, since it is based on data analysis in almost all areas of its application. Marketing takes advantage of the data to a large extent - from studying consumer needs, analyzing the market, understanding customers and competition information, conducting events in various communication or distribution channels, and measuring the results and effects of adopted strategies. Marketing is becoming a natural beneficiary of the development of information technology. The proximity of both domains allows for a synergistic effect. Therefore, it seems important to emphasize the potential of artificial intelligence and available AI-based tools and discuss the commercial application of AI in the field of marketing.

In 2013, the American Marketing Association approved a new version of the definition of marketing. According to the association, ″marketing is an activity, a set of institutions and processes for creating, exchanging, delivering and exchanging offers that are valuable to customers, customers, partners and society as a whole”.

A critical aspect of marketing is providing value to customers, while value can represent various aspects of a product, such as products, ideas, services, information, or any type of solution that satisfies customer needs.

McCarthy proposed the idea of a ″marketing mix″ as a conceptual framework that brings marketing planning to life. Although the marketing mix is not a scientific theory, its tools can develop both long-term strategies and short-term tactical marketing programs. McCarthy refined Borden's previous concept of target market satisfaction. He grouped 12 Borden elements (product planning, pricing, branding, distribution channels, personal sales, advertising, promotion, packaging, demonstration, service, physical processing, fact finding and analysis) into four elements called 4P: product, price, promotion and place. Further improvements have been made in the concept of marketing, such as the addition of another P - people, processes, physical evidence, although the idea of 4P is still widely used and accepted. AI could be used in Promotion part of 4P, because this part covers advertising, messages, conversation, a lot of data, where AI could show results.

Figure 1. The 4 P's of marketing mix
Source: Author

Methods

Before companies can begin implementing AI marketing solutions, it is better to understand the parts and components of AI and how they make them work faster, easier and more efficiently. The following are explanations of AI components based on Brookings Institutions definitions:

Artificial intelligence is a collection of machines that respond to stimulation in the same way as humans. He can make decisions that usually require human experience. For example, chat bots in messenger, that automatically answer for customers questions.

Machine learning is a technology that analyzes huge amounts of data to identify trends and receive information. It provides AI systems with the ability to automatically learn and improve. For example, Smart Bidding in Google Ads.

Smart Bidding is a subset of automated bid strategies that use machine learning to optimize for conversions or conversion value in each and every auction—a feature known as "auction-time bidding".

Data science is the study of where information comes from, what it means and how it can be interpreted. For example, there are a lot of data in Google Analytics and Yandex Metrika of each company.

Typically, all three of these technologies go hand in hand. They give marketers the opportunity to understand the sheer volume of data in order to inform them of creative and strategic decisions.

Most companies already know about live chat bots or artificial intelligence systems that you communicate with in instant messaging, and many already use this feature on their site. But have you ever thought about updating traditional chats with AI-based chat bots? The time has just come to do this. Recently, National Australian Bank launched a customer support chat chat to help customers find answers to common banking requests. The bot is able to answer more than 200 common questions related to banking.

There are a huge number of programs for creating business logic for chat bots in the Facebook, Telegram and WhatsApp messengers. After analysis and a series of tests of these programs, the most stable and successful was revealed, and this is Xenioo.
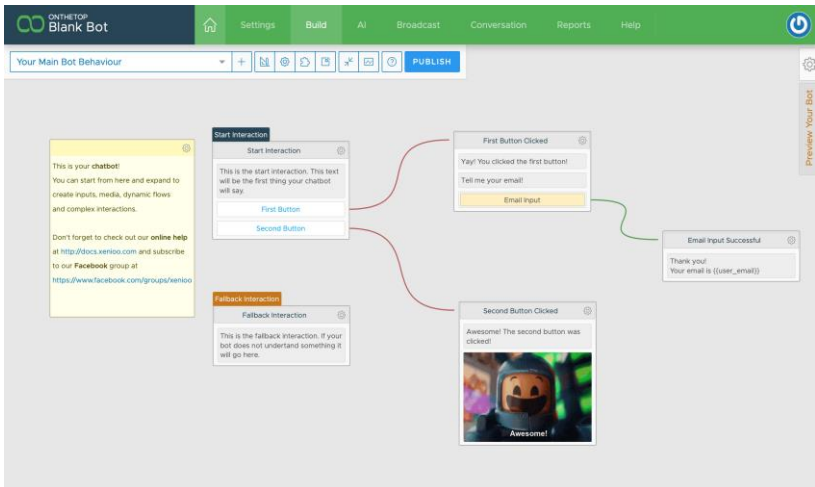

Figure 2. Logic of sample WhatsApp chat bot in Xenioo
Source: Author

As the experiment we developed WhatsApp bot and forwarded people from Facebook and Instagram ads to this chat bot. Before it was just usual WhatsApp of company, where manager answered for questions of clients only at the working hours. But companies launches ads around the clock and everyday. It means that customer could write to manager of company at anytime, it could be early morning or late night. As the experiment shows WhatsApp chat bot have positive effect to customer relationship.
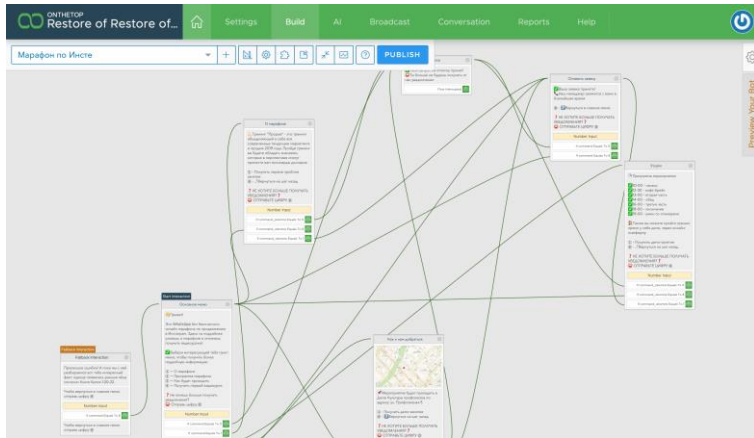

Figure 3. WhatsApp chat bot in Xenioo
Source: Author

In Figure 4 is screenshot of how WhatsApp chat bot works. For this research authors developed simple chat bot, we could make it more complicated and complex, functionality depends on goals of business.

Figure 4. How WhatsApp chat bot works
Source: Author

Results

In the Figure 5 we see how many click Facebook Ads campaigns get. Totally it is 3 352 clicks and all people, when clicked to the button in the ads, were forwarded to usual WhatsApp and chat bot. And the huge number of click of ad campaigns were gotten at the evening, after 7PM till 6 AM. Using WhatsApp chat bot we have automated communication with client and managers got more conversional leads, because requests from clients were qualified and they are ready to buy product of company. Lead processing time reduced from 1 working day to 8 minutes without losing quality.

Figure 5. Facebook Ads Manager. Source: Author

According the research of "99 Firms" that 79% of customers prefer chat for getting their questions answered quickly. Here are the benefits of customer service using WhatsApp chatbots from our research:

• Zero customer wait time

• 24X7 availability

• Ever-expanding knowledge database

• Chat bots have the ability to route complex queries to human

Bots can also announce new product launches and share information about discounts and coupons to drive user engagement up. The data collected by these chatbots throughout customer interactions helps marketers develop insight on consumer behavior and mindset – and, again, they do this at scale.

Thus, ML-powered chatbots not only help digital marketers save money, but also ensure better business outcomes.

Discussion

Implications for marketing

The authors analyzed the collected examples and synthesized how these examples reflect the marketing structure. The findings are presented in Table 1. Each proven example shows that AI affects every area of the marketing program. This penalty is especially important for practitioners who are responsible for developing innovations, since AI affects the entire spectrum of marketing

activities. In addition, AI applications that extend the core product require an innovative design approach to find ideas that fit ideas that go beyond a product or even a category. This is important for the implementation of AI in the field of "product" and "promotion" in the marketing mix program.

Table 1. Areas of the impact of AI on marketing mix Source: Author

Product	Price	Promotion (Brand)	Place (Sales and Distribution)
New product development	Price management	Creating a unique experience	Convenient shopping
Hyper personalisation	Dynamic price matching to customer profile	Personalised communication	The faster and simpler sales process
Automatic recommendations		Creating the wow factor and offering benefits	24/7 customer service (chatbot)
Creating additional value		Elimination of the process of learning product categories	Purchase automation
Additional solutions beyond product category		Positive impact on the customer	Service-free shops
		Minimised disappointment	Consultant-less customer support
			New distribution channels
			Merchandising automation

The analysis of the collected cases shows that AI activities have a two-way impact on marketing. On the one hand, the consumer is the beneficiary of the changes, but on the other hand, new solutions affect all ongoing marketing activities.

Conclusion

When it comes to marketing management, AI has a significant impact on contemporary practices, and will surely require a new approach to tasks fulfilled in marketing teams:

- Elimination of laborious and time-consuming activities. AI automates routine and repeatable tasks (e.g. data collection and analysis, image search and adaptation/processing).
- Bigger significance of creative and strategic activities. Precise analyses performed by AI increases the role of creative and strategic activities to build competitive advantage.

- Developing new competences in the marketing team. AI requires incorporating data scientist skills as well as an understanding of the new technology possibilities in the marketing team.
- A new marketing ecosystem. The complexity of AI increases the role of companies producing AI solutions. Due to the current level of AI advancement, there is a need to develop a new model of cooperation with AI entities offering data engineering or ML tools.

References

1 Joydeep, B. 12 Ways to Use Machine Learning in Digital Marketing. Singlegrain.com. 2018. URL: https://www.singlegrain.com/artificial-intelligence/12-ways-to-use-machine-learning-in-digital-marketing/.
2 Live Chat Statictics. I99firms.com. January 2019. URL: https://99firms.com/blog/live-chat-statistics/#gref.
3 Google Ads Help. Support.google.com, 2014. URL: https://support.google.com/google-ads/answer/7065882?hl=en.
4 Jarungjit, T., Jomkwan, J. The Artificial Intelligence (ai) with the future of digital marketing. Ssrn.com. May 22, 2019. URL: https://ssrn.com/abstract=3405184.
5 Thiraviyam, T. Artificial Intelligence marketing. March 2, 2018. V.O. Chidambaram College, Thoothukudi. URL: researchgate.net.

IRSTI 28.23.01

K. Kaiyp[1], M. Alimanova[2],
Suleyman Demirel University, Kaskelen, Kazakhstan

USING ARTIFICIAL INTELLIGENCE TO IMPROVE DIGITAL MARKETING STRATEGIES

Abstract. The use of artificial intelligence (AI) will provide huge advantages in the digital marketing strategy of each company. This is a new face of productivity, efficiency and profitability. Making decisions about the start of a new era based on artificial intelligence should not replace the work of marketers or advertisers. It is here to unleash their true strategic and creative potential. For a business executives and marketers, the time has come to identify the problems facing the business or the marketing campaign, and how accurate ideas can solve these problems. This study discusses how AI could affect to effective of marketing strategies, shows real cases of using AI tools, and how companies could increase their profit.

Keywords: artificial intelligence, machine learning, big data, digital marketing, marketing strategy.

***

Аңдатпа. Жасанды интеллектті пайдалану әр компанияның сандық маркетингтік стратегиясында үлкен артықшылықтар береді. Бұл өнімділіктің, тиімділіктің және пайдалылықтың жаңа кезеңі. Жасанды интеллект негізінде жаңа дәуірдің басталуы туралы шешім сатушылар мен жарнама берушілердің жұмысын алмастырмауы керек. Бұл жерде сіздің шынайы стратегиялық және шығармашылық әлеуетіңізді ашу керек. Кәсіпорын басшылары мен маркетологтар үшін бизнеске және маркетингтік кампанияға тап болатын проблемаларды анықтайтын және нақты идеялардың осы мәселелерді қалай шешетінін білетін уақыт жетті. Бұл зерттеуде ЖИ маркетингтік стратегиялардың тиімділігіне қалай әсер ететіні, ЖИ құралдарын қолданудың нақты жағдайлары және компаниялар онымен өз кірістерін қалай арттыра алатындығы туралы айтылады.

Түйін сөздер: жасанды интеллект, машиналық оқыту, үлкен мәліметтер, сандық маркетинг, маркетинг стратегиясы.

***

Аннотация. Использование искусственного интеллекта (ИИ) обеспечивает огромные преимущества в стратегии цифрового маркетинга каждой компании. Это - новый этап производительности, эффективности и прибыльности. Принятие решений о начале новой эры на основе искусственного интеллекта не должно заменить работу маркетологов или рекламодателей. Именно здесь, чтобы раскрыть свой истинный стратегический и творческий потенциал. Для руководителей фирм и маркетологам, пришло время определить проблемы, стоящие перед бизнесом и маркетинговой кампанией, и выяснить, как точные идеи могут решить эти проблемы. В этом исследовании обсуждается, как ИИ может влиять на эффективность маркетинговых стратегии, показываются реальные случаи использования инструментов ИИ и как компании могут увеличить свою прибыль с помощью него.

Ключевые слова: искусственный интеллект, машинное обучение, большие данные, цифровой маркетинг, маркетинговая стратегия

Introduction

One of the major innovations in the digital marketing industry is the introduction of artificial intelligence tools to help streamline marketing processes and make businesses more effective. According to QuanticMind, 97% of leaders believe that the future of marketing lies in the ways that digital marketers work alongside machine-learning based tools.

As machine learning and artificial intelligence become more commonplace in the digital marketing landscape, it's imperative that best-in-class digital marketers learn how to apply machine learning to their digital marketing strategies.

Main part

The aim of research is how AI algorithms and tools could change the results of digital marketing strategies and campaigns, could AI improve results or not.

For now, AI helps marketers become even more effective at targeting high-value customers, driving conversions and generating sales. Here are three ways you can leverage AI to transform digital marketing campaigns:

1. Turn big data into action. Big data is nothing without the ability to translate it into actions that drive business outcomes. Predictive analytics and propensity modeling help marketers use customer behavior to execute more effective campaigns. The beauty of this model is that the more information it receives, the better it gets at producing results.

2. Use Chatbots to give customers the speed and service they command. 2016 saw the first wave of chatbots deployed at cutting-edge organizations. By many measures, consumers responded favorably, which is prompting other organizations to follow suit. A national survey in the USA of 1000 consumers revealed that 49% of respondents prefer conducting all customer service interactions via text, chat, or messaging app instead of with customer service agents. Millennials' preference for using chatbots was the highest (54%) of any subgroup, indicating that businesses must consider these and other AI-powered tools for the long term.

3. Create personalized digital experiences that drive engagement and sales. Tech savvy consumers expect personalized experiences that are seamlessly integrated across devices. Google's Audience Solutions is poised to help marketers do just that while providing higher click-through rates and sales. How? With the power of machine learning. Google tracks user activity across several digital properties and combines it with other user data to identify key sales opportunities for relevant vendors.

As we understood, in digital marketing we have a lot of data and AI allows marketers to analyze more data than a human mind could comprehend, respond to an audience's preferences better, and using natural language processing to understand the target market.

We have been using AI almost every day for quite some time, after all. For example:

- Google Maps analyzes anonymous data from smartphones. Every time you use it, the app uses machine learning-powered insights to help you avoid traffic congestions.
- Another of Google's AI platforms, Rankbrain, interprets your search queries. It helps the search engine understand your search intent. Rankbrain then uses those insights to deliver you the right information.
- Gmail uses machine learning to protect you from spam.
- Credit card processors use artificial intelligence to detect fraud.
- Various brands offer AI-powered platforms to help us with such mundane aspects of our work lives as project management or time management.
- Many business platforms use machine learning to deliver personalized content, offers, and so much more to enrich your customer experience.
- And AI-powered marketing analytics platforms let you analyze unbelievable amounts of data to drive the marketing ROI further.
- Yet, in spite of the above, little evidence suggests any negative impact of AI on marketing, in general.

Plenty of evidence confirms the positive impact of AI to digital marketing:

- 84% of marketing companies have implemented or expanded their use of AI in 2018.
- Next year, 40% of digital transformation initiatives within organizations will include artificial intelligence.
- By 2020, 30% of companies will use AI in at least one of their sales processes

Furthermore, AI helps drive meaningful results and an incredible ROI:

- 3 of 4 companies that have implemented AI achieved a 10% or more boost in sales.
- For 75% of organizations, using AI has helped drive customer satisfaction by 10% as well.
- Finally, a report by Forrester revealed that, in just two years, businesses using AI to power data-driven insights in marketing would grow to $1.2 trillion combined.

Methods and Materials

AI opens up incredible opportunities for marketers. It can be hard to realize its full potential. Particularly, when you try to imagine how you could use it in your work. Let me show some of the ways to use artificial intelligence to enrich marketer work.

Case #1. Better Customer Segmentation and Personalization. Today's customers expect a personalized marketing experience. In fact, to even consider buying from you, they want you to make them feel as if you knew them in person. And the minimum prerequisite to meeting those expectations is delivering the right message to the right customer. And at the right time, at that. Which is quite a challenge. That's especially true, if you try doing it without having a deep understanding of various customer segments your brand can serve.

That is where AI comes in. Artificial intelligence allows marketers to analyze their customer data in detail. Such insight helps create precise customer segments. And also, map those to the entire customer journey. But that is just a start. Such in-depth data analysis could also reveal each segment's motivations, desires, and pain points. Correlated with other data points, it could even help predict the customers' next moves. For example, it could help forecast each segment's buying pattern throughout the year per product or service.

And with such information, marketers can launch campaigns designed to engage a specific segment. And do so with a message tailored to those customers' needs, and perfectly-timed.

For example, this is screenshot from Ads Manager of Facebook, which I used for my work. There are a lot of ad campaigns. Each campaign has specific goal and they were used algorithms of machine learning of Facebook. As the result, when people see ads 2-3 times with specific offer, effect of campaign increases.

Figure 1. Ad campaigns in the Ads Manager Facebook
Source: Author

Case #2. Improving the Depth of Marketing Data. For most marketers, the benefits of data-driven marketing remain limited by their ability to access, and then, analyze the information. Incorporate artificial intelligence to help process and correlate large data sets to obtain deeper insights. AI platforms can help marketers spot and understand anomalies in the market behavior or campaign performance. In turn, they could act and tackle problems before they escalate.

Having a deeper understanding of the data could help predict future campaign performance as well. It could even aid forecast the growth and set realistic, achievable expectations. For example, here is screenshot of Yandex Metrika, where we can see number of visitor from each ad type and we could optimize which ad type give conversion and sales and which not.
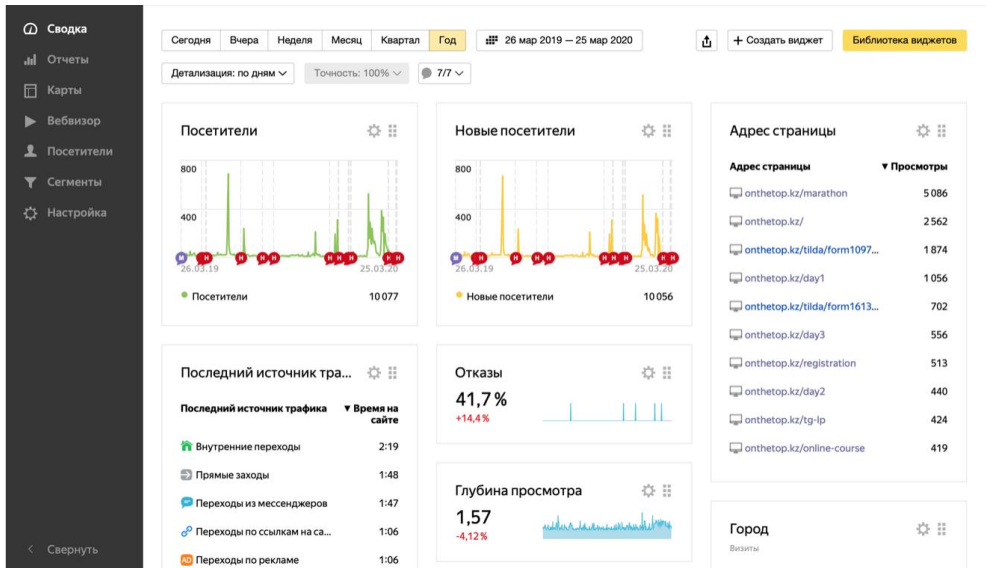
Figure 2. Statistics of web-site at the Yandex Metrika
Source: Author

Data and Results

As the result we can see how brands use AI in digital marketing:

1. Dynamic Product Recommendations

By far, the most recognizable example of artificial intelligence in marketing is Amazon using AI to recommend products for users.

Amazon's AI analyzes a person's past purchases and viewing history, and identifies products they are the most likely to buy next.

2. Dynamic Pricing

Car rental companies, hotels, and many other organizations use AI to monitor buying trends and determine the most competitive pricing. By doing so, they can offer customers prices based on external factors and their buying trends.

Similarly, many e-commerce stores use AI to monitor competitor prices as well as internal factors (like costs, etc.) to adjust pricing to an optimum point of competitiveness. For example, analyzing demand for our item and if it increases, we can increase price and as the result we can increase profit. The implementation is in progress.
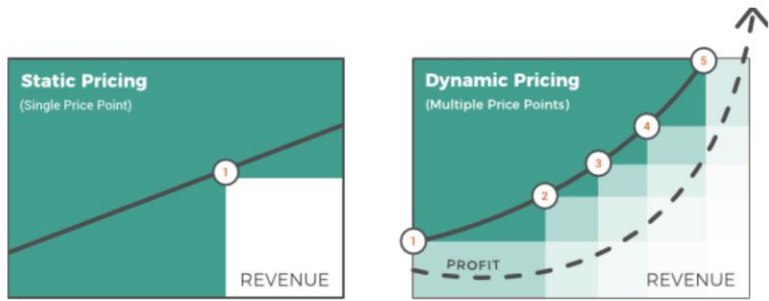
Figure 3. How Static and Dynamic Pricing could change revenue
Source: blog.prisync.com

3. Personalization

Spotify's AI analyzes each user's listening history to suggest other artists, records or playlists that should match their taste in music. And they use quite a sophisticated algorithm to do that. In our project we can give discount for people, who visited web-site 3 times and did not buy yet.

Discussion

Analyzing results we understand that AI in digital marketing has 3 advantages:

1. Faster data analysis. With artificial intelligence, marketers can analyze complex data sets faster than a human. But this increased speed doesn't mean greater efficiency only. Or the ability to gather and act on insights faster. It also suggests that organizations could reduce the time associated with processing information manually. As a result, they could launch more effective campaigns faster and deliver higher ROI at a lower cost.

2. More accurate insights. Using AI opens up the possibility to conduct a more in-depth analysis of the data. A machine-learning algorithm could break down complex data sets, correlate them with other information and deliver deeper insights. For a marketer, the above means finally having the ability to utilize more insights when planning campaigns. And also, being able to act much faster on those findings.

3. Greater efficiency. For them to work, today's marketing campaigns must be 100% relevant to the target audience. Unfortunately, many marketers lack data and insights to launch an initiative capable of engaging their intended audience. With AI, they can acquire all the insight they need and increase the efficiency of their efforts.

But AI in digital marketing also has disadvantage. It is creativity. In spite of many attempts, AI is still incapable of being creative. Machine learning algorithms can't act on the data in the same manner as a human would. And what goes with it, their ability to create something based on those insights remains

severely limited. That is just one reason why AI-created content lacks the magic touch making a blog post, article or even a Facebook Ad engaging.

Conclusion

In the end, it is clear that machine learning, big data and AI will help marketers do their job. From analytics to forecasting and endless optimization possibilities, digital marketing job will look a lot different in 10 years from now. Joe Pulizzi, founder of the famous Content Marketing Institute, has a very clear vision for the future of content creation: "In 10 years the majority of content will be generated by software. In 20 years, humans will wonder why we wasted so much time on content creation. I can't see any other way around this."

References

1 Gartner Customer 360 Summit 2011. Gartner.com. 2011. URL: https://www.gartner.com/imagesrv/summits/docs/na/customer-360/C360_2011_brochure_FINAL.pdf.

2 Artificial Intelligence for marketers 2018: finding value beyond the hype. Iab-switzerland.ch. October 2017. URL: https://www.iab-switzerland.ch/wp-content/uploads/2017/11/eMarketer_Artificial_Intelligence_for_Marketers_2018.pdf.

3 2016 Aspect consumer experience index. Aspect.com. October 26, 2016. URL: https://www.aspect.com/globalassets/2016-aspect-consumer-experience-index-survey_index-results-final.pdf.

4 Statt, N. AI is Google's secret weapon for remaking its oldest and most popular apps. Theverge.com. May 10, 2018. URL: https://www.theverge.com/2018/5/10/17340004/google-ai-maps-news-secret-weapon-remaking-old-apps-products-io-2018.

5 Abramovich, G. Consumer demand for personalized content reaches all-time high. Cmo.adobe.com. 2018. URL: https://cmo.adobe.com/articles/2018/1/adobe-2018-consumer-content-survey.html#gs.1n761y.

IRSTI 28.23.15

Y. Amirgaliev[1], A. Tastembekov[2], Sh. Bertailak[3]
[1,2,3]Suleyman Demirel University, Kaskelen, Kazakhstan

COMPUTER ANALYSIS OPTICAL COHERENCE TOMOGRAPHY IMAGES BY USING UNSUPERVISED MACHINE LEARNING ALGORITHM

Abstract. In recent years, computer image analysis has been developing rapidly. In the field of medicine has been identified to a new level that has greatly helped for the diagnostic system. There are many information systems in the field of ophthalmology and cardiology. Advanced technologies not only accelerate the work of doctors but also help to diagnose the disease in a timely manner and prescribe the treatment. In this research paper was carried out an analysis of the machine learning algorithm using a database of tomographic images of blood vessels in the eye system. Were studied the used methods for calculating several reasons in order to select a specific model, methods for calculating its properties and advantages. The main goal of this research is that doctors can not only check the current condition of the patient's eye but also diagnose certain diseases, such as diabetes and anemia.

Keywords: linear discriminant analysis, subretinal fluid segmentation, level set, local Gaussian pre-fitting energy**.**

*** ***

Аңдатпа. Сонғы жылдары суреттерді компьютерлік анализ жасау қарқынды дамып келе жатыр. Медицина саласында диагноз кою жүйесі үшін көптеген көмегін тигізу аркылы жаңа деңгейге шығарды. Қазіргі таңда офтальмология және кардиология саласында ақпараттық жүйелер көптеп кездеседі. Дамыған технологиялар дәрігерлердің жұмыстарын тездетіп қана қоймай ауру жағдайын ерте анықтап, ем тағайындауға көмектеседі. Бұл ғылыми мақалада көз жүйесіндегі қан тамырларының томографиялық суреттерің дереккорын қолдана отырып машиналық оқытудың алгоритмдерінің анализі жасалынды. Белгілі бір модельді таңдаудың бірнеше себептерін, оның қасиеттерін, кейбір артықшылықтарын және маңыздылығын есептеу үшін қолданылатын әдістерді зерттелді. Бұл зерттеу жұмыстарының басты мақсаты дәрігерлер өздерінің емделушінің көзінің қазіргі жағдайын тексеріп қана қоймай, диабет және анемия сияқты белгілі бір ауру жүйелеріне диагноз қоя алуы.

Түйін сөздер: сызықтық дискриминанттық талдау, сұйықтықтың субретинальды сегментациясы, деңгей жиынтығы, жергілікті Гаусстың алдын-ала орнатылатын энергиясы.

***

Аннотация. В последние годы компьютерный анализ изображений развивается быстрыми темпами. В области медицины был выведен на новый уровень, оказав большую помощь для диагностической системы. На сегодняшний день существует множество информационных систем в области офтальмологии и кардиологии. Передовые технологии не только ускоряют работу врачей, но и помогают своевременно диагностировать заболевание и назначать лечение. В данной научной статье был выполнен анализ алгоритма машинного обучения с использованием базы данных томографических изображений кровеносных сосудов в глазной системе. Были изучены используемые методы для расчета нескольких причин в целях выбора конкретной модели, а также методы для расчета его свойств и методы для расчета некоторых преимуществ и значимости. Основная цель этого исследования состоит в том, что врачи могут не только проверить текущее состояние глаза пациента, но и диагностировать определенные заболевания, такие как диабет и анемия.

Ключевые слова: линейный дискриминантный анализ, сегментация субретинальной жидкости, набор уровней, локальная гауссова энергия предварительной подгонки.

Introduction

Linear Discriminant Analysis (LDA) are methods used in statistics, pattern recognition and machine learning to find a linear combination of characteristics which describes or splits two or more classes of objects. The resulting combination may be used as a linear classifier. LDA is closely related to Principal Component Analysis (PCA) [2] for both of them are based on linear and matrix multiplication, transformations. In case of PCA, the transformation is based on minimizing mean square error between original data vectors and data vectors that can be estimated for the reduced dimensionality data vectors and the PCA does not considers any difference in class. However, for LDA the transformation is based on maximizing a ratio of "between-class variance" to "within-class variance" to lower data variability in the same class and increasing the separation between classes.

Main part

To find out LDA, we need to aware what is the "between-class variance" and "within-class variance". Then we have to maximize the ratio between these two. Assume we have a set of D-dimensional samples

$$X = \left\{x^1, x^2, ..., x^m\right\}, N_1 \tag{1}$$

of which belong to class C_1 and N_2 belong to class C_2. In our case, class C_1 is fluid associated region, and class C_2 is outer region, respectively. For this case we also assume the mean vector of two classes in X space:

$$u_k = \frac{1}{N_k} \sum_{i \in C_k} x^i \tag{2}$$

where $k=1,2$, and in y space:

$$\hat{u}_k = \frac{1}{N_k} \sum_{i \in C_k} y^i = \frac{1}{N_k} \sum_{i \in C_k} \theta^T x^i = \theta^T u_k \tag{3}$$

where $k=1,2$. One of the ways to define a measure of separation between two classes is to choose the distance between the projected means, which is in y space, so the between-class variance is:

$$\hat{u}_2 - \hat{u}_1 = \theta^T(\hat{u}_2 - \hat{u}_1) \tag{4}$$

and within-class variance for each class C_k is:

$$\hat{s}_k^2 = \sum_{i \in C_k}(y^i - \hat{u}_k)^2 \tag{5}$$

Final Fisher criterion in terms of some measure scatters as following:

$$J(\theta) = \frac{\theta^T S_B \theta}{\theta^T S_W \theta} \tag{6}$$

where

$$S_B = (u_2 - u_1)(u_2 - u_1)^T \quad (7)$$

$$S_W = \sum_k \sum_{i \in C_k} (x^i - u_k)(x^i - u_k)^T \quad (8)$$

The easiest way to maximize the object function J is to derive it and set it to zero.

$$\frac{\partial J(\theta)}{\partial \theta} = \frac{\partial}{\partial \theta}\left(\frac{\theta^T S_B \theta}{\theta^T S_W \theta}\right) \quad (9)$$

By solving above equation we get the direction of the θ, which is the:

$$\theta^* \infty S_W^{-1}(u_2 - u_1) \qquad (10)$$

Intensity inhomogeneity phenomenon presents a systematic change on intensities of both object and background and usually manifests itself as a smooth spatially varying function across the image [3]. A novel region based model is proposed to segment image with intensity inhomogeneity. The model consists of three components: linear discriminant analysis, region scalable fitting energy and regularization term of the level set function. The local discriminant analysis is used to classify pixels to background and foreground, while energy functional and regularization term are used to differentiate the image differences between the foreground and the background of an object, and iteratively evolve the initial contours. According to above analysis, new feature space obtained by linear discriminant analysis can be incorporated into the LBF energy functional to assist in image segmentation. So the final energy functional can be expressed as:

$$E^{RSFLDA} = \sum_{i=1}^{2} \iint K_\sigma(x, y)\left[|I(y) - f_i(x)|^2 + \alpha|Y(y) - u_i(x)|^2\right] \times H_i(\phi(y))dydx. \quad (11)$$

where α is nonnegative constant and $Y(y)$ is a new feature space obtained from Eq.(1). α is a parameter of linear discriminant analysis (LDA) term, it used to balance the effects of LDA term. $f_i(x)$ and $u_i(x)$ denote the intensity means for the image $I(x)$ and $Y(x)$, accordingly. By combining the regularization term and energy functional, the final fitting energy functional is given by:

$$\mathrm{E}(\phi) = E^{RSFLDA} + \mu P(\phi) \quad (12)$$

$E(\phi)$ is minimized with respect to the functions $f_i(x)$ and $u_i(x)$, which satisfy the following:

$$f_i(x) = \frac{\int K_\sigma(x,y)H_i(\phi(y))I(y)dy}{\int K_\sigma(x,y)H_i(\phi(y))dy} \quad (13)$$

$$u_i(x) = \frac{\int K_\sigma(x,y)H_i(\phi(y))Y(y)dy}{\int K_\sigma(x,y)H_i(\phi(y))dy} \quad (14)$$

Keeping $f_i(x)$ and $u_i(x)$ fixed, $E(\phi)$ is minimized with respect to ϕ, resulting in the evolution formula of the level set function ϕ:

$$\frac{\partial \phi}{\partial t} = -\delta(\phi)\left(e_1 - e_2 + v\,div\left(\frac{\nabla \phi}{|\nabla \phi|}\right)\right) + \mu\left(\nabla\phi - div\left(\frac{\nabla \phi}{|\nabla \phi|}\right)\right) \quad (15)$$

$$e_i = \int K_\sigma(x,y)\left(|I(y) - f_i(x)|^2 + \alpha|Y(y) - u_i(x)|^2\right)dy, \quad i=1,2 \quad (16)$$

where $\delta(\phi)$ is the derivative of the function $H(\phi)$, $div(.)$ denotes the divergence operator, and $e_i(x)$ simultaneously quantifies the image difference between foreground and background for the original image. In contour evolution, the level set function ϕ was initially assigned to a positive constant 1 outside a region and -1 inside. σ was assigned to 25 to balance the convergence rate and computational efficiency. Δt and μ were related by $\Delta t * \mu = 0.1$ to satisfy the Courant Friedrichs Lewy (CFL) condition for numerical stability [4] and they were set $\Delta t = 0.1$, $\mu = 1$, respectively. The parameter v was set $v = 0.007 \times 255 \times 255$.

Fig. 1 gives the preview of our system. Automated initialization stage targets to find candidate fluid zone by estimating region of interest. Then level set method with Linear Discriminant Analysis is applied to segment subretinal fluid.
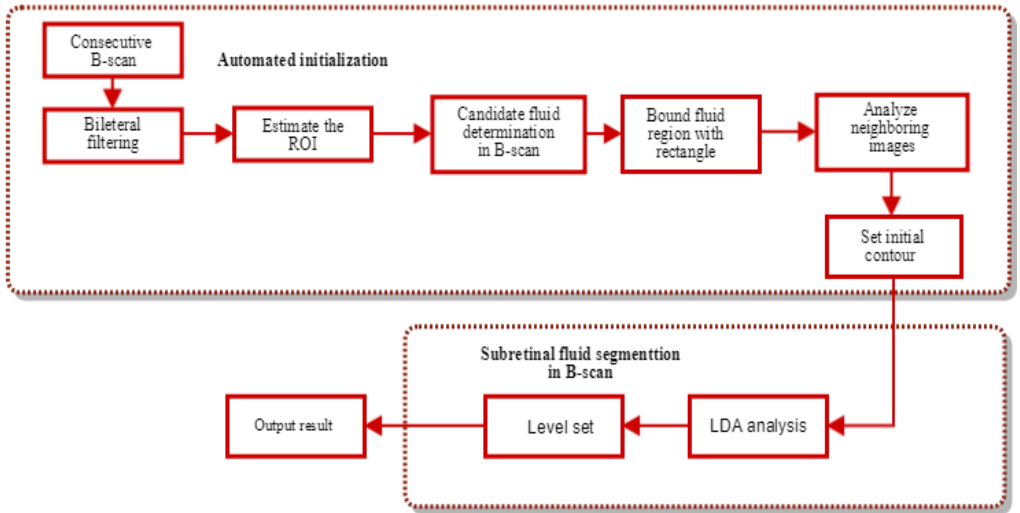
Fig. 1 Overview of proposed method

Result

The developed linear discriminant analysis is used to construct the intensity fitting term $|Y(y) - u_i(x)|^2$. This causes that the proposed method has potential for handling intensity inhomogeneity and avoiding unnecessary contour evolution in segmentation by classifying image information to foreground and background, respectively. To demonstrate the performance of the proposed method, 23 longitudinal SD-OCT cube scans from 12 eyes of 12 patients acquired with the Cirrus OCT device (Carl Zeiss Meditec, Inc., Dublin, CA) were used in which all the subjects were diagnosed with CSCR with only NRD. Fig. 4.2 and Fig.4.3 demonstrates the performance of proposed model to segment NRD associated subretinal fluid. In a qualitative comparison (Fig. 4.2), the proposed method provided a smooth boundary of the fluid region, while the LPHC and SS-KNN method do not guarantee the smoothness of the contour. The LPHC method suffers from a strong label propagation constraint. If the retinal structure changes dramatically, the regions might be segmented (delineated by the dashed yellow ellipse).The automatic layer segmentation is not always correct, which may result in failure of layer segmentation method results, because of NRD which affects to retinal layer structure. Our model surpasses other state-of-art methods and generates the segmentation results

similar to the ground truths. The results in Table 1 summarize the PPV and DSC. Overall, the proposed method is capable to produce a higher segmentation results without utilizing any layer segmentation results.
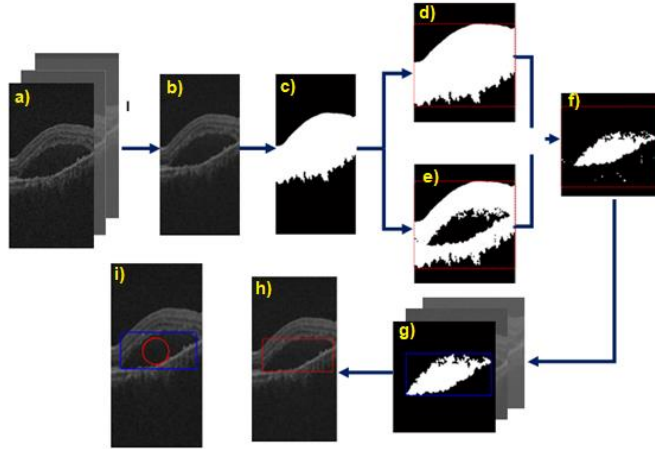
Fig. 2 Flowchart of processing

Table 1. To summarize the quantitative findings (mean ± standard deviation) between the segmentations and the manual gold standards (segmentations of two individual experts).

Methods	Expert 1		Expert 2	
	PPV	DSC	PPV	DSC
LPHC[9]	54.6±12.3	64.3±9.4	54.8±11.8	64.7±9.5
SS-KNN [22]	90.9±3.8	85.1±3.1	90.8±2.8	84.9±3.1
FLSCV [4]	85.2±6.3	77.9±20.7	85.8±6.3	78.4±1.2
CMF [23]	92.0±2.4	92.9±1.5	93.0±2.5	93.3±1.6
EFD [5]	92.0±3.8	92.7±3.0	93.1±4.3	93.6±3.1
Proposed	95.52±0.013	93.79±1.2	96.59±0.1	94.4±1.6

Conclusion

In summary, we report a fully automatic method for the segmentation of subretinal fluid. Our framework can handle intensity in homogeneity which can

be seen in B-scan images. Compared with the other existing methods, the advantage of our method as follows: firstly, this method limits the spatial extent of the fluid region in B-scans by incorporating region of interest and thus improves the segmentation performance. Second, the experimental results reveal that two-stage automatic framework is robust to possible errors of automatic layer segmentation compared with SS-KNN method. Furthermore, linear discriminant analysis based level set segmentation can provide a smooth boundary of the subretinal fluid.

References

1 Taubaldy, N., Ji, Z. Beyond Retinal Layers: An Automatic Active Contour Model with Pre-Fitting Energy for Subretinal Fluid Segmentation in SD-OCT Images. *2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*, Chongqing, 2018, pp. 326-330.
2 Wang, L., Chen, G., Shi, D., Chang, Y., Chan, S., Pu, J., Yang, X. Active contours driven by edge entropy fitting energy for image segmentation. *Signal Processing,* (2018): pp. 27-35.
3 Wang, L., Zhu, J., Sheng, M., Cribb, A., Zhu, Sh., Pu, J, Simultaneous segmentation and bias field estimation using local fitted images. *Pattern Recognition,* 74 (2018): pp. 145-155.
4 Lawi, A., La Wungo, S., Manjang, S. Identifying irregularity electricity usage of customer behaviors using logistic regression and linear discriminant analysis. *3rd International Conference on Science in Information Technology (ICSITech),* (2017): pp. 552-557.
5 Wu, M., Chen, Q., He, X.J., Li, P., Fan, W., Yuan, S.T., Park, H. Automatic Subretinal Fluid Segmentation of Retinal SD-OCT Images With Neurosensory Retinal Detachment Guided by Enface Fundus Imaging. *IEEE Transactions on Biomedical Engineering*, (2018): pp. 87-95.
6 Ji, Z., Xia, Y., Sun, Q., Cao, G., Chen, Q. Active contours driven by local likelihood image fitting energy for image segmentation. *Information Sciences*, (2015): pp. 285-304.

Б.К. Жолдасов[1], Г.С. Рысмендеева[2]
[1,2]Казахский национальный исследовательский технический
университет имени К.И. Сатпаева, г. Алматы, Казахстан

ПРЕОБРАЗОВАНИЕ БАНКА В ОТКРЫТУЮ ЭКОСИСТЕМУ API

Аннотация. Работа посвящена преобразованию банка в открытую экосистему API. В статье будет рассматриваться факторы внедрения открытой экосистемы API в банки, связанные с этим возможности и банковской отрасли и описываются успешные API стратегии.

Ключевые слова: Открытая экосистема API, факторы внедрения, возможности и угрозы для банковской отрасли, успешная стратегия API, информационная безопасность.

***

Аңдатпа. Бұл жұмыс Банктің API ашық экожүйесіне айналуына арналған. Мақалада банктерде open API экожүйесін енгізу факторлары қарастырылады. Мақалада банк саласы үшін мүмкіндіктер мен қауіп-қатерлер, сондай-ақ API табысты стратегиялары қарастырылады.

Түйін сөздер: API ашық экожүйесі, енгізу факторлары, банк саласы үшін мүмкіндіктер мен қауіптер, API табысты стратегиясы, ақпараттық қауіпсіздік.

***

Abstract. The work is devoted to the transformation of the Bank into an open API ecosystem. The article discusses the factors for implementing an open API ecosystem in banks. The article also discusses the opportunities and threats for the banking industry and also discusses successful API strategies.

Keywords: Open API ecosystem, factors for implementation, opportunities and threats for the banking industry, successful API strategy, information security.

Введение
«Открытый» недавно стал новым модным словом в индустрии финансовых услуг, то есть открытые данные, открытые API, открытые банковские операции.

Термин «открытый» означает способность компаний предоставлять свои услуги внешнему миру, с тем чтобы внешние партнеры или даже конкуренты могли использовать эти услуги для того, чтобы принести дополнительную ценность своим клиентам. Эта тенденция стала возможной благодаря технологической эволюции открытых API (интерфейсов прикладного программирования), которые являются цифровыми портами, делающими эту связь возможной.

Компании, связанные между собой через открытые API, образуют настоящую экосистему API, предлагая лучший в своем роде опыт работы с клиентами, объединяя цифровые услуги, предлагаемые несколькими компаниями.

В технологическом секторе эта эволюция продолжается уже несколько лет в секторе путешествий, позволяющем вам забронировать онлайн любую гостиницу. Отличный пример-история успеха Uber [1]. Всего за несколько лет эта компания приобрела рыночную капитализацию, которая больше, чем у BMW. Это в то время как Uber в основном объединяет несколько API-сервисов, предлагаемых другими компаниями, т. е.

- Позиционирование осуществляется операционной системой (iOS, Android);
- Расчет маршрута и карты предоставляются MapKit и Google Maps;
- Twilio отправляет клиентам текстовые сообщения в реальном времени;
- Оплата производится компанией Braintree;
- Квитанция отправляется через Mandrill;
- Сервисы размещаются в облаке Amazon Web Services (AWS).

Объединение этих лучших в своем роде API-сервисов позволяет стартапам, таким как Uber, предоставлять отличный и инновационный пользовательский опыт в очень короткие сроки, что способствует быстрому росту.

После этого эти стартапы обычно предоставляют свои собственные API, которые, в свою очередь, интегрированы в предложение других компаний. Например, API Uber также интегрирован в приложение United Airlines.

Эти примеры показывают взаимные выгоды такой открытой экосистемы API, т. е. компания, ориентированная на клиента, может предоставлять дополнительные услуги своим клиентам, в то время как компания, предоставляющая услуги, может получать прибыль от более широкого использования своих API. Это приводит к увеличению доходов обеих компаний.

Пример Uber, безусловно, не является единичным случаем, например, UPS успешно увеличила свою долю рынка, интегрировав свои API в интернет-магазины, или eBay генерирует уже 60 процентов своих доходов через свои API (например, API для отправки товара на листинг на eBay).

Банковская отрасль, традиционно довольно медленно интегрирующая новые технологии, также будет испытывать все большее и большее воздействие. Открытый банкинг становится новой тенденцией, подталкиваемой растущими и меняющимися потребностями клиентов, конкуренцией финтехов (есть финтех-компания для каждой услуги, предлагаемой банками) и регуляторами, подталкивающими банки открывать свои данные и архитектуру (например, PSD2 (Payment Service Directive 2) директива о платёжных услугах), все еще подчиняясь растущим правилам защиты клиентов (например, GDPR (General Data Protection Regulation) европейский генеральный регламент о защите персональных данных). В отчете Digital Banking [2] за 2018 год руководители банков назвали открытый банкинг четвертым по значимости трендом 2018 года. В версии этого отчета за 2016 год эта тенденция не была даже в первой десятке.

Факторы внедрения

Быстрое внедрение открытых банковских операций обусловлено многочисленными эволюциями в банковской отрасли:

- – Потребности клиентов растут и меняются: клиенты требуют мульти-и кросс-канальный опыт, который доступен в режиме реального времени и 24/7. Кроме того, опыт должен быть ориентирован на клиента, а не на продукт-ориентированный подход, который в настоящее время предлагают большинство банков. Например, клиенты требуют, чтобы банки предлагали такие услуги, как полное целостное управление личными финансами (т. е. включая активы и обязательства, хранящиеся в других финансовых учреждениях). Это дает клиентам не только возможность управлять своими бюджетами, но и немедленно запускать внутренние и внешние сервисы из анализа, происходящего в этом модуле. Примером внутренней услуги может быть инвестирование избыточных денег в ценные бумаги, в то время как примером внешней услуги может быть автоматическое предложение и управление переключением от коммунальной компании, когда сравнение с коллегами показывает, что клиент платит слишком много за свои коммунальные услуги.

– Регуляторное давление: регуляторы (особенно в Европе) все больше подталкивают банки к тому, чтобы открыть свою архитектуру, с помощью PSD2 (Payment Service Directive 2) [3] в Европейском Союзе и открытой банковской инициативы CMA (Competition and Market Authority) в Великобритании. Оба постановления направлены на усиление конкуренции в сфере финансовых услуг (с целью предоставления потребителям более качественных услуг при более низких затратах) путем навязывания банкам права разрешать третьим лицам напрямую получать информацию о счетах и другую информацию от банков. Например, инициатива Open Banking обязывает банки делиться информацией о продуктах и услугах (например, ценами, сборами, условиями и положениями) и информацией о клиентах (например, информацией о счете и возможностью осуществлять платежи напрямую).

– Новые технологии: быстрые технологические изменения в отрасли (IoT, анализ больших данных, аналитика клиентов в реальном времени, искусственный интеллект, блокчейн...) делают практически невозможным для банка инвестировать (и быть на вершине) в любую новую технологию. Поэтому партнерство со специализированными компаниями является почти необходимостью, чтобы оставаться впереди всех этих технологических эволюций. Кроме того, этим партнерствам должна способствовать открытая архитектура API.

Возможности и угрозы для банковской отрасли

Создание открытых API-экосистем открывает перед банковской отраслью несколько возможностей, но и создает значительные угрозы.

Банки, не открывающие свою архитектуру и не участвующие в этих экосистемах API, как ожидается, потеряют больше всего. Интересно процитировать здесь BBVA [4] (Banco Bilbao Vizcaya Argentaria - одна из крупнейших банковских компаний в Испании): «компания без API-это как компьютер без интернета». В то же время выгоды, которые получат банки, участвующие в таких экосистемах, также будут сильно зависеть от той роли, которую банк будет играть в экосистеме.

При самом оптимистичном сценарии Банк будет центральным игроком в экосистеме, управляющей клиентской принадлежностью. Финтехи будут конкурировать друг с другом, чтобы получить доступ к клиентской базе банка. В результате банк сможет выбирать между различными финтех-игроками, выбирая тот, который предлагает лучшие услуги для клиентов банка, и тот, который предоставляет лучшие условия

для банка. В этом сценарии инновации обходятся банку очень дешево, т. е. новые игроки могут экспериментировать с новыми подходами, причем банку не придется вкладывать деньги в эти испытания.

С другой стороны, вполне возможно, что финтех-компании (или, возможно, один из технологических гигантов Gafa, например Google, Apple, Facebook или Amazon) будут лидировать в экосистеме. В этом сценарии финтех-компания будет получать большую часть прибыли и управлять отношениями с клиентами, в то время как банкам придется конкурировать друг с другом, чтобы предлагать базовые (невидимые для клиента) банковские услуги и продукты. В этом сценарии банки будут сведены к роли невидимых поставщиков сырьевых услуг.

Сторона, управляющая отношениями с клиентами, не только получит большую часть прибыли, но и получит доступ к данным клиента, которые могут быть использованы для тонкой настройки и персонализации клиентского опыта и увеличения возможностей кросс-продаж.

Трудно предсказать, какую «роль» банки будут играть в этих будущих экосистемах, но ближайшие годы будут иметь решающее значение для того, чтобы банки заняли доминирующее положение. У банков, безусловно, есть много преимуществ, таких как более широкое предложение услуг, дополнительное и улучшенное распределение и усиленное смягчение рисков.

При сравнении банков с финтехами сегодня оба имеют конкурентные преимущества. Партия, которая сможет наилучшим образом использовать свои преимущества и улучшить свои недостатки, выиграет эту «гонку» за то, чтобы стать доминирующим актором в экосистемах:

- Преимущества банка;
- Надежные бренды;
- Большая клиентская база;
- Разнообразные продукты и услуги;
- Уникальный опыт работы в банковской сфере;
- Банки обладают уникальными знаниями о клиенте;
- Доступ к большому объему капитала;
- Многоканальный опыт;
- Банки имеют всю необходимую инфраструктуру для обработки, клиринга и расчетов платежей, ценных бумаг;
– Недостатки и проблемы банка:

- Длинные и дорогостоящие циклы изменений: самое большое препятствие для банков, чтобы конкурировать с финтехами, вероятно, заключается в их неспособности быстро и эффективно развивать свои ИТ-приложения. В основном это происходит по двум причинам:

1. Унаследованные системы: большинство банковских услуг были построены поверх унаследованных систем, которые были построены десятилетия назад и не адаптированы к современным цифровым требованиям. Переход к открытому банку, предоставляющему привлекательные и инновационные API-сервисы, создаст огромную проблему трансформации, которая потребует значительного времени и денег.

2. Банковская культура: из-за их долгой истории ИТ, их сложной архитектуры приложений и присущей им склонности к риску банки имеют культуру медленных, но устойчивых изменений. Это находит свое отражение в крупных и сложных релизах один или два раза в год, широко распространенном использовании традиционных методологий разработки и том факте, что ИТ подразделение часто все еще рассматривается как непрофильный центр затрат, имеющий мало полномочий на принятие решений (т. е. банки не сделали переход к превращению в «технологическую компанию»).

Независимо от того, какую роль банк будет играть в экосистеме, клиент, безусловно, получит наибольшую выгоду от этой эволюции:

– Повышенная конкуренция, ведущая к снижению цен и улучшению уровня обслуживания

– Большая прозрачность, т. е. будет легче сравнивать различные финансовые продукты и услуги. Этому будут способствовать веб-сайты, которые позволяют напрямую сравнивать цены (cfr. Booking.com по ценам гостиниц).

– Новые формы распространения, т. е. клиент сможет инициировать финансовые услуги и продукты с веб-сайтов других компаний в других секторах (например, розничных торговцев). Клиент также сможет запускать нефинансовые услуги с сайта Банка.

Успешная стратегия API

Решающее значение для успешной стратегии API имеет понимание того, что открытый API-это также коммерческий бизнес-продукт, а не просто технический интерфейс. Таким образом, конвертация банковских услуг в открытые API должна быть не просто техническим ИТ-проектом, а ориентироваться на бизнес. Это означает, что банки должны нанимать менеджеров по продуктам API на стороне бизнеса.

Успешный открытый API должен позволять:

– Создание новых потоков доходов, т. е. монетизация API. Возможны различные модели монетизации:
  - Конечные пользователи, оплачивающие транзакционные сборы за использование решения;
  - Партнеры и/или разработчики, оплачивающие услуги/использование данных;
  - Партнеры и банки, заключающие соглашение о совместном использовании доходов, такие как реклама с оплатой за клик (т.е. выход из традиционных соглашений о лицензионно оплате за продукт/услугу);
– Улучшение качество обслуживания и удовлетворенность клиентов, т.е. API должны быть разработаны для клиентов, т. е. предоставлять клиенту ценную услугу, а не только продукты и необработанные данные (например, историю транзакций со счета). Это может быть достигнуто путем обогащения необработанных данных (например, добавление классификации к истории транзакций счета) или путем добавления дополнительных услуг на основе необработанных данных (например, предоставление сберегательного или инвестиционного предложения на основе необработанных данных истории транзакций).
– Получение большего объема данных: сбор большего количества данных о клиентах, что позволяет получить лучшую информацию о клиентах, которая, в свою очередь, может быть использована для повышения доходов (например, через кросс-продажи) и обслуживания клиентов и удовлетворения их потребностей.

Кроме того, успешная стратегия API должна быть направлена не только на исходящие API, то есть на API, предоставляемые компанией финансовых услуг. Компании, предоставляющие финансовые услуги, также должны иметь стратегию использования API от других компаний (например, финтех-компаний). Это позволяет быстро создавать новые сервисы, опираясь в дальнейшем на функционал, предоставляемый компаниями-партнерами.

Заключение

Банки должны уже сейчас перейти к адаптации своей внутренней архитектуры, чтобы предоставить четко определенные и хорошо документированные услуги внешнему миру. Вместо того, чтобы делать только голый минимум (т.е. платежи и информацию о счете), требуемый регуляторами (т.е. PSD2) [4], банки должны уже начать открывать и другие

свои продукты и услуги (т.е. ценные бумаги, кредиты, страхование и др.) [5]. Эта стратегия предоставления продуктов и услуг в качестве API не только позволит бизнесу банка исследовать новые возможности, но и подтолкнет ИТ-организации к реструктуризации, позволяя им эволюционировать в более гибкую, ориентированную на клиента организацию.

Список использованной литературы:

1   Uber. URL: https://developer.uber.com/.
2   Abrosimova, K. 5 Reasons to Integrate Uber API. URL: https://yalantis.com/blog/5-reasons-think-uber-api-integration-app/.
3   Digital Banking. URL: https://www.digitalbankingreport.com/.
4   Open Bank Project PSD2 Suite. URL: https://www.openbankproject.com/psd2.
5   BBVA. URL: https://www.bbva.com.

IRSTI 49.03.05

Sh. Habiburahman[1], O. Baimuratov[2], N. Abdinurova[3]
[1,2,3]Suleyman Demirel University, Kaskelen, Kazakhstan

ANALYSIS OF QUANTUM CRYPTOGRAPHY AND TECHNOLOGIES IN INDUSTRIES

Abstract. In today's connected world it's crucial to make sure telecommunication is not a risk. Eavesdroppers will always find a way to attack and harm big companies systems or governmental databases. It's very important to find the best possible way to keep our services safe. Quantum cryptography is one the best way since it's based on rules of quantum physics. In this paper we are going to analyse the best solutions, protocols and different aspects of encryption. Real life implementations by different IT companies and investors will also be included in this paper. Weakness and pros always exist in every system and it's impossible to indicate the system we are proposing is not breakable but it's going to be the best possible solution for now. Why? It's going to be discussed in later sections.

Keywords: Index Terms—Quantum technologies, Qubit, Quantum gates, Transmission, Quantum cryptography.

***

Аңдатпа. Қазіргі заманауи әлемде телекоммуникацияның қауіпті емес екендігіне көз жеткізу керек. Қателер әрдайым компанияның ірі жүйелеріне немесе мемлекеттік дереккорларға шабуыл жасаудың және бүлдірудің жолын табады. Біздің қызметтеріміздің қауіпсіздігін қамтамасыз етудің жақсы әдісін табу өте маңызды. Кванттық криптография - бұл жақсы әдістердің бірі, өйткені ол кванттық физика ережелеріне негізделген. Бұл мақалада біз ең тиімді шешімдерді, хаттамаларды және шифрлаудың әртүрлі аспектілерін талдаймыз. Бұл мақалада әр түрлі IT компаниялары мен инвесторлардың нақты енгізулері қосылады. Кемшіліктер мен атрықшылықтары әр жүйеде әрқашан бар және біз ұсынып отырған жүйенің бұзылмайтындығын көрсету емес, бірақ қазіргі уақытта бұл ең жақсы шешім болып табылады. Неге? Бұл келесі бөлімдерде талқыланады.

Түйін сөздер: кванттық технологиялар, кубит, кванттық қақпалар, беріліс, кванттық криптография.

***

Аннотация. В современном соединенном мире важно убедиться, что телекоммуникации не представляют опасности. Подслушивающие всегда найдут способ атаковать и наносить вред системам больших компаний или правительственным базам данных. Очень важно найти наилучший способ обеспечить безопасность наших услуг. Квантовая криптография - один из лучших способов, поскольку она основана на правилах квантовой физики. В этой статье мы собираемся проанализировать лучшие решения, протоколы и различные аспекты шифрования. Реальные реализации различных ИТ-компаний и инвесторов также будут включены в эту статью. Слабость и плюсы всегда существуют в каждой системе, и невозможно указать, что предлагаемая нами система не поддается разрушению, но на данный момент это будет наилучшее возможное решение. Почему? Это будет обсуждаться в следующих разделах.

Ключевые слова: квантовые технологии, кубит, квантовые врата, передача, квантовая криптография.

Introduction

Keeping the data and information safe is the most important thing and with the development of technology breaking any security systems or accessing any secure systems were becoming easier. Everyone was looking for something new in order to stop hackers or eavesdroppers. Quantum physics was the only hope and researchers thought of using quantum physics which seems they have made the right decision by applying the quantum rules on quantum cryptography. European union and big companies like IBM [1], Ali Baba [2] and Microsoft [3] announced their interest and that they are willing to invest and build a secure communication system based on this technology which is known as SECOQC [4] or secure communication based on quantum cryptography. Of course, Quantum computers and quantum algorithms also received a lot of interest in the past. Quantum mechanics [5] is the reason behind the technology that we are using today. It's mainly because it has the ability to do some tasks better and faster than classical cryptography.

Limitations of modern cryptography

As we know cryptography is the process of exchanging information in the presence of a third party called adversaries). Or in simple words it's about constructing and analyzing protocols that block adversaries. Since World War I, the methods used to carry out cryptology[6] have become an interest for many big IT companies because everyone noticed that using computers are very

helpful but not secure if there's no way to keep the data secured. It protects your identity, transactions, and prevents your competition from accessing and reading your confidential documents. Although it's very important now but in the future it will become more and more vital. Eavesdroppers will always find a way to harm a system and they don't need many vulnerabilities, one is enough for them to turn down the whole system. Today's security systems might be safe but not forever. Once your application is being used widely it will become a target for criminals. No matter how great your application or a system is, it measures by its security system in the market. It's impossible to guarantee 100 percent security. But it's possible to work toward 100 percent. Since calculations are relatively slow in public key cryptography, they exchange keys instead of encrypting the data. RSA and Diffie Hellman [7] are used widely to distribute symmetric keys between users. However, as we already know that asymmetric encryption is a lot slower than symmetric, that's why the best possible way is to use the advantage of the speed of a public key system in order to exchange symmetric key. RSA and Diffie-Hellman are not based on concrete mathematical proofs that's why encryption algorithms could be defeated soon or later. It's true that the current Cryptosystems may be good but in future it might not provide enough confidentiality with advancements in technology and computer systems. In the past DES [8] with 56 bit keys was secure enough but nowadays it's not considered to be secure enough since the advancement in technology has proven it wrong. Or also we could say quantum computing could break the RSA with the matter of time. It's impossible to say that today's cryptosystem [9] is not hackable but we can say for sure that it's possible to break any cryptosystem with the manner of time. Or a theory could be developed in the future that proves that cryptosystems are vulnerable. If it became true that means that large organizations, governments and other affected institutions should spend a lot of money to create and deploy a new cryptography system as fast as possible.

Quantum cryptography in theory

Quantum encryption [10] has two pillars, one is the Heisenberg Uncertainty principle [11] and the second one is principle of photon polarization [12]. Heisenberg claims that it's impossible to measure the quantum state of any system without distributing it. On the other hand photon polarization of light particles can only be known when it's measured. It plays an important role to stop the eavesdroppers from attacking. Secondly, principles of polarization explain how light photons can be oriented in specific directions. In other words a photon filter can detect only a polarized photon with a correct polarization or it will be destroyed. This is the reason why quantum cryptography is a better option for ensuring the privacy of our data and stopping attackers. In 1984 Charles Bennet and Gilles Brassard [13] developed the concept of quantum

cryptography. Depending on the amount of photons reaching to a receiver it's possible to create an encryption key which corresponds to the fact that light can behave with the characteristics of particles in addition to light waves photons can be polarized at various orientations and Zeros and ones represent the bits that can be used by orientations. The foundation of quantum cryptography is polarized photons that serve as the important principles of quantum key distribution. Although the strength of the modern (digital) cryptography depends on factoring large numbers but quantum cryptography completely depends on physics rules and is also not dependent on the processing power of current computing system That's quantum cryptography has the answer to the problems that current cryptography suffers from. And being worried about the computing power of eavesdroppers or a theory that has the ability to quickly solve the large integer factorization problem is no longer required.

Quantum key distribution example

In this section we are going to provide an example of how Quantum cryptography distributes keys [14] securely. It includes a sender, receiver and a malicious eavesdropper which is called in order Alice, Bob and Eve. Alice sends a message to Bob using a photon gun . This gun will send a stream of photons in an opposing direction which is randomly chosen in one of four polarization that could be vertical, horizontal or diagonal. Bob will randomly choose a filter for each photon and use a photon receiver to measure the polarization which is either diagonal (45 or 135) and rectilinear (0 or 90) and keeps a log of correct measurement that has been selected by Alice and the incorrectly measured will be discarded while the correct ones are translated into bits on their polarization. They will be used to send encrypted information. The important thing about this key is that both parties neither sender or receiver can't determine in advance what the key will be. The reason behind that is because it is the product of their random choices. Let's suppose even if an attacker defeats the quantum key distribution she must also randomly select either a diagonal or a rectilinear filter to measure Alice's photon correctly. It's true that Eve will have an equal chance of selecting the right or wrong filter but he won't be able to confirm with Alice the type of filter he used. Which means that Eve can't interpret the final key or the photon that forms the final key and can't do anything. First of all, according to the Heisenberg Uncertainty principle photons will be destroyed once they are measured and will no longer exist. That's why they can not be duplicated. Secondly, in order to know the length of the one time path since it corresponds to the length of the message, sender and receiver must calculate the amount of photons which is required to form the encryption key.
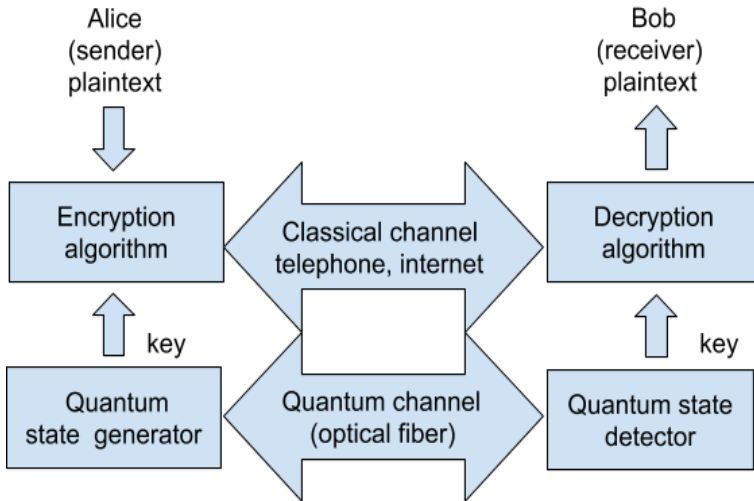
Fig. 1. Quantum key distribution example

Bob should receive about 25 percent of transmitted photons if not he can be certain that there's something wrong. The fact is that a photon will no longer exist to be detected by Bob. Even if an eavesdropper tries to create a photon and pass it to Bob, she must be lucky to randomly choose its orientation correctly too since the chances of not being correct is 50 percent is enough to reveal her presence.

1 - Alice sends a random sequence of photons polarized horizontal, vertical, right circular And left circular;

2 - Bob measures the photons polarization in a random sequence of bases, rectilinear (+) and circular;

3 - result of Bob's measurement (some photons may not be received at all);

4 - Bob tells Alice which bases he used for each photon he received;

5 - Alice tells him which bases were correct;

6 - Alice and Bob keep data only from these correctly measured photons discarding all the rest;

7 - This data is interpreted as a binary sequence according to the coding scheme = = 0 and = = 1.

Fig. 2. Basic quantum key distribution protocols signs.

Confidentiality of keys

It is possible that Diffie-Hellman may perhaps be broken in the future by eavesdropping. Beside this classic secret system has suffered from different problems due to the insider threats or some other problems. Also public key suffers from ongoing uncertainty and mathematically its intractable and its widely used as internet security architecture nowadays. Since QKD [15] is capable of providing automatic distribution of keys that may offer more security, we can assume it as properly embedded techniques and overall secure system.

QKD protocols implementation

Many aspects of QKD protocols [16] are unusual both in motivation and implementation and it might be an interest in communication protocols for specialists. Because quantum cryptography contains specialized protocols which are called as QKD protocols.
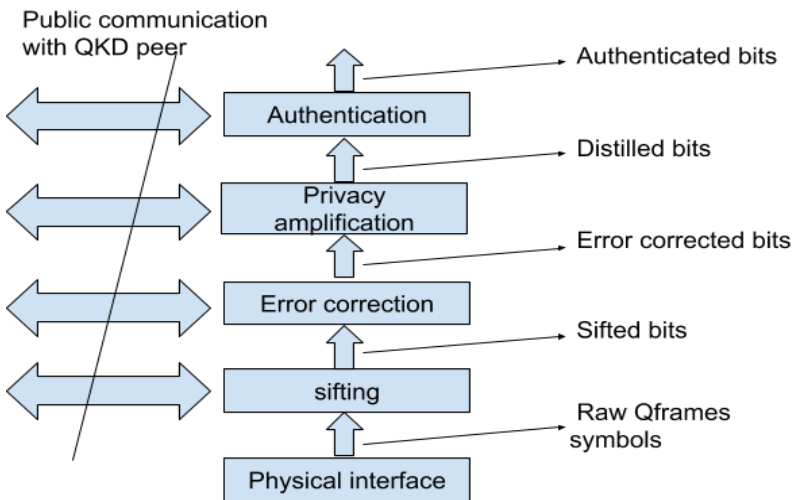

Fig. 3. QKD protocol implementation.

The protocols that we are talking about here are running in C language which is designed by DARPA that makes plugging new protocols easier and it's also possible that they invent and practice new QKD protocols in coming years. These protocols are more like pipeline stages and could be examples as sub layers.

Quantum solution and tools in industries

Nowadays , it's almost impossible to imagine a company or a big organization without using IT facilities. Banking systems, nuclear power plants, aircrafts, satellites and space crafts, all of them are being controlled and measured by their security level. Availability, integrity and confidentiality are the main factors in development secure telecommunication systems. Cryptographic systems are the best way to ensure they are working effectively. This is a great system but there's a problem which is Key distribution, but it can be solved with the help of SECOQC. After analysing different papers it seems that QKD could be an alternative solution for key distribution problems. Quantum key distribution protocols are used to generate keys and distribute them between two parties using quantum and classical channels. The first protocol was proposed by Bennett and Brassard from IBM and Montreal university in 1984 using single qubit with polarization states. (0, 45, 90, 135) are the four polarization states of photons.

Authentication

Authentication job is to guard Alice and Bob against attacks like "man in the middle attacks". It helps to make sure that Alice is communicating with Bob not eavesdroppers and vice versa. Since eavesdroppers may get into the conversation between Bob and Alice at any stage that's why it's recommended to perform authentication on an ongoing basis for all key management traffic.

Types of cryptography	Description	Advantages	Limitations
Modern cryptography (DES (Tuchman, 1997), IDES (Dang and Chau, 2000), AES (Zeghid et al., 1996), RSA (Cormen et al., 2001).	Algorithms operate on strong mathematical concepts that make them computationally efficient for protection and secrecy of highly sensitive.	Non-dependency on the medium colossal communication range multiple platforms for implementation. very high security.	Absolutely impractical because of the inherent properties of image such as bulk data capacity, strong correlation among adjacent pixels and high redundancy.
Quantum cryptography or quantum key distribution (QKD)	Makes use of the secret key whose randomness and secrecy are assured based on the Heisenberg uncertainty principle of physics.	The QKD would be unconditionally secure even with the endurance of quantum computer and with the users can perform QKD without quantum	Weak properties of coherent pulses and the detectors used in the implementation of QKD (Valerio and Christian, 2014).

Fig. 4. QKD comparison.

Based on hash functions introduced by Wegman and Carter [17] the solution to the authentication problem and discussed a solution. To solve the authentication problem Alice and Bob should already share a secret key in order to use a hash function from the family and generate an authentication between them. With the use of hashing the chances of accessing or eavesdropping between two parties is really low no matter how high the system computational power is. There are many more details including symmetric authentication which limits the opportunities for attackers and the main point is that the bits of a secret key can not be used on a different data once it's used. We also need to mention that authenticating QKD protocols is not the only thing we should care about. Authenticating VPN traffic is also as important as QKD protocols and we must apply the techniques to control the traffic of data. After drawing the circuit shown in figure and applying CNOT and Hadamard gate we got two results. The figure 5 shows the result of running our model on a simulator and the figure 4 shows the result on a real quantum device.
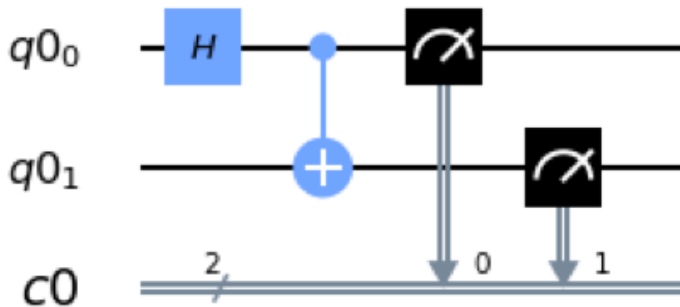
Fig. 5. Result of running a model on a simulator.

Below is the result of Aer's Qasm simulation on a classical device and on a real quantum device on IBM Q Experience. The full source code is on my GitHub's [18] account.
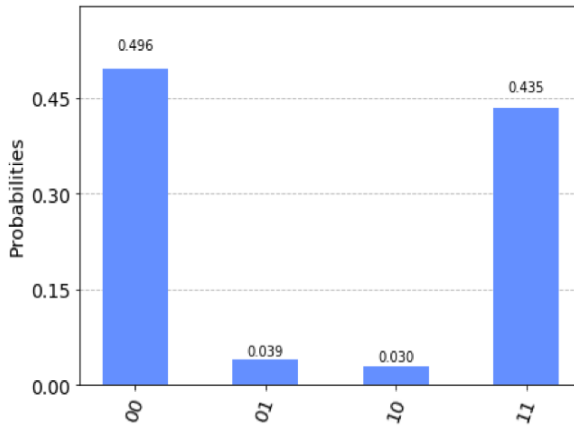

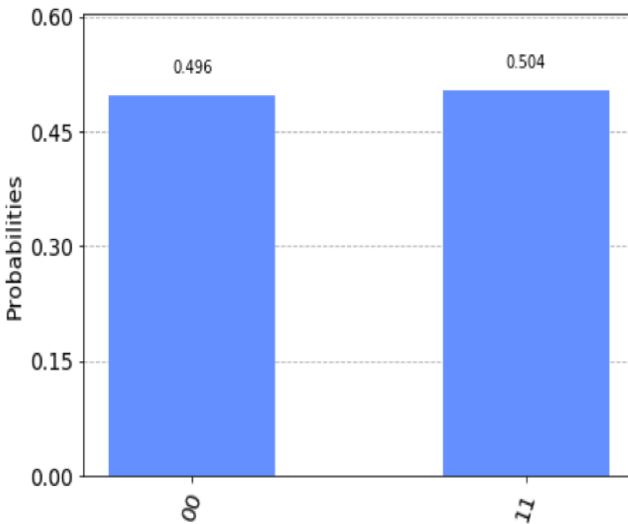Fig. 6. Result of running a model on a real quantum device.

Fig. 7. Result of running a model on a simulator.

Discussion and conclusion

DARPA [19] is one of the biggest leading companies in quantum products and devices and has started to build QKD links woven into an QKD network that connects its endpoints via routers. But in some cases when the given point to point QKD link fails, example fiber cut or too much noise it uses another link instead. This quantum network can be engineered even when it's under the denial of service attack or Dos attack. DARPA quantum network is aiming to reach a great deal of active research to solve the geographic reach problem. And if they achieved these practical devices these problems may not exist anymore and it will be a new step towards a quantum revolution. One of the proposed solutions could be chaining the quantum cryptography links in different stations or it's also possible to transfer through orbiting satellites which here satellite act as bridge or intermediary station. Researchers are still working on this area to send quantum keys to satellites and vice versa to another station securely which is under supervision of giant technology companies and governments like US and European countries. Its true that there's been a huge progress in quantum cryptography in the last decades But still there's a lot of questions remained not answered that's why it's not the correct time to deploy and use quantum cryptography as key distribution system for governments or business Developing new devices with capability of higher qualities and to be able to transfer to longer destinations are part of the not answered questions or challenges. However, advancement of processing powers in computer systems will remain as a threat for cryptography systems and it could be an influence in

development of quantum cryptography. There's been a huge interest in investing big amounts in quantum cryptography technologies. Because it's not because it has the potential to make a valuable contribution in security of businesses and ecommerce but it could open a new door and take us to a new world of science.

References

1 IBM Research Lab, Online IBM Quantum computing. URL: https://www.ibm.com/quantum-computing/.

2 Microsoft, Online Microsoft: Quantum computers. URL: https://www.microsoft.com/en-us/quantum.

3 Ali baba Researchers, Online Ali baba: Quantum computing. URL: https://damo.alibaba.com/labs/quantum.

4 Peev, M. and et.al. The SECOQC quantum key distribution network. URL: https://iopscience.iop.org/article/10.1088/1367-2630/11/7/075001/meta.

5 Gordon L. S. Artical quantum mechanics, Quantum mechanics. URL: https://www.britannica.com/science/quantummechanics-physics.

6 Khan academy, Cryptography. URL: https://www.khanacademy.org/computing/computerscience/cryptography.

7 Exabeam, Information security. URL: https://www.exabeam.com/information-security/rsa-algorithm/.

8 W-pedia, Data encryption standard. URL: https://en.wikipedia.org/wiki/Data-Encryption-Standard.

9 Science direct, Computer science cryptographic science. URL: https://www.sciencedirect.com/topics/computer-science/cryptographicsystem.

10 Wired, Quantum-cryptography and the future of security. URL: https://www.wired.co.uk /article/quantum-cryptography-and-the-futureof-security.

11 Conversation, Heisenberg's Uncertainty-principle, URL: http://theconversation.com/explainerheisenbergs-uncertainty-principle-7512.

12 Wiki, Photon polarization, URL: https://en.wikipedia.org/wiki/Photon-polarization.

13 Gate, R. The Quantagrid project RO-Quantum-security in grid-computing applications. URL: https://www.researchgate.net/publication/234853582-The-

Quantgridproject-RO-Quantum-security-in-grid-computing-applications.

14 Quantum, Quantum Key Distribution, URL: https://qt.eu/understand/underlying-principles/quantum-key-distributionqkd.

15 Kuppam, S. Modelling and Analysis of Quantum Key Distribution Protocols, BB84 and B92, in Communicating Quantum Processes (CQP) language and Analysing in PRISM. URL: https://arxiv.org/pdf/1612.03706.pdf.

16 Intechopen, Advanced technologies of quantum key distribution. URL: https://www.intechopen.com/books/advanced-technologies-of-quantumkey-distribution/security-of-quantum-key-distribution-protocols.

17 Sciencedirect, Hash functions. URL: https://www.sciencedirect.com/science/article/pii/0022000081900337.

18 Darpa, Quantum key distribution in industrie, URL: https://www.darpa.mil.

19 Shirzad, H. Quantum Encryption. URL: https://github.com/habibshirzad/ Quantum-Encryption.

O. Baimuratov[1], Zh. Mamatnabiyev[2], Sh. Dadakhanov[3], B. Berlikozha[4], B. Rustauletov[5]

[1,2,3,4,5]Suleyman Demirel University, Kaskelen, Kazakhstan

RFID TECHNOLOGY AS A PART OF MONITORING SYSTEMS

Abstract. The Internet of Things (IoT) technologies are getting more popular and being implemented as a solution for many relevant problems in information technology purposing low-costed, secure, and controlled remotely systems. Radio Frequency Identification (RFID) system is used as a type of IoT technology, which has three basic parts: tags, reader and system that manages tag identification (ID) number and its real time location. RFID systems are used in financial institutions, healthcare industry, mobile phones, cars, supply chain management, smart retails, smart house, object localization, security systems and various types of applications for positioning, managing people, assets, and inventory. This paper discusses performances of RFID technologies that use passive tags. Role of RFID technologies in monitoring systems and system architecture are reviewed and compared. Significance of RFID technologies and challenges are also considered for future works.

Keywords: RFID, internet of things, passive tag, monitoring system.

<center>***</center>

Аңдатпа. Заттардың Интернет технологиялары (IoT) неғұрлым танымал болып, аз шығынды, қауіпсіз және басқарылатын қашықтан жүйелермен байланысты ақпараттық технологиялардың көптеген өзекті мәселелерін шешу ретінде енгізіледі. Радиожиілікті Сәйкестендіру Жүйесі (RFID) үш негізгі бөліктен тұратын IoT технологиясының түрі ретінде пайдаланылады: тегтер, оқу құралы және тегтерді сәйкестендіру нөмірін (ID) және оның нақты уақыттағы орнын басқаратын жүйе. RFID жүйесі қаржы мекемелерінде, денсаулық сақтау индустриясында, ұялы телефондарда, автомобильдерде, жеткізу тізбектерін басқаруда, «ақылды» бөлшек сауда дүкендерінде, «ақылды үй», объектілерді оқшаулауда, қауіпсіздік жүйелерімен және жайғастыру, адамдарды, активтер мен қорларды басқару үшін қосымшалардың әртүрлі үлгілерімен пайдаланылады. Бұл мақалада пассивті белгілерді пайдаланатын RFID технологиясының сипаттамалары талқыланады. RFID технологиясының

мониторинг жүйелеріндегі және жүйелік архитектурадағы рөлі қарастырылады және салыстырылады. RFID технологиясының мәні мен мәселелері болашақ жұмыстар үшін де қарастырылады.

Түйін сөздер: RFID, интернет заттар, пассивті таңба, мониторинг жүйесі.

<center>***</center>

Аннотация. Технологии Интернета вещей (IoT) становятся все более популярными и внедряются в качестве решения многих актуальных проблем информационных технологий, связанных с низкозатратными, безопасными и управляемыми удаленными системами. Система радиочастотной идентификации (RFID) используется в качестве типа технологии IoT, которая состоит из трех основных частей: тегов, считывателя и системы, которая управляет номером идентификации тегов (ID) и его местоположением в реальном времени. Системы RFID используются в финансовых учреждениях, индустрии здравоохранения, мобильных телефонах, автомобилях, управлении цепочками поставок, «умными» розничными магазинами, «умным домом», локализацией объектов, системами безопасности и различными типами приложений для позиционирования, управления людьми, активами и запасами. В этой статье обсуждаются характеристики технологий RFID, использующих пассивные метки. Роль технологий RFID в системах мониторинга и системной архитектуре рассматривается и сравнивается. Значение технологий RFID и проблемы также рассматриваются для будущих работ.

Ключевые слова: RFID, интернет вещей, пассивная метка, система мониторинга.

Introduction

The Internet of Things (IoT) is being known as the main component of the new technological revolution called Industry 4.0 that focuses on automation, real-time data, interconnectivity and machine learning. Number of Internet enable devices that are increasing and they can interact each other through the network to be informed and control the sequence of actions of users. Embedded sensors invisibly gather very big amount of data from the environment around us for storing, processing and analyzing, which are used while making decisions for both real-time and future actions. The IoT technologies use this data for controlling their systems according to the decisions made. There are several ways of collecting the data by their types and purpose of use such as sensor network technology and Radio Frequency Identification (RFID).

RFID technologies are one of the main components in the IoT systems that works with a tag, reader, and system. Between reader and tag are not needed direct connection because of radio channels. Installed RFID systems simplify and accelerate the working procedure. It gives very good choice on monitoring people using tags on ID cards in real time location and attendance monitoring. There are two types of RFID tags: active and passive. Passive RFID tags are powered by the reader's power and no additional battery is needed in it. The applications that use passive RFID are found in access control applications and transportation. The active tags are powered by batteries and they can be identified in a long distance used in port containers for monitoring cargo [1].

In current RFID systems, data about cardholders is registered and stored in the memory of the system's reader for the processing and computing. The data is available only when controlled manually. The importance of using RFID technology in the monitoring systems is that the data is stored in the server and can be controlled remotely.

This work introduces architecture of RFID technologies and its use in monitoring systems proposed by previous authors. Actuality of this technology and its performances are discussed.

Radio Frequency Identification

Radio Frequency Identification (RFID) is an automatic technology and identifies tagged objects from environment through radio waves. RFID system is consisted of readers and tags [2]. The tag is a microchip that is attached to an object to identify the reader. The reader communicated with tag through radio waves. The main benefit of using RFID technology is the identification process is done automatically. RFID systems are used for real-time monitoring purpose. The components of RFID system are as follows: tags, reader, and application system. When object with a tag is tagged to the reader, the reader identifies ID number of the tag, which is unique in every tag. ID number is sent to the server, or as in most standard RFID systems, it is stored in the controller for checking whether it is correct ID or not [Fig. 1].
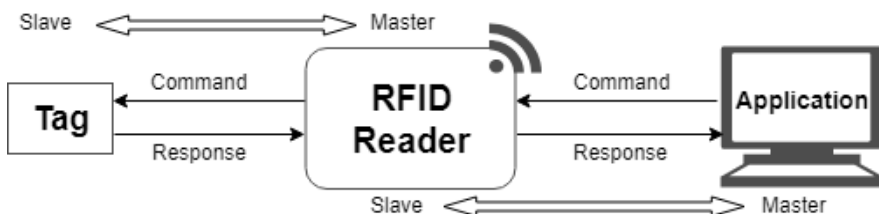

Fig. 1. Architecture and data flow of a RFID system

Tag is a transponder (transmitter/responder), whereas reader is transceiver (transmitter/receiver). There are two types of tags: active and passive. Active tags are powered by batteries, and can communicate with other active tags. Passive tags have no built-in power source, and they take power from electromagnetic energy transmitted from the reader during identification [3]. Tags are made up of coiled antenna and a microchip. Xiaolin et al. [2] classified active tags into five classes according to its functionality. Active tags can be detected from long distance: up to 30 meters. Maximum distance for passive tag is 6 meters. The advantage of using active tag is its long distance and highest data. However, it costs more expensive than passive tag (around 15-20$ per tag for active, 0.1-0.2$ per tag for passive). The benefit of using passive tag is tag life does not depend on battery, and it is more resistant to physical damage. Disadvantage of passive tag is the read range is limited and communication depends on the antenna size and shape. Norsaidah at el. [4] tested two types of UHF RFID passive tag: AZ-9640 and UPM DogBone for different distances. UPM DogBone is better in terms of detection, and outperformed AZ-9640 in terms of data transfer. AZ-9640 is more compact and discreet. Both types were experimented in the monitoring system. The tags mostly attached to the ID cards, trinkets, wearable devices, etc. In Offline Intelligent Payment System Mifare Classic 1K card was used, which is divided into 16 sectors protecting each sector by two different keys, called key A and key B [5].

Fig. 2. RFID Passive tag types

RFID reader is responsible for communication with tags within its operation range and send sending the tags' data to server or presenting in application. Attached antenna emits signals to the tag and then receive from it [6]. Reader can be many different sized and has many types. For example, Mifare RC522 reader in Attendance and Information System [11], RS532 RFID reader in Security and Monitoring System [7], PN532 NFC/RFID Controller in Smart Home project [3], ITEAD PN532 NFC in Smart Restaurant system [6], and MFRC522 in Offline Intelligent Payment System. Reader can be affixed in different positions, on the table, in door, in tourniquet, etc.
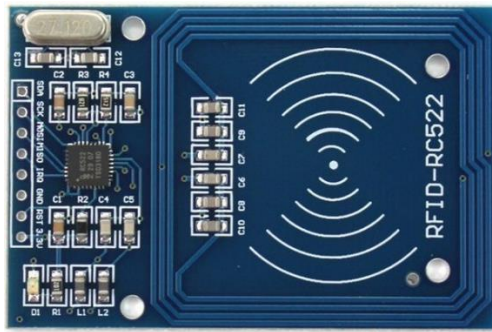
Fig. 3. RC522 RFID Reader

Data received from tag by reader is presented in an application. The data is used directly when it is tagged in many systems. Although the data is stored in server (fog, cloud) for monitoring remotely and in analytics. RFID applications are implemented in healthcare, monitoring systems, security, etc.

Comparative review of RFID based monitoring systems

Application of IoT technologies in the both closed and open areas make huge changes that increase the working process of the system and decrease human power on making actions. The most of the monitoring systems are developed using IoT hardware platform with RFID reader, which makes the hardware part of the system and send data to the server for controlling it in application part. In Table 1, RFID based monitoring systems are compared and discussed by their RFID reader type, IoT hardware platform, and main findings.

Table 1. Comparative review of previous authors' works

System	RFID type	IoT hardware platform	Main findings

Smart Restaurant System [6]	ITEAD PN532 NFC module	Raspberry Pi 3 model B	NFC module is placed on the table, and tags are under plates. The systems offers faster ordering scenery than manual ordering.
Robotic Control System [8]	RFID reader	Raspberry Pi, Arduino Uno	RFID reader services for capturing data. The data is sent to the robotic arm via web app by using embedded computer.
Offline Intelligent Payment System [5]	MFRC522 RFID reader	Raspberry Pi 3 model B	The authors tested the system according the time, distance (between tag and reader), and special cases of algorithm. The results show that time is less for declined operation than successful operation.
RFID Ecosystem [1]	RFID reader	n/a	The system includes 44 RFID readers, and each of them equipped with up to four antennas. The readers positioned at the entrances, on the stairwells, and throughout the corridors.
Smart Home project [3]	PN532 NFC/RFID controller	Raspberry Pi 3	The authors used RFID technology for monitoring real-time attendance at home by web user interface app.
Security and Monitoring System [7]	RFID reader	Raspberry Pi module B+	Data is stored in database located in raspbian SD card, and computing is done in Operating system of the microprocessor.

Wireless Sensor Node (WSN) with UHF RFID for monitoring system [4]	UHF RFID	Raspberry Pi 3	The author compared two types of tags: UPM DogBone and AZ-9640.
Paid Parking System [9]	RFID reader	ESP8266 microcontroller, Raspberry Pi	RFID reader is connected to the ESP8266 microcontroller, which has built-in Wi-Fi chip that is responsible to establish a connection with Raspberry Pi.
Real Time Locating System [10]	RFID reader	Raspberry Pi	The main purpose of the project is to monitor student participation in lectures, teaching and laboratory sections by reading tags from cards.
Attendance and Information System [11]	Mifare RC522	Arduino	Read data from tags placed in credit sized cards.
Smart Classroom Roll Caller System [12]	RFID reader	n/a	The problem of the system is that teacher must control students while taking back ID cards from special places for the ID cards. Another problem is what if student forgets (or loses) his/her ID card.

All of the systems use passive tags planting them into the objects like credit sized cards and tables. RFID reader has a connection to the microcontroller or microprocessor that allows sending the captured data to the server or displaying in the monitor. However, the passive tags are needed to contact to the reader directly by human help. Reviewing the previous authors' works, several questions can be asked: Is it possible to monitor objects that use passive tags without human help? Memory capacity of passive tag is maximum 2KB. Is it

possible to increase memory capacity for storing more information? These are the main challenges for future work.

Conclusion

RFID technology is an important and foundational component of the Internet of Things. It is used for different purposes and one of them is using in monitoring systems. Many monitoring systems use passive RFID tags that are low-costed and does not require power. RFID system is a good solution for real-time systems and getting location of objects in the environment. RFID system is analyzed and monitoring systems are reviewed. Two challenges for future work are discussed.

References

1   Welbourne, E. et al. Building the internet of things using RFID. *IEEE INternet Computing* (2009), pp. 48–55.
2   Jia, X., Feng, Q., Fan, T., Lei, Q. RFID technology and its applications in internet of things (IoT). *2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 – Proceedings,* (2012): pp. 1282-1285.
3   Mihalov, J., Hulic, M. NFC/RFID technology using Raspberry Pi as platform used in smart home project. *IEEE 14th International Scientific Conference on Informatics,* (2017): pp. 259-264.
4   Nadzir, N.M., Rahim M.K.A., Zubir, F. Wireless sensor node with UHF RFID for monitoring system," *2017 International Symposium on Antennas and Propagation (ISAP), Phuket,* (2017): pp. 1-2.
5   Noer, A., Hasanuddin, Z.B., Djamaluddin, D. Implementation of RFID based raspberry pi for user authentication and offline intelligent payment system. 15th *International Conference on Quality in Research (QiR); International Symposium on Electrical and Computer Engineering,* (2017): pp. 251-255.
6   Eric, K.B., Ya, W.H. IoT based smart restaurant system using RFID, *4th International Conference on Smart and Sustainable City (ICSSC 2017)*, Shanghai, 2017, pp. 1-6.
7   Sowmiya, M., Sabeenian, R.S. Security and monitoring system by using RFID tags and multiple sensors. *International Conference on Electrical, Instrumental and Communication Engineering (ICEICE2017),* (2017): pp. 1-5.
8   Barenji, A.V., Degirmenci, C. Robot control system based on web application and RFID technology. *MATEC Web of Conference,* 28, (2015): pp. 1-3.

9   Bazzi, A., Ghandour, H., Chebbani, A., Ghareeb, M., Abdul-Nabi, S. RFID based paid parking system. *International Conference on Current Trends in Computer, Electrical, Electronics and Communication (ICCTCEEC-2017),* (2017): pp. 1238-1241.

10   Saimounika, T., Kishore, K. Real time locating system using RFID for Internet of things, *International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017),* (2017): pp. 3507-3508.

11   Rjeib, H.D., Ali, N.S., Al-Farawn, A., Al-Sadawi, B. Attendance and information system using RFID and web-based application for academic sector. *International Journal of Advanced Science and Applications,* 9 (1), (2018): pp. 266-273.

12   Chang, Ch.H. Smart classroom roll caller system with IoT architecture. *2011 Second International Conference on Innovations in Bioinspired Computing and Applications,* (2011): pp. 256–360.

IRSTI 81.93.29

O. Baimuratov[1], Sh. Dadakhanov[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

ANALYZE AND DEVELOPMENT SYSTEM WITH MULTIPLE BIOMETRIC IDENTIFICATION

Abstract. Cause of a rapid increase in technological development, increasing identity theft, consumer fraud, the threat to personal data is also increasing every day. Methods developed earlier to ensure personal the information from the thefts was not effective and safe. Biometrics were introduced when it was needed technology for more efficient security of personal information. Old-fashioned traditional approaches like Personal identification number (PIN), passwords, keys, login ID can be forgotten, stolen or lost. In biometric authentication system, user may not remember any passwords or carry any keys. As people they recognize each other by the physical appearance and behavioral characteristics that biometric systems use physical characteristics, such as fingerprints, facial recognition, voice recognition, in order to distinguish between the actual user and scammer. In order to increase safety in 2005, biometric identification methods were developed government and business sectors, but today it has reached almost all private sectors as Banking, Finance, home security and protection, healthcare, business security and security etc. Since biometric samples and templates of a biometric system having one biometric character to detect and the user can be replaced and duplicated, the new idea of merging multiple biometric identification technologies has so-called multimodal biometric recognition systems have been introduced that use two or more biometric data characteristics of the individual that can be identified as a real user or not.

Keywords: Fingerprint, face recognition, voice recognition, biometric identification, security, accuracy.

***

Аннотация. Причина быстрого роста технологий, увеличения кражи личных данных, мошенничества потребителей, угроза персональных данных, также увеличивается с каждым днем. Методы, разработанные ранее для обеспечения личной информации от краж не были эффективными и безопасными. Биометрия была введена, когда понадобилась технология для более эффективной защиты личной информации. Старомодные традиционные подходы, такие как

персональный идентификационный номер (ПИН), пароли, ключи, логин, могут быть забыты, украдены или утеряны. В системе биометрической аутентификации пользователь не может запоминать пароли или носить какие-либо ключи. Как люди они узнают друг друга по внешнему виду и поведенческим характеристикам, которые биометрические системы используют физические характеристики, такие как отпечатки пальцев, распознавание лиц, распознавание голоса, для того, чтобы отличить реального пользователя от мошенника. В целях повышения безопасности в 2005 году были разработаны методы биометрической идентификации в правительственном и бизнес-секторах, но сегодня он охватил практически все частные сектора, такие как банковское дело, финансы, домашняя безопасность и охрана, здравоохранение, безопасность и защита бизнеса и т.д. После биометрических образцов и шаблонов биометрической системы, имеющей один биометрический символ для обнаружения, и пользователь может быть заменен и дублирован, была предложена новая идея объединения технологий множественной биометрической идентификации с так называемыми мультимодальными системами биометрического распознавания, которые используют две или более характеристики биометрических данных отдельного человека это может быть идентифицировано как реальный пользователь или нет.

Ключевые слова: отпечатки пальцев, распознавание лиц, распознавание голоса, биометрическая идентификация, безопасность, точность.

***

Аңдатпа. Технологиялардың жылдам өсуі, жеке мәліметтерді ұрлаудың, тұтынушылардың алаяқтығының артуы, дербес деректердің қауіп-қатері күн сайын артып келеді. Ұрлықтан жеке ақпаратты қамтамасыз ету үшін бұрын әзірленген әдістер тиімді және қауіпсіз болған жоқ. Биометрия жеке ақпаратты тиімді қорғау үшін технология қажет болған кезде енгізілді. Жеке сәйкестендіру нөмірі (ЖСН), парольдер, кілттер, логин сияқты ескі үлгідегі дәстүрлі тәсілдер ұмытылуы, ұрлануы немесе жоғалуы мүмкін. Биометриялық аутентификация жүйесінде пайдаланушы парольдерді есте сақтау немесе кез келген кілттерді кию мүмкін емес. Адамдар бір-бірін биометриялық жүйелер саусақ іздері, тұлғаларды тану, дауысты тану сияқты физикалық сипаттамаларды қолданатын сыртқы түрі мен мінез-құлық сипаттамалары бойынша қалай біледі. 2005 жылы қауіпсіздікті арттыру мақсатында Үкімет және бизнес-секторларда биометриялық сәйкестендіру әдістері әзірленді, бірақ бүгінгі күні ол Банк ісі, Қаржы, үй қауіпсіздігі және қорғау, денсаулық сақтау,

қауіпсіздік және бизнесті қорғау және т.б. сияқты барлық жеке секторларды қамтыды. Биометриялық үлгілер мен биометриялық жүйенің үлгілерінен кейін, анықтау үшін бір биометриялық символы бар және пайдаланушы ауыстырылуы және қайталануы мүмкін, жеке адамның биометриялық деректерінің екі немесе одан да көп сипаттамасын пайдаланатын биометриялық айырудың мультимодалдық жүйелері деп аталатын көптеген биометриялық идентификациялау технологияларын біріктірудің жаңа идеясы ұсынылды, бұл нақты пайдаланушы ретінде сәйкестендірілуі мүмкін немесе жоқ.

Түйін сөздер: саусақ іздері, бет тану, дауысты тану, биометриялық сәйкестендіру, қауіпсіздік, дәлдік.

Introduction

In today's, security is the main problem and everybody will be looking for reliable ways to ensure safety. Old ways of securing our homes and things used key and lock systems, which is quite inefficient keys can be duplicated. Later, the next level of protection was provided by modern technologies with PIN and password. Modern systems are quite effective, but they can also be hacked and gain access. To achieve with high accuracy and reliability, a biometric identification technology has been introduced that uses physical or behavioral characteristics to verify the individual. The main reason for choosing biometric identification. The technology above the traditional identification method is that traditional identification techniques are vulnerable security, unreliable and uncertain. Most developed biometric systems use one biometric technology for biomass identification and verification. These unimodal systems are unable to meet some of the challenges such as enrollment large population, high performance etc. Later advanced biometric identification technology with better Performance and a high degree of accuracy, called a multimodal biometric recognition system, are introduced. Multimodal systems are capable of using two or more physical or behavioral characteristics of a person write, verify and provide a decision. Multimodal biometric systems also combine two or more identification technologies, such as systems, fingerprint systems and face recognition, with more sensors and provides decisions by combining results from each subsystem. When using multimodal biometric systems, if one sensor or the system fails to carry out identification, other systems can be used to make decisions. Multimodal systems can be used in various fields, for example in homes for the biometric door locks to avoid theft, hospitals to record details of patient in software companies and educational institutions, to ensure participation in the banks for safe and secure payment processing, biometric

alarm systems in case of data security in different sectors. Multimodal systems are more convenient and overcome all limitations of unimodal systems with increased security, high accuracy and liveliness.

General statement of the multimodal authentication problem

The task of multimodal authentication consists of several steps [1]:

1. Get results from individual systems.
2. To normalize these results.
3. Perform the merger of normalized components.

Related works

In recent years, a lot of work has been done on different types of biometric identification techniques and their work, advantages and functioning of multimodal biometrics com- pared to unimodal and traditional approaches [2]. Biometrics refers to the automatic authentication of a person based on his physiological and behavioral property. The use of biometrics as a reliable method of verification occurs in almost all EU countries government and private sector. Some limitations of unimodal biometric systems may be reduced by the use of multimodal biometric systems that integrate information at different levels to improve performance [3]. In this the paper proposed a new multimodal biometric recognition system with a fusion of fingerprints and irises recognition to achieve higher accuracy. The main goal of this work is to show that the merger of unrelated, independent identification techniques achieve better accuracy than any unimodal biometric systems. Output scores from two different systems merge into a single score at the score level using three standardizations methods and four Fusion approaches. They also used standardization steps to transform unrelated, different scores to the common scale of the two techniques. In this article, they told about the types of mergers level in biometric systems. Sensor level, function level, score level are types of Fusion levels. First step on the score level is the normalization of the score, when the scores are transformed into a common format. Step two the Fusion level has two categories, such as classification and combination. Classification approach classifies decisions to a cheater or real. Combined approach combines score multiple decisions into one comparative score. The accuracy achieved by this work is more than 60 percentage [4]. By this article, I understand that a merger at the rank level can be a fairly new merger access. Fusion is carried out at the level of rank, when the output of each biometric system was a subset of possible matches sorted by declining self-esteem. The intention of the merger at rank level was to combine the output individual biometric subsystems to achieve greater accuracy. They used facial recognition, ear signature recognition and recognition systems and processed ones that use Eigen and Fisher face projection projection for registration and identification of the face,

projection of own ears for registration and identification of ears, and Self-Signature projection for registration and signature identification. So use the assignment function based on in the ranks of the face, ear and signature there was a merger at the level of rank, and the final exit from them was obtained. From their by experiment, they came to the conclusion that the fishing face works more efficiently than the technique of its own face and of the three biometric face recognition systems, it worked or worked better than its own ear and your own signature. [5] In this article, they considered the extraction and evaluation of fingerprints, as well as the extraction of the veins of the fingers and conversion to the knowledge of a person. They also combined two biometric recognition systems using Enhanced partial discrete Fourier transformation (EP-DFT), since the DfT Matrix has its own characteristics, such as orthogonality. Like The DfT Matrix shortens the time for its multiplication by The Matrix, so that it becomes a partial discrete Fourier transformation compact and computationally efficient. They considered three different merger options where they have considered a set of fingerprint functions based on markants and a set of fingerprint functions based on an image using an element level Fusion Strategy. Their analysis concluded that EP-DFT significantly increases system security compared to EP-DFT original P-DFT. They also concluded that it is necessary to design a good, effective irreversible transformation functions for cancellable multi- biometric systems.

A. Eigenfaces method

The basis of the eigenfaces method is the Principal Compo- nent Analysis (PCA). Eigenfaces and PCA have been used by Sirovich and Kirby to represent the face images efficiently [6]. They have started with a group of original face images, and calculated the best vector system for image compression. Then Turk and Pentland applied the Eigenfaces to face recognition problem. The Principal Component Analysis is a method of projection to a subspace and is broadly used in pattern recog- nition. An objective of PCA is the replacement of correlated vectors of large dimensions with the uncorrelated vectors of smaller dimensions. Another objective is to calculate a basis for the data set. Main advantages of the PCA are its low sensitivity to noise, the reduction of the requirements of the memory and the capacity, and the increase in the efficiency due to the operation in a space of smaller dimensions.

B. Viola-jones

This method is highly effective for search objects in images and video sequences in real time [7]. This detector has an extremely low probability of false detection of the face. The method works well and detects facial features even when observing an object at a slight angle, up to about 30°. Recognition

accuracy using this method can reach values over 90 percentages, which is a very good result. When the angle of inclination is more than 30°, the probability of detecting a face drops sharply. The indicated feature of the method does not allow in a standard implementation to detect a person's face, turned at an arbitrary angle, which greatly complicates or makes it impossible to use the algorithm in modern production systems, taking into account their growing needs.

Proposed approach

Individual or unimodal biometric systems are not enough for a person to effectively recognize a person, so I suggest multi biometric system for authentication to achieve better safety and reliability. I focus in particular on the use and degree of accuracy achieved by multibiometric recognition systems in domestic security and various area. I will explore more about biometric recognition systems in different areas.

A. Methodology

The following steps are procedures for identifying an individual.

1) *Enrollment of the biometric samples of a candidate.* Enrollment is when a candidate first uses a biometric system, sample a biometric character as a fingerprint or face recognition is captured and stored in a database for later comparison.
2) *Obtain/Acquire Live Samples from Candidate.* First, get a biometric sample from the user using sensors.
3) *Extract feature.* Process and extract prominent features from the captured sample.
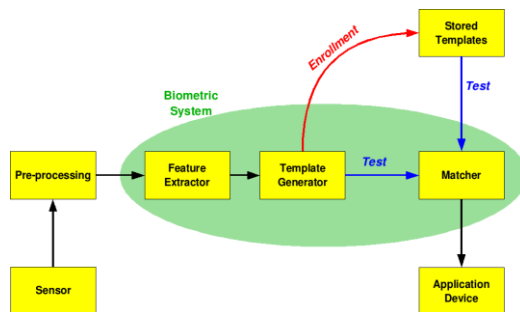4) *Comparison of samples.* Process and extract prominent features from the captured sample....

Fig. 1. Simple diagram showing the main logical block of a biometric system

5) *Display decision.* When the input samples coincide with the registered

samples, it accepts the candidate or refuses.

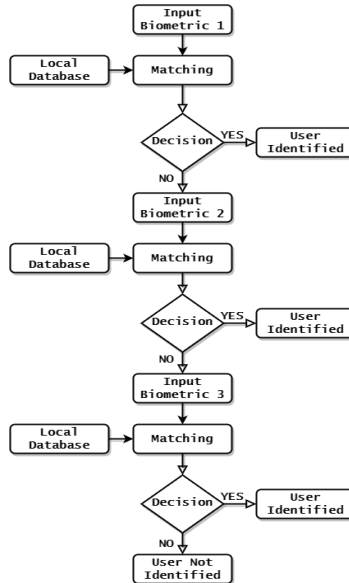The below is the flow of working procedure of multi biometric recognition systems.

Fig. 2. Flow Diagram of Multimodal Biometric Identification Systems

- Initially, the sample biometric function is captured from the user when the user wants access. Biometric features can be fingerprints, voice recognition, face recognition.
- The captured biometric data is pre-processed, which includes the removal of unwanted data, noise and a prominent feature is obtained on which a person is to be recognized
- The extracted function is compared to registered samples that are stored in the database both samples have simi- larities.
- The logged sample and the captured sample are compared at different angles using some defined algorithms and corresponding accuracy are displayed.
- Based on the degree of accuracy, the decision is made as a real user or fraudster
- If one biometric system provides 60 percent accuracy, which is not sufficient for any decision other a system with a different biometric character is used in the same procedure.

- The final results obtained from all subsystems are scaled and transformed into a normal format; and the decision appears on the screen.

Nowadays, biometrics have become a new trend in public and private workspace, where data or any other personal security is a major concern. Most nations move away from the traditional way to secure houses of technology road. Instead of the lock and key system, more biometric door locks are used, which is a combined system of two or more biometric identification techniques for verification and verification. The biometric door will have a latch with fingerprint recognition or palm print recognition in order to identify the homeowner. And were introduced videos, which offer an easy way to find out who's at the door, without get close to the door. Bells with video can be connected to smartphones via Wi-Fi and the user can get alert when someone approaches the door. Video Bell records video when the bell is pressed and it offers two-way audio communication that allows you to communicate with the visitor from anywhere through your phone. Other features include facial recognition technology, which identifies visitors by name, motion sensing technolgy that knows the difference between humans, cars and animals. Biometrics is also used in many organizations and educational institutions to record employees participation. The Multi biometric attendance system provides employees with flexibility in recording their presence; and working time at the right time interval. The main advantage of using multimodal biometric systems is fast identification and authentication. If one of the modalities fails to determine and submit a decision, the user can choose different modality or based on the convenience of the user, he can choose a modality to gain access. Biometrics are, it is also used in financial sectors such as banks, ATMs, insurance companies for Secured Transactions. Financial sectors are in terms of transactions very sensitive, because spoofing can lose a huge amount of money. To ensure secured transactions, financial sectors adopt biometric identification techniques identify account holders and, also for KYC. Scanning the veins and scanning the iris are popular today where the user does it does not require contact with the sensor and is more reliable and faster than other biometric technologies. Healthcare the Centers also use biometrics to identify the right patient, to provide a medical history and patient treatment plan.

Conclusion

In this digital era, most existing biometric systems use information from a single biological function verification and identification. The captured sample is due to the vulnerability of the biometric sensor to noisy or bad data biometric functions could become fake and it will be possible to reject the

Registered User incorrectly and falsely accept the fake user. In the case of a fingerprint recognition system, scanners may not recognize dirty or injured fingers also underdeveloped fingerprint combinations in the case of young children and faded fingerprint combinations in the case of the elderly. Where, as in the case of a facial recognition system, sensors may not be able to detect identical twins, whose appearance will be almost similar. Also, in the case of voice recognition systems, a person can imitate the voice of another person and gain access to their personal information. In all of the above cases due to an erroneous decision from the scanning devices gives unauthorized access and leads to fraudulent activity. In order to overcome these problems, a biometric system with a merger of two or more biological characteristics and sensors called multi-biometric systems are used. The main advantage of using multimodal biometric recognition there is an increased accuracy of verification. Thus, the use of multi-biometric recognition systems helps us in identifying and more precisely, in comparison with the use of a single biometric recognition system. I learned about different biometric recognition systems in order to use the necessary multimodal method biometrics for smart homes to have safe and reliable access to our homes. I can do this multimodal biometrics are more reliable and accurate compared to unimodal biometric recognition systems.

References

1   Rossand, A., Jain, A.K. Information Fusionin Biometrics. *Proc. of AVBPA : conference*. — June 2001. — P. 354—359.

2   Mir, A.H., Rubab, S., Jhat, Z.A. Biometrics Verification: A Literature Survey. *International Journal of Computing and ICT Research*, 5 (2), (2011): pp. 67-80.

3   Vishi, K., Yayilgan, S.Y.Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management. *In 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.* pp. 334-341.

4   Monwar, Md. M., Gavrilova, M.L. Multimodal Biometric System Using Rank- Level Fusion Approach. *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics*, 39 (4), (2009): pp. 867-878.

5   Yang, W., Wang, S., Hu, J., Zheng, G., Valli, C. A Fingerprint and Fingervein Based Cancelable Multi-Biometric System. *Pattern Recognition,* 78 (2018): pp. 242-251.

6   Turk, M.A., Pentland, A.P. Face Recognizing Using Eigen

faces. *Proc. IEEE*, (1991): pp. 586-591.

7   Viola, P., Michael J. Jones. Robust real-time face detection. *International journal of computer vision,* 57 (2), (2004): pp. 137-154.

Л. Атымтаева[1], О. Баймуратов[2], Д.А. Хашимова[3], Ш. Шамилулы[4]
[1,2,3]Университет имени С. Демиреля, Каскелен, Казахстан
[4]Компания Yahoo, США

ОБЗОР УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРЕДПРИЯТИИ

Аннотация. В данной статье представлены результаты анализа по выявлению групп угроз, специфичных для инфраструктуры и систем предприятии которое является одним из основных этапов в прогнозировании. Рассмотрены состояние информационной безопасности на предприятиях, проанализированы квалификации угроз безопасности и методов классификации, основанные на методах атак и на воздействии угроз. Оценены угрозы по безопасному использованию Интернета и взламыванию сайтов, краж данных, атакам фишинга и социальной инженерии; выявление угроз безопасности облачных вычислений, которые встречаются в интернет сетях предприятии. Изучены преимущества и недостатки Файрвол веб-приложений (WAF), который применяются для защиты атак, такие как *DDoS-атаки, SQL-инъекции, межсайтовый скриптинг (XSS), и др.* Представлены работы для обеспечения защиты с применением искусственного интеллекта и машинного обучения.

Ключевые слова: информационная безопасность, файрвол веб-приложений (WAF), классификация угроз информационной безопасности.

***

Abstract. This article presents the results of an analysis to identify groups of threats specific to the infrastructure and systems of an enterprise, which is one of the main stages in forecasting. The state of information security at enterprises is considered, the qualifications of security threats and classification methods based on attack methods and the impact of threats are analyzed. Threats for the safe use of the Internet and hacking sites, data theft, phishing attacks and social engineering are assessed; Identification of cloud computing security threats that are encountered in the enterprise's Internet networks. The advantages and disadvantages of Web Application Firewall (WAF), which are used to protect attacks, such as DDoS attacks, SQL injections, cross-site scripting (XSS), and others, are studied. Works for providing protection using artificial intelligence and machine learning are presented.

Keywords: information security, Web Application Firewall (WAF), classification of information security threats.

***

Аңдатпа. Бұл мақалада болжаудың негізгі кезеңдерінің бірі болып табылатын кәсіпорынның инфрақұрылымы мен жүйелеріне тән қауіптер тобын анықтау үшін жасалған талдау нәтижелері келтірілген. Кәсіпорындардағы ақпараттық қауіпсіздіктің жай-күйі қарастырылады, қауіп-қатерлердің біліктілігі, шабуыл әдістеріне және қауіп-қатерлерге негізделген классификациялау әдістері талданады. Интернетті қауіпсіз пайдалану және сайттарды бұзу, деректерді ұрлау, фишингтік шабуылдар және әлеуметтік инженерия үшін қауіптер бағаланады. Кәсіпорынның Интернет желілерінде кездесетін бұлтты есептеу қауіпсіздігіне қауіптерді анықтау. DDoS шабуылдары, SQL инъекциялар, сайттар аралық сценарийлер (XSS) және басқалары сияқты шабуылдардан қорғау үшін қолданылатын Web Application Firewall (WAF) артықшылықтары мен кемшіліктері зерттелген. Жасанды интеллект пен машиналық оқытуды қолдана отырып қорғауды қамтамасыз ететін жұмыстар ұсынылған.

Түйін сөздер: ақпараттық қауіпсіздік, Web Application Firewall (WAF), ақпараттық қауіпсіздік қауіптерін жіктеу.

Введение

В современных условиях процесс успешного развития предприятий зависит от прогнозирования потенциальных угроз информационной безопасности. Все угрозы нуждаются в контроле и ликвидации со стороны предприятий, так как они способны нанести убытки и спровоцировать новые угрозы. Однако отечественные организации вкладывают средства только в реализацию мероприятий по устранению наступившей угрозы, а не действуют изначально на ее предупреждение.

На сегодняшний момент существуют две основные проблемы, препятствующие процессу организации деятельности по предупреждению угроз безопасности:

– несовершенство моделей оценки потенциальных угроз безопасности предприятия;

– слабая проработанность вопроса превентивных мер защиты предприятия [1].

Классификация угроз безопасности

В исследованиях [2] рассмотрен структурированный подход для выявления групп угроз, специфичных для предприятия, что является важным шагом для специалистов по планированию безопасности, которые

участвуют в разработке экономически эффективных стратегий для устранения рисков информационной безопасности своих организаций. Успех программы управления рисками информационной безопасности на предприятиях основан на точной идентификации угроз для информационных систем организации.

В [2] представлены набор из пяти категорий угроз высокого уровня:
· Персонал и администрация
· Сети
· Аппаратное обеспечение
· Программное обеспечение
· Экологическая и физическая безопасность

В рамках этих категорий было выявлено 21 угроз, которые использовались для взвешивания состояния безопасности информационных систем, как показано в Таблице 1 [2]. С этого момента примерно 450 рекомендуемых мер безопасности были отнесены к этим категориям угроз.

Таблица 1. Список устаревших угроз

Персональные/Административные угрозы	Террористические/Гражданские беспорядки Деятельность для личной выгоды Злоумышленные действия отдельного сотрудника Подделка или разрушение аппаратных средств и/или связанных с ними компонентов Кража оборудования и/или связанных с ними компонентов Кража ресурсов
Сетевая угроза	Необходимая линия связи/отказ оборудования Подделка Прослушивание
Аппаратное обеспечение	Существенный аппаратный сбой
Программное обеспечение	Ошибка программиста/оператора Ошибка программного обеспечения Вторжение вредоносных программ Несанкционированный доступ или привилегии исполнения

Экологическая/Физическая угрозы безопасности	Кража или фальсификация оборудования
	Потеря стабильной электроэнергии
	Оборудование или пожарное оборудование
	Стихийное бедствие
	Экстремальные температуры/влажность

Однако работа с пятью категориями угроз вызвала обеспокоенность. Хотя был предпринят квази-аналитический подход к определению восприятия состояния безопасности системы, анализ становился все более субъективным. При рассмотрении списка угроз было замечено несколько аномалий, которые могли поставить под сомнение достоверность общих результатов.

Таким образом, должен быть разработан полный и сбалансированный список угроз, от которых могут быть защищены информационные системы. В этой статье описывается процесс в форме шага, который используется для составления списка угроз предприятия.

На основе приведенных пяти категорий угроз субъективно определено положение безопасности и дополнительные меры безопасности для снижения риска [2].

Одним из задач в организации/предприятии является детальное и полное представление об угрозах для их информационных активов и как получить необходимые средства для борьбы с ними, что возможно скрыто продолжает создавать утечку информации. Чтобы улучшить понимание угроз безопасности, в работе [3] предлагается модель классификации угроз безопасности, которая позволяет нам изучать влияние класса угроз вместо воздействия угрозы, поскольку угроза меняется с течением времени и рассматриваются различные критерии классификации рисков безопасности информационных систем и дается обзор моделей классификации большинства угроз, также определяют гибридную модель для классификации угроз безопасности информационной системы, чтобы предложить архитектуру классификации, которая поддерживает все принципы классификации угроз и помогает организациям реализовывать свои стратегии информационной безопасности.

В исследовании [3] разделили подходы классификации угроз на два основных класса:

1. Методы классификации, основанные на методах атак

- *Трехмерная ортогональная размерная модель* - модель угроз для классификации угроз безопасности, решающая проблему путем введения трехмерной модели, которая подразделяет пространство угроз на подпространства в соответствии с тремя ортогональными измерениями, обозначенными как мотивация, локализация и агент (рис.1):

Рисунок 1. Измерение угроз [3]

- *Гибридная модель для классификации угроз* - рассматривает три основных критерий:
  - Частота угроз безопасности;
  - Область действий угроз безопасности;
  - Источник угрозы безопасности;
- *Модель пирамиды классификации угроз информационной безопасности* - классифицирует преднамеренные угрозы на основе трех факторов:
  - Знания злоумышленников о системе;
  - Критичность области;
  - Потери, которые могут возникнуть в системе или в организации;
- *2. Методы классификации, основанные на воздействии угроз*

STRIDE Model (*Spoofing* identity, *Tampering* with data, *Repudiation*, *Information* disclosure, *Denial* of service and *Elevation* of privilege) - это целенаправленный подход, при котором делается попытка проникнуть в сознание злоумышленника путем оценки угроз.

ISO model - Стандарт ISO (ISO/IEC 27001) с целью формирования комплексных требований к безопасности информации определяет три основных показателя:

- оценка рисков, с которыми сталкивается организация (определение угрозы для ресурсов, их уязвимость и вероятность возникновения угроз, а также возможный ущерб);
- соблюдение законодательных, нормативных и договорных требований, которые должны выполняться самой организацией, ее партнерами по бизнесу, подрядчиками и поставщиками услуг;
- формирование комплекса принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности [4].

Большинство классификаций угроз безопасности обычно ограничиваются использованием одного или двух критериев для классификации угроз (не все угрозы включены в классификацию), и их категории не взаимоисключающие. Этого может быть достаточно для стабильной среды (небольшой организации), где угрозы безопасности относительно стабильны, но в постоянно меняющихся средах организации не могут защитить от внутренних угроз [5].

На самом деле, организации подвержены нескольким видам угроз, которые влияют на их репутацию, и важно, чтобы они идентифицировали все характеристики угроз, чтобы снизить их риски.

Классификация позволяет организации знать угрозы, которые влияют на их активы и области, на которые может повлиять каждая угроза, и следовательно, заранее защищать свои активы. Кроме того, помогает менеджерам создавать информационные системы своих организаций с меньшей степенью уязвимости [5]. Основные проблемы могут быть выявлены в работе существующих угроз. Фактически, существующие классификации не поддерживают принципы классификации [6], [7], [8]. На этом этапе обычным решением является объединение различных классификаций и создание гибридной.

Из-за приведенных выше результатов, [3] предлагают гибридную модель для классификации угроз безопасности информационной системы,

которую назвали многомерной моделью для классификации угроз с целью соблюдения всех принципов классификации угроз.

В следующей работе [9] были оценены «угрозы по безопасному использованию Интернета», опросив избирателей, задавая следующие вопросы: «Какая угроза поразила вас больше всего?», «Как вы думаете, какая угроза имеет значительное влияние на общество?» и т.д., разделив респондентов на три группы: «организации», «пользователи» и «системные администраторы/разработчики», и выявили 10 основных угроз безопасности. Соответствующие угрозы были назначены каждой группе, а затем собраны сведения, включая краткое изложение инцидента, как он произошел, степень ущерба и как он был нанесен, и какие меры были приняты. Следующим образом были представлены угрозы трех групп:

- *Угрозы для организаций:*
  o угроза отравления DNS-кешем;
  o сложные целевые атаки;
  o утечка информации, происходящая ежедневно;
- *Угрозы для пользователей:*
  o разнообразные пути заражения компьютерных вирусов и ботов;
  o угрозы, возникающие из-за уязвимости шифрования беспроводной локальной сети;
  o никогда не уменьшать спам;
  o угрозы, возникающие при использовании одного и того же идентификатора пользователя и пароля;
- *Угрозы системным администраторам/разработчикам:*
  o Угрозы атак через законный сайт;
  o Актуальные пассивные атаки;
  o Потенциальная уязвимость встраиваемых систем/устройств;

Далее рассмотрим облачные вычисления в корпоративной инфраструктуре, приведенные в [10], где обсуждены риски и проблемы безопасности в облачных вычислениях и просвещенные шаги, которые предприятие может предпринять, чтобы снизить риски безопасности и защитить свои ресурсы.

Облачные вычисления - модель обеспечения удобного сетевого *доступа по требованию* к некоторому общему фонду конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам — как вместе, так и по отдельности), которые могут быть

оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру [11].

Предприятия начинают рассматривать технологию облачных вычислений как способ сокращения затрат и повышения прибыльности, потому что во всех отраслях ИТ-директорам постоянно приходится сокращать капитальные активы, количество сотрудников и расходы на поддержку, а облачные системы дают им возможность достичь этих целей. На рисунке 2 показано доступные ресурсы для предприятий в облаке (Брендл, 2010) [10].

Рисунок 2. Ресурсы облачных вычислений (CloudTweaks, 2010) [10]

Рентабельность облачных вычислений может быть объяснена в формулах «ассоциативность затрат», показанных в формуле (1). Левая часть умножает чистый доход на пользовательский час на количество часов пользователя, давая ожидаемую прибыль от использования облачных вычислений, в то время как правая сторона выполняет те же вычисления для центра обработки данных с фиксированной емкостью, учитывая среднюю загрузку, включая непиковые рабочие нагрузки центра

обработки данных; какая сторона больше, тем больше возможностей для получения прибыли (Armbrust et al., 2009) [12].

В работе [12] (Armbrust et al., 2009, стр. 10-11) привели пример эластичности с расчетами потенциалов экономии облачных вычислений и снижения затрат:

$$\text{Пользовательские часы}_{\text{облочный сегмент}}$$
$$\times (\text{Доход} - \text{Стоимость}_{\text{облочный сегмент}}) \geq$$

$$\geq \text{Пользовательские часы}_{\text{Центр обработки данных}} \times (\text{Доход} -$$
$$\frac{\text{Стоимость}_{\text{облочный сегмент}}}{\text{Использование}}) \qquad (1)$$

Существует несколько крупных поставщиков облачных вычислений, в том числе Amazon [21], Google [22], Salesforce [23], Yahoo [24], Microsoft [25], Alibaba [26], IBM [27] и другие, которые предоставляют услуги облачных вычислений, предоставляя клиентам разнообразные услуги, такие как Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a-Service и Infastructure-as-a-Service (IaaS) в число которых входят электронная почта, хранилище, программное обеспечение и инфраструктура в качестве услуг.

Облачные вычисления сталкиваются с таким же количеством угроз безопасности, которые в настоящее время встречаются в существующих вычислительных платформах, интернет сетях предприятии. Эти угрозы, уязвимости риска бывают разных форм. Cloud Security Alliance [13] провел исследование угроз, стоящих перед облачными вычислениями, и выявил семь основных угроз:

- злоупотребления и злонамеренное использование облачных вычислений;
- небезопасные интерфейсы прикладного программирования;
- злобные инсайдеры;
- уязвимости общих технологий;
- потеря данных/утечка;
- учетная запись, обслуживание и угон трафика;
- неизвестный профиль риска;

Перенос ваших данных в облачный сервис - это все равно, что «положить все яйца в одну корзину» согласно [14]. Исследования показали, что злоумышленники могут точно определить, где находятся данные в «облаке», и использовать различные приемы для сбора

информации. Для успешной реализации облачных вычислений на предприятии требует правильного планирования и понимания возникающих рисков, угроз, уязвимостей и возможных контрмер. В [10] полагают, что предприятие должно проанализировать риски безопасности, угрозы и имеющиеся меры противодействия компании/организации, прежде чем применять эту технологию.

Структура веб-приложений и типы атак

С развитием технологий каждое предприятие имеет свой веб-сайт. А веб-сайт, в свою очередь, это система электронных документов (файлов данных и кода), принадлежащий частному лицу или организации, и может быть доступным в компьютерной сети под общим доменным именем и IP-адресом или локально на одном компьютере. Как правило, веб-интерфейс, обращенный к общедоступному Интернету, считается наиболее уязвимым и «рискованным», когда речь идет об уязвимостях, поэтому веб-сайты являются одной из основных целей для хакеров. Как только злоумышленник достигнет веб-приложения, это может привести к тому, что он достигнет компьютерной системы или базы данных, сервера или конфигураций реализации или операционной системы.

Приведем некоторые анализы по взламыванию сайтов на предприятиях.

В среднем от 30 000 до 50 000 сайтов каждый день взламывается, и на самом деле большинство из этих 30 000 сайтов являются законными малыми предприятиями, которые невольно распространяют вредоносный код для киберпреступников.

64% компаний сталкивались с веб-атаками на основе доступной в настоящее время статистики. 62% подвергались атакам фишинга и социальной инженерии, а 59% компаний сталкивались с вредоносным кодом и ботнетами [15].

По приведенным выше данных видим значимость необходимости обеспечения информационной безопасности веб-приложений предприятий, каждодневно использующие интернет ресурсы.

В связи с этим рассмотрим структуру веб-приложений и приведем типы атак для исследования дальнейшей работы.

Чтобы понять слабость веб-среды, мы также должны знать компоненты веб-приложения. Веб-приложения состоят из трех основных частей, как показано на *рисунке 3.* Язык программирования используется для разработки клиентской части и для создания запросов к базе данных. Протокол передачи гипертекста (http), который используется для связи

стороны клиента со стороной сервера. В добавок бизнес-процесс, который является отличительной частью любого веб-приложения.
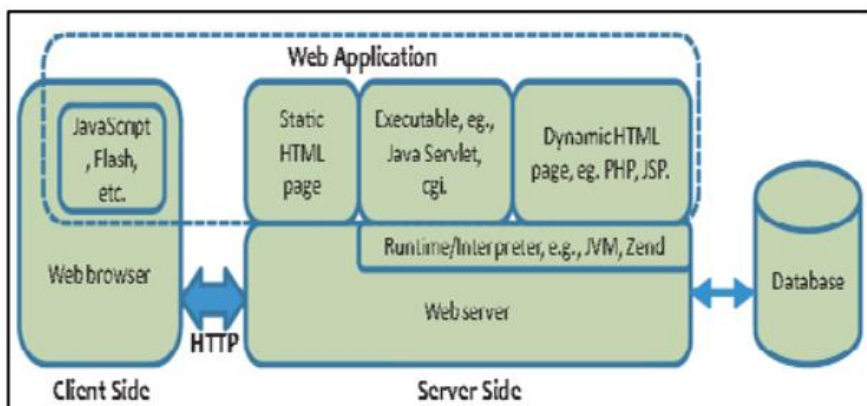

Рисунок 3. Компоненты веб-приложения [16]

Еще одна главная угроза в интернет-безопасности и веб-приложениях, которую пользователи просматривают через порт по умолчанию номер 80 с использованием протокола http и номер порта 443 с использованием протокола безопасного уровня https. Злоумышленник начинает использовать Интернет как обычный клиент или пользователь веб-сайта, затем эти порты используются для атаки на сайт и доступ к данным и файлам клиентов. Размер атаки зависит от важности данных и бизнеса компаний, которые владеют этими сайтами [16].

Далее приведем самые распространенные виды атак в веб-приложениях:

1. *DDoS-атаки:* DDoS-атаки направлены на подавление целевого веб-приложения/ веб-сайта/сервера ложным трафиком, снижая пропускную способность сети и делая ее недоступной для законных пользователей. Некоторые распространенные, но опасные типы DDoS-атак включают усиление DNS, Ping of death, Smurf-атаки, HTTP-флуд, SYN-флуд и т. д. [17].

2. *Атаки SQL-инъекций.* В этих атаках злоумышленник внедряет вредоносный код SQL в виде запросов или запросов в поля ввода пользователя в веб-приложениях, таких как формы отправки, контактные формы и т. д. Таким образом, они получают доступ к внутренней базе данных приложения, куда они проникают извлекать конфиденциальную информацию о клиентах или самой компании, получать несанкционированный административный доступ, изменять или удалять данные и т.д. или даже получать полный контроль над веб-приложением [17].

129

3. *Атаки межсайтового скриптинга (XSS).* Атаки XSS направлены на пользователей уязвимых веб-приложений/веб-сайтов, чтобы получить доступ к браузерам и управлять ими. Здесь злоумышленники используют уязвимости и пробелы в приложении для внедрения вредоносных скриптов/кодов, которые выполняются, когда ничего не подозревающий пользователь загружает приложени/веб-сайт. Атаки XSS ставят под угрозу личную и конфиденциальную информацию пользователя и часто приводят к краже личных данных, перехвату сеансов и т.д. [17].

4. *Атаки нулевого дня (Zero-day Attacks).* Атаки нулевого дня - это те, в которых организация знает о существовании уязвимостей в аппаратном/программном обеспечении только тогда, когда атака происходит. Это неожиданно и, следовательно, очень вредно для бизнеса, поскольку у них нет быстрых исправлений или исправлений для защиты своего приложения [17].

5. *Атаки бизнес-логики (Business Logic Attacks).* Бизнес-логика является критическим элементом, соединяющим и передающим информацию между пользовательским интерфейсом и базами данных и системами программного обеспечения, позволяя пользователям эффективно использовать веб-приложение/веб-сайт. Когда в бизнес-логике есть пробелы, ошибки или совпадения, это создает уязвимости, которые часто используются кибер-атакующими для получения денежных и других преимуществ. Злоумышленники не используют искаженные запросы и вредоносную нагрузку для организации атак бизнес-логики. Они используют законные ценности и правовые запросы для использования косвенных уязвимостей в приложении [17].

6. *Атаки «человек посередине» (Man-in-the-middle attacks).* Эти атаки происходят, когда злоумышленники позиционируют себя между приложением и законными пользователями для извлечения конфиденциальной информации, такой как пароли, учетные данные для входа, данные кредитной карты и т. Д., Выдавая себя за одну из двух сторон. Атака может быть организована с помощью простых средств, таких как предоставление бесплатных, вредоносных точек доступа в общественных местах, которые не защищены паролем. Когда жертвы подключаются к этим точкам доступа, они предоставляют злоумышленнику полную прозрачность обмена данными в Интернете [17].

7. Вредоносные программы (Malware). Атаки вредоносных программ организуются путем использования уязвимостей приложений или с помощью методов социальной инженерии, таких как фишинг, для внедрения вредоносных программ, таких как трояны, вымогатели, шпионское ПО, руткиты и т.д., на веб-сайт/веб-приложение/сервер. Тем самым злоумышленник получает доступ к конфиденциальной информации, конфиденциальным частям приложения, изменениям конфигурации системы [17].

8. Пороки (Defacements). При атаках с использованием фальсификации, самой простой из всех кибератак, злоумышленники изменяют контент веб-сайта и заменяют его своим собственным контентом, чтобы отразить политическую идеологию/повестку дня, шокировать пользователей спорными сообщениями или образами. До устранения порчи веб-приложение может стать недоступным для пользователей [17].

Исследуя вышеуказанные работы выявили какие есть угрозы безопасности в организациях, и рассмотрели структуры веб-приложений с распространенными видами атак.

Традиционные решения безопасности, такие как сетевые брандмауэры, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), хороши для предотвращения незаконного трафика и обеспечения безопасности на уровне сети. Но у них нет возможности обнаруживать и останавливать внедрение SQL, перехват сеансов, межсайтовый скриптинг (XSS) и другие атаки, возникающие в результате уязвимостей, присущих веб-приложениям, одним из решений является конфигурация WAF (Web application firewall).

Обоснования WAF (Web application firewall) и его преимущества

Файрвол веб-приложений предоставляют эффективное решение для обнаружения угроз путем проверки входящих HTTP-запросов еще до того, как они достигнут сервера. WAF (Web application firewall) обнаруживает и блокирует злонамеренные атаки, связанные с безопасным трафиком веб-сайта, который мог просочиться через традиционные решения безопасности. WAF также используются, чтобы помочь организациям соблюдать требования HIPAA и PCI-DSS [20].
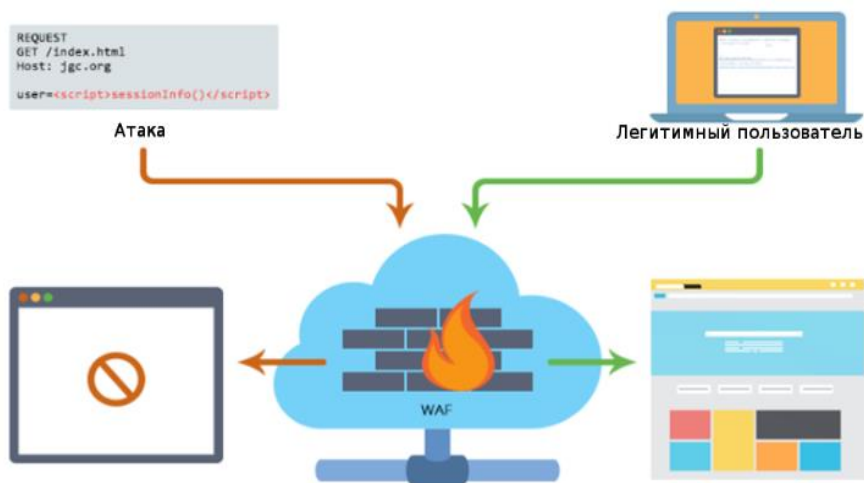
Рисунок 4. Структура защиты WAF

Работа WAF обычно основана на одной из трех моделей безопасности:

1. Черный список или модель с отрицательной защитой - при этом используются общие подписи для защиты сайта от известных атак и специальные подписи для предотвращения атак, которые могут использовать уязвимости в веб-приложении;

2. Белый список или модель позитивной безопасности - при этом используются сигнатуры, а иногда и дополнительная логика, чтобы разрешить только трафик, соответствующий определенным критериям. Примером является разрешение только HTTP-запросов GET с определенного URL-адреса и блокирование всего остального;

3. Гибридная модель безопасности - это касается как негативных, так и позитивных моделей. Некоторые из настраиваемых параметров включают блокировку запроса, блокировку сеанса, блокировку IP-адреса, блокировку пользователя или выход пользователя из системы [20].

Веб-приложения и SQL-инъекция

Связь между базой данных и веб-приложениями очень прочна, поскольку большинство веб-приложений предназначены для извлечения и хранения данных клиентов в базах данных. Поэтому SQL-инъекция становится серьезной атакой на веб-приложение для извлечения или хранения данных без авторизации или разрешения доступа. SQL-инъекция

- это метод внедрения веб-приложения с параметром ошибки через SQL-сообщения для получения несанкционированного доступа [16].

У WAF есть некоторые недостатки из-за отсутствия автоматизации, масштабируемости и охвата возникающих угроз, поскольку современные бот-сети становятся все более и более эффективными и агрессивными. Эти ботнеты теперь создаются с помощью функции искусственного интеллекта (ИИ) поверх «старых» ботнетов Интернет вещей (IoT), которые становятся все более универсальными в своей способности атаковать с различными векторами. Функциональность, которую предлагает классический WAF, стала предметом недовольства, в то время как WAF следующего поколения, которые были рождены как системы искусственного интеллекта, которые могут справиться с такой многомерной сложностью угроз, встречаются довольно редко.

В сегменте киберзащиты сети и защиты приложений не так много решений по искусственному интеллекту/машинному обучению (AI/ML). Однако все больше и больше решений AI и ML начинают проявляться в качестве основного успеха против атак распределенного отказа в обслуживании (DDoS) и, более конкретно, против мира приложений DDoS (Distributed Denial of Service), что было продемонстрировано L7 Defense с его неконтролируемым подходом к обучению. Такая технология также может играть решающую роль в решениях WAF, таких как защита от тех же многоцелевых ботнетов [18].

Заключение

Что касается защиты, традиционные методы используют некоторый словарь или базу данных известных уязвимостей.

WAF должен быть в состоянии бороться с множеством многовекторных атак, таких как внедрение SQL, удаленное выполнение команд, включение удаленных файлов, включение локальных файлов, внедрение PHP, внедрение LDAP, внедрение Memcache и межсайтовый скриптинг (XSS); все вместе. Нам нужен опыт, чтобы идентифицировать эти типы атак и классифицировать их с максимальной точностью с первого запроса. Объективно, это критически важная часть для определения по «самому первому запросу» [18].

Ложные срабатывания и ложные отрицания должны быть ограничены, что было бы близко к нулю на уровне веб-страницы.

Нам нужно найти решение, которое использует те же концепции AI из Applicative DDoS и необходимо добавить конкретные классификации в дополнение к возможности алгоритмически динамически идентифицировать все типы атак на лету. WAF должна быть предоставлена дополнительная возможность, чтобы он мог точно

определить, есть ли какая-то агрегация трафика в вашем веб-интерфейсе, идущем к вам, используя машинное обучение, которое будет нашей дальнейшей работой [18].

Для качественной организации деятельности по предупреждению угроз информационной безопасности предприятию необходимо:

– качественное прогнозирование угроз;

– разработка превентивных мер защиты предприятия.

В организации деятельности по предупреждению угроз информационной безопасности основной задачей является прогнозирование и оценка возможных угроз предприятии.

Таким образом, очень важно, чтобы предприятие приняло структурированную методологию для определения соответствующих угроз, переоценки остаточных уязвимостей и выявления новых угроз.

Список использованной литературы:

1   Сергеева И.А., Володин В.М. Прогнозирование потенциальных угроз - основа превентивных мер финансовой безопасности организации // Общественные науки. Экономика. – 2017. – № 1 (41). – С. 140-148.
2   Stacey, T.R., Helsle, R.E., Baston, J.V. Identifying Information Security Threats. – pp. 1-13.
3   Jouinia, M., Rabaia, L.B.A., Aissab, A.B. Classification of security threats in information systems. Procedia Computer Science, 32 (2014): pp. 489 – 496.
4   ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001). URL: https://rusregister.ru/standards/iso-27001/
5   Geric, S., Hutinski. Z. Information system security threats classifications. Journal of Information and Organizational Sciences, 31 (1), (2007): pp. 51-61.
6   Lindqvist, U., Jonsson, E. How to systematically classify computer security intrusions. IEEE Symposium on Security and Privacy, (1997): pp.154-163.
7   Tang, J., Wang, D., Ming, L., Li, X. A Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory; 2012.
8   Howard J.D. An Analysis Of Security Incidents On The Internet 1989 – 1995. Doctoral Dissertation, Carnegie Mellon University Pittsburgh, PA, USA; 1998

9   10 M a j o r Security Threats Attacking Techniques Become More and More Sophisticated. Information Security White Paper, Japan, June 2009 – P. 1-25.

10 Bisong, A., Rahman, S.M. An overview of the security concerns in enterprise cloud computing. International Journal of Network Security & Its Applications (IJNSA), 3 (1), (2011): pp. 30-44.

11 Облачные   вычисления.   URL: https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D0%B0% D1%87%D0%BD%D1%8B%D0%B5_%D0%B2%D1%8B%D1%87% D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F

12 Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. Above the Clouds: A Berkeley View of Cloud Computing. – pp. 10-11 URL: http://d1smfj0g31qzek.cloudfront.net/abovetheclouds.pdf

13 Cloud Security Alliance (2010). Top Threats to Cloud Computing. Cloud Security   Alliance.   URL: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

14 Perez, S. (2009). The Cloud Isn't Safe?! (Or Did Black Hat Just Scare Us?).   August   5,   2009.   ReadWriteWeb.   URL: http://www.readwriteweb.com/archives/the_cloud_isnt_safe_or_did_bl ackhat_just_scare_us.php

15 What is Web Application Firewall (WAF)? Updated: July 19, 2019 by Agnes   Talalaev.   URL: https://www.webarxsecurity.com/web-application-firewall/

16 Abusaimeh, H., Shkoukani, M. Survey of Web Application and Internet Security Threats. IJCSNS International Journal of Computer Science and Network Security, 12 (12), (2012): pp. 67-76.

17 8 Types of Cyberattacks a WAF is Designed to Stop. April 17, by Venkatesh Sundar URL: https://www.indusface.com/blog/8-types-of-cyberattacks-a-waf-designed-to-stop/

18 The WAF backed by artificial intelligence (AI). By Matt Conran, Oct 2, 2018. URL: https://www.networkworld.com/article/3310359/the-waf-backed-by-artificial-intelligence-ai.html.

19 Web Application Firewall — защита сайта от хакерских атак. Luka Safonov, 27 мая 2009 в 14:08. URL: https://habr.com/ru/post/60590/

20 What   is   a   Web   Application   Firewall?   URL: https://chesstrending.com/crm/knowledge-base/web-application-firewall-waf.

21 Что такое облочные вычисления. URL: https://aws.amazon.com/ru/what-is-cloud-computing/.

22 Google Cloud Platform Overview. URL: https://cloud.google.com/docs/overview.

23 Cloud computing – apps on tap. URL: https://www.salesforce.com/ap/cloudcomputing/.

24 Cloud Computing Today. URL: https://cloud-computing-today.com/category/yahoo/.

25 Microsoft Azure. URL: https://en.wikipedia.org/wiki/Microsoft_Azure.

26 Alibaba Cloud. URL: https://en.wikipedia.org/wiki/Alibaba_Cloud.

27 Cloud computing: A complete guide. URL: https://www.ibm.com/cloud/learn/cloud-computing.

МРНТИ 27.03.66

В.В. Вербовский[1]
[1]Университет имени С. Демиреля, Каскелен, Казахстан

О ЛОКАЛЬНОЙ МОНОТОННОСТИ ОДНОМЕСТНЫХ ФУНКЦИЙ ОПРЕДЕЛИМЫХ В КОНЕЧНО ПРОСТЕГАННЫХ УПОРЯДОЧЕННЫХ СТРУКТУРАХ

Аннотация. Как было доказано Б. Кулпешовым, любое сечение в слабо о-минимальной структуре может иметь максимум два расширения до полных типов, причем множества всех реализаций этих типов являются выпуклыми в любых элементарных расширениях. В данной статье мы обобщаем понятие слабой о-минимальности и получаем следующее понятие n-стеганых структур: линейно упорядоченная структура называется n-стеганой, если любое сечение имеет не более n расширений до полного типов. Обратите внимание, что мы здесь опускаем условие, что множество всех реализаций типа должно быть выпуклым. В этой статье мы исследуем свойство локальной монотонности для одноместных функций, определимых в конечно простеганных структурах.

Ключевые слова: математическая логика, теория моделей, о-минимальность, упорядоченные структуры, сечение, полный тип.

***

Abstract. As it was proved by B. Kulpeshov, any cut in a weakly o-minimal structures can have at most two extensions up to complete types, and the sets of realizations of these types are convex in any elementary extensions. In this paper we consider a generalization of weak o-minimality, namely notion of an n-quilted structure: a totally ordered structure is said to be n-quilted if any cut has at most n extensions up to complete types over the structure. Note that we omit here condition that the set of all realizations of a type must be convex. In this article we investigate the property of local monotonicity for unary functions definable in finitely quilted ordered structures.

Keywords: mathematical logic, model theory, o-minimality, ordered structures, a cut, a complete type.

***

Аңдатпа. Б. Күлпешов дәлелдегендей, әлсіз минималды құрылымдағы кез-келген қима толық типке дейін ең көбі екі кеңейтімге ие бола алады, ал осы типтердің барлық іске асырылу жиынтығы кез-келген

қарапайым кеңейтулерде дөңес болады. Бұл мақалада әлсіз минимализм ұғымын қорытып, *n*-қабулы құрылымдар туралы келесі ұғымды аламыз: сызықты реттелген құрылым, егер қандай да бір қимада толық типтерге кеңейтілген *n* болса, *n*-қабулы деп аталады. Мұнда типтің барлық іске асыруларының жиынтығы дөңес болуы керек деген шартты ескермейміз. Бұл мақалада біз біртектес функциялар үшін жергілікті монотондылық қасиетін ақырғы қабулар құрылымында анықтауға болатындығын қарастырамыз.

Түйін сөздер: математикалық логика, модельдер теориясы, о-минимум, реттелген құрылымдар, қима, толық тип.

Пусть $M = (M, <, \dots)$ будет линейно упорядоченной структурой. *Открытый интервал I* в структуре M есть параметрически определимое подмножество структуры M вида $I = \{c \in M : M \vDash a < c < b\}$ для некоторых $a, b \in M \cup \{-\infty, \infty\}$, где $a < b$. Аналогично, мы можем определить *замкнутые, полуоткрытые-полузамкнутые* и тому подобные интервалы в M, так что, например, произвольная точка структуры M является сама (тривиальным) замкнутым интервалом. Подмножество A линейно упорядоченной структуры M называется *выпуклым*, если для любых $a, b \in A$ и $c \in M$ всякий раз, когда $a < c < b$ мы имеем $c \in A$.

Выпуклым компонентом множества A назовем максимальное выпуклое подмножество множества A. Выпуклым замыкание множества A является наименьшее выпуклое множество, содержащее множество A. Будем обозначать его A^c. Запись $A < B$ означает, что каждый элемент из A меньше всякого элемента из B.

Одно из основных понятий в теории моделей — понятие о-минимальной структуры — было введено А. Пиллаем и Ч. Стайнхорном [1]. Слабая о-минимальность — его обобщение, введенное в [2]. *Слабо о-минимальной структурой* называется линейно упорядоченная структура $M = \langle M, =, <, \dots \rangle$ такая, что любое определимое (с параметрами) подмножество структуры M является объединением конечного числа выпуклых множеств в M. Вспомним, что структура M называется *о-минимальной*, если каждое определимое (с параметрами) подмножество структуры M является объединением конечного числа интервалов и точек в M.

Для двух подмножеств A и B множества M будем писать $A < B$, если $a < b$ при любых $a \in A$ и $b \in B$. будем говорить, что элемент a лежит между двумя множествами B и C, если либо $B < a < C$, либо $C < a < B$.

Пара подмножеств (C, D) линейно упорядоченной структуры M называется *сечением*, если $C \cup D = M$ и $C < D$. Скажем, что сечение (C, D) определимо, если множество C формульно. По сечению (C, D) можно построить частичный тип $s \in S_\varphi(M)$, где $\varphi(x; y, z) \stackrel{\text{def}}{=} y < x < z$, при помощи закона: $c < x < d \in s$ тогда и только тогда, когда $c \in C$ и $d \in D$. Легко понять, что и любой <-тип определяет сечение. Поэтому будем называть такие <-типы сечениями.

Заметим, что любое сечение в модели M слабо о-минимальной теории имеет самое больше два расширения до полных типов над M, причем реализации этих типов выпуклы [3]. Если $p \in S_1(M)$, то будет писать (C_p, D_p) для единственного сечения, которое совместно p, то есть для <-части типа p.

Определение 1. Линейно упорядоченная структура $(M, <, \dots)$ называется n-простеганной, если любое сечение в M имеет самое большее n пополнений до полных типов над M. Здесь, n — положительное целое число. Линейно упорядоченная структура $(M, <, \dots)$ называется конечно-простеганной, если любое сечение в M имеет конечное число пополнений до полных типов над M.

Элементарная теория называется n-простеганной (конечно-простеганной), если любая ее модель такова.

Из работы [3] следует, что слабо о-минимальные теории являются 2-простеганными. Некоторые свойства конечно-простеганных теорий были рассмотрены в работе [4].

Вспомним такое понятие из топологии, как росток множеств, переложенное для топологии, индуцированной линейным порядком. Пусть в упорядоченной структуре дано сечение $s = \langle C, D \rangle$. Для заданного сечения определим росток множеств следующим образом. Два множеств A и B лежат в одном и том же ростке, если существуют такие элементы $c \in C$ и $d \in D$, что $(c, d) \cap A = (c, d) \cap B$. Если $D = \emptyset$, то A и B лежат в одном и том же ростке, если существует такой элемент $c \in C$, что $(c, \infty) \cap A = (c, \infty) \cap B$. Если $C = \emptyset$, то A и B лежат в одном и том же ростке, если существует такой элемент $d \in D$, что $(-\infty, d) \cap A = (-\infty, d) \cap B$. Очевидно, что данное отношение является отношением эквивалентности.

Вообще говоря, понятие ростка в топологии вводят для функций. Но так как можно рассмотреть вместо подмножеств их характеристические функции, то становится понятным, что понятие ростка можно и перенести на подмножества.

Определение 2. Будем называть функцию f *локально монотонной*, если для любого $a \in dom\, f$ существует бесконечное подмножество,

содержащее элемент a, такое что сужение функции на данное подмножество является монотонным.

Определение 3. Предположим, что элементарная теория T линейно упорядоченной структуры $(M, <, \dots)$ является конечно-простеганной, а сама модель $(M, <, \dots)$ достаточно насыщенной. Теорию T назовем *почти гладкой*, если для любого интервала существует такой подынтервал I и такое конечное множество одноместных попарно несовместных формул $P_1, \dots, P_n$, что любой 1-тип над M определяется сечением и включением ровно одной из формул $P_1, \dots, P_n$.

Вопрос 1. Является ли каждая конечно-простеганная теория почти гладкой?

Теорема 1. Предположим, что элементарная теория линейно упорядоченной достаточно насыщенной структуры $(M, <, \dots)$ является почти гладкой конечно-простеганной, а f — ее формульной функцией. Пусть N будет достаточно насыщенным элементарным расширением структуры M. Тогда для любого сечения $s = \langle C, D \rangle$ и любого ростка A из этого сечения сужение функции f на множество $s(N) \cap A$ является локально монотонным.

Доказательство. Пусть элементарная теория линейно упорядоченной структуры $(M, <, \dots)$ будет конечно-простеганной, а f ее формульной функцией. Рассмотрим сечение $s = \langle C, D \rangle$. Легко понять, что множество всех формульных подмножеств заданной упорядоченной структуры разбивается на конечное число ростков относительно данного сечения. Пусть N будет достаточно насыщенным элементарным расширением структуры M. Возьмем некоторый росток A, заданный на сечении s и рассмотрим подмножество $B = s(N) \cap A$ структуры N. Очевидно, что, на самом деле, B является множеством всех реализаций в структуре N некоторого 1-типа над структурой M. Заметим, что это множество неформульное. Пусть $\alpha, \beta \in s(N)$. Можем заменит рассмотрение неформульного множества B на рассмотрение формульного множества $E = (\alpha, \beta) \cap B$. Его формульность можно нетрудно доказать.

Рассмотрим сужение функции f на E. Заметим, что если рассматривать определимые множества над M и множества вида $f(x) > f(\gamma), f(x) = f(\gamma), f(x) < f(\gamma)$, где $\gamma \in E$, то полученная структура будет слабо о-минимальной, в следующем смысле.

Рассмотрим формулу $f(x) > f(\gamma) \wedge x \in E$. Предположим, что множество всех ее реализаций состоит из бесконечного числа выпуклых компонент. Тогда существует сечение, которое совместно как с формулой $f(x) > f(\gamma) \wedge x \in E$, так и с ее отрицанием. Пусть интервал (a, b) в M

будет таким, что $a < E < b$. Тогда в силу того, что рассматриваемая теория почти гладкая можно понять, что существует подынтервал I в M, содержащий E, в котором все типы определяются сечением и попарно несовместными формулами $P_1, \dots, P_n$. Но тогда мы получаем, что количество формул, определяющих типы в сечении, выросло. Но эта формула имеет параметры из элементарного расширения. Но в силу того, что структура M является достаточно насыщенной, получаем, что можно найти параметры уже из M, так что формулы $P_1, \dots, P_n$ уже не определяют полностью тип, совместный с некоторым сечением. Получаем противоречие. Иначе говоря, если множество всех реализаций формулы $f(x) > f(\gamma) \wedge x \in E$ не является конечным объединением выпуклых множеств, то можно найти сечение в E, которое имеет два расширения. Но само E было получено, как одно из n возможных расширений сечений. Следовательно, в новом найденном сечении количество расширений выросло. Поскольку теория является конечно-простеганной, подобное возможно лишь конечное число раз.

Формулы $f(x) = f(\gamma) \wedge x \in E$ и $f(x) < f(\gamma) \wedge x \in E$ рассматриваем аналогично.

А теперь можно провести один в один доказательство о локальной монотонности одноместной функции, как это было проделано для слабо о-минимальных теорий. Действительно, для слабо о-минимальных структур верна теорема о локальной монотонности формульных функций одной переменной [2]. Поскольку функция f определена над M, то получаем, что сужение функции f на множество E будет локально монотонным. Так как выбор α и β был произвольным, то получаем, что сужение функции f на множество B так же является локально монотонным.

Таким образом, теорема доказана.

Список использованной литературы

1 Pillay A., Steinhorn Ch. Definable sets in ordered structures.1 // Trans. Amer. Math. Soc. — 1986. — Vol. 295. — P. 565–592.

2 Macpherson D., Marker D., Steinhorn Ch. Weakly o-minimal structures and real closed fields // Transactions of The American Mathematical Society. — 2000. — Vol. 352. — P. 5435–5483.

3. Kulpeshov B.Sh. Weakly o-minimal structures and some of their properties // The Journal of Symbolic Logic. — 1998. — Vol. 63. — P. 1511–1528.

4. Bektursynova A., Yergozhina N., Verbovskiy V. Some properties of finitely quilted ordered structures // SDU Khabarshysy, 2016, № 1 (36), P. 103–108.