МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное
автономное образовательное
учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ
ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

СКФУ СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Сборник материалов
IX Всероссийской научно-практической конференции
(г. Ставрополь, 19-21 декабря 2018 года)

Часть 2

Министерство науки и высшего образования Российской Федерации
Северо-Кавказский федеральный университет (г. Ставрополь)
Институт компьютерных технологий и информационной
безопасности Инженерно-технологической академии
Южного федерального университета (г. Таганрог)
Ростовский государственный экономический университет (РИНХ)
(г. Ростов-на-Дону)
Новосибирский государственный технический университет
Оренбургский государственный университет

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

**Сборник материалов IX Всероссийской
научно-технической конференции**
(г. Ставрополь, 19-21 декабря 2018 года)

Часть 2

Ставрополь
2019

УДК 004.2/.9 (082)
ББК 32.97 я43
С 88

ОРГКОМИТЕТ КОНФЕРЕНЦИИ

Председатель

Лиховид А. А. – проректор по научной работе и стратегическому развитию СКФУ, доктор географических наук, кандидат биологических наук, профессор.

Члены оргкомитета:

Мезенцева О.С. – директора Института информационных технологий и телекоммуникаций Северо-Кавказского федерального университета (ИИТТ СКФУ), кандидат физико-математических наук, доцент.

Петренко В.И. – заместитель директора по научной работе ИИТТ СКФУ, заведующий кафедрой организации и технологии защиты информации, кандидат технических наук, доцент.

Веселов Г.Е. – директор института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета (г. Таганрог), доктор технических наук, доцент.

Самойлов А.Н. – заместитель директора института компьютерных технологий и информационной безопасности по научной и международной деятельности Инженерно-технологической академии Южного федерального университета (г. Таганрог), кандидат технических наук, доцент.

Тищенко Е.Н. – заведующий кафедрой информационных технологий и защиты информации Ростовского государственного экономического университета (РИНХ) (г. Ростов), доктор экономических наук, профессор.

Лапина М.А. – заместитель директора по международной деятельности ИИТТ СКФУ, доцент кафедры информационной безопасности автоматизированных систем, кандидат физико-математических наук, доцент.

Бакаев М.А. – доцент кафедры автоматизированных систем управления Новосибирского государственного технического университета, кандидат технических наук, доцент.

Парфенов Д.И. – доцент кафедры прикладной математики Оренбургского государственного университета, кандидат технических наук, доцент.

Соломонов Д.В. – старший преподаватель кафедры информационной безопасности автоматизированных систем ИИТТ СКФУ.

Костюк Д.В. – инженер-лаборант кафедры инфокоммуникаций ИИТТ СКФУ.

Ответственный секретарь

Плетухина А.А. – доцент кафедры информатики ИИТТ СКФУ, кандидат технических наук, доцент.

С 88 Студенческая наука для развития информационного общества: сборник мат-лов IX Всероссийской науч.-техн. конференции. Ч.2. – Ставрополь: Изд-во СКФУ, 2019. – 381 с.

ISBN 978-5-9296-0992-3

Материалы конференции посвящены вопросам развития инновационных образовательных и инфокоммуникационных технологий, проблемам информационной безопасности объектов информатизации, изучению информационных систем и технологий. Изложены результаты научных исследований в области разработки информационных технологий решения экономических задач.

УДК 004.2/.9 (082)
ББК 32.97 я43

ISBN 978-5-9296-0992-3

СОДЕРЖАНИЕ

Секция 3 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

Секция 3. Информационная безопасность объектов информатизации
Подсекция 1 7
Sevastianov S. A., Orel D. V., Minkina T. V., Antonov I. V. The main aspects of the use of technology implement the Internet of Things 8
Борисов А. П., Сергеев Д. Н. Разработка кодграббера на основе Arduino NANO для обучения студентов направления «Информационная безопасность» .. 14
Ванина А.Г., Галачиев С. Обеспечение безопасности транспортных средств 25
Выборнова О.Н., Дёмин К.С. Вирусы-майнеры - способы их обнаружения и удаления 33
Орёл Д.В., Карабанова А.Н., Минкина Т.В., Брехов М.А., Букреев А.В. Биометрическое распознавание голоса в системе безопасности 42
Петренко В. И., Заволокина У. В., Унтевский Н. Ю., Гурчинский М. М., Пижевский Д. Е. Применение методики прогнозирования на основе полиномиальных трендов для анализа киберактивности в РФ 53
Петренко В. И., Кочанов М. С., Павлов А. С. Сравнительный обзор методов обеспечения информационной безопасности от утечки информации в задачах цифровой экономики 62
Петренко В. И., Нечволода В. Э., Смыкова В. Н., Рябцев С. С. Сравнительный анализ функциональных возможностей средств мониторинга компьютерной сети 69
Родин Д. А., Бесланеева Е. Ю., Лапина М. А., Емельянов Е. А. Исследование возможности создания SIEM-систем на основе открытых источников показателей компрометации 79
Степанян Н. Э., Минкина Т. В., Орел Д. В. Защита шаблонов в биометрических системах аутентификации 88
Тебуева Ф. Б., Джамиев Н-М.Д., Стручков И.В. Оценка применимости отечественной криптографии в протоколе Matrix 97
Тебуева Ф. Б., Ермолов И. В., Шутова Ю. А. Структурный анализ уязвимостей технологии распределенного реестра на примере криптовалютных систем 107
Тебуева Ф.Б., Пижевский Д.Е., Антонов В.О., Заволокина У.В., Унтевский Н.Ю. Анализ мировой тенденции роста киберугроз на основе линейной аппроксимации статистических данных об атаках 118
Унтевский Н.Ю., Минкина Т.В., Орел Д.В. Анализ функциональных возможностей продуктов компании Инфотекс по защите мобильных коммуникаций в корпоративной среде 128
Секция 3. Информационная безопасность объектов информатизации
Подсекция 2 136

Ажмухамедов И.М., Гончаров А.Б. Разработка методики построения психологического портрета потенциального нарушителя путем анализа его активности в социальных сетях 137
Ажмухамедов И.М., Мачуева Д.А., Глебов В.В. Модель информационного взаимодействия в социальной среде как основа противодействия идеологическому экстремизму 148
Ажмухамедов И.М., Полетаев Н.С., Гурская Т.Г. Разработка программного обеспечения для реализации защищённого удостоверения личности на основе стеганографических и криптографических алгоритмов..... 157
Выборнова О.Н., Александрович В.П. Мониторинг информационного фона в вузе на основе протокола тайного голосования 166
Данилов М.М., Шилина А.Н., Московченко В.М., Гайдаревский А.А. Предложения по совершенствованию методики расчета показателей эффективности управления системой обеспечения безопасности объектов информатизации 176
Данилова О. Т., Иниватов Д. П. Анализ действий пользователя в операционной системе Linux 183
Калашникова В.А., Жолобов П. А., Филатов А. Д., Песков М.В. Поддержка актуального состояния программного обеспечения как средство защиты данных 192
Калмыков И.А., Калмыков М.И., Чистоусов Н.К., Степанова Е.П. Разработка протокола аутентификации космического аппарата для повышения информационной скрытности системы спутниковой связи 200
Кузина Н.Н., Наумова А.В. Формирование культуры информационной безопасности у учащихся 209
Курчеева Г.И., Затолокин М.Ю. The process model requirements for the "Smart City" system using the Blockchain distributed transaction network 216
Лапина М. А., Анзина А. В., Медведева А. Д. Исследование аутентификации в протоколе SSH..... 224
Лапина М.А., Маршанский Н.А., Ходакова В.А. Исследование принципов работы, технических и эксплуатационных аспектов средств идентификации и аутентификации..... 233
Лапина М.А., Моторикин Д.В., Барышев Д.М. Анализ внутренних уязвимостей корпоративных сетей..... 242

Секция 4. «Робототехнические системы»

Секция 4. Робототехнические системы 250
Исаев А. М., Абелян А. А., Уварова А. А. Разработка подсистемы сенсоров мобильного балансирующего робота 251
Исаев А. М., Важенская И. А., Тупикина М. А. Проектирование мобильного двухколесного балансирующего робота в среде Solidworks..... 261
Исаев М. А., Исаев А.М., Линец Г.И., Адамчук А.С. Исследование вибраций конструкции мультироторного беспилотного летательного аппарата методами спектрального анализа 271
Мокшин В.В., Стадник Н.А., Золотухин А.В. Имитационное моделирование авиатранспортного предприятия 281

Мыцко Е.А., Рачис В.А., Медетова Г.М., Бейшенбаев Э.И., Галлингер В.А. Разработка робототехнической платформы для интеллектуального ремонта дорожного полотна «RoadBot» 289
Новикова Е.Н., Операйло К.В., Якимов М.А. Анализ перспективных направлений искусственного интеллекта 297
Оленев А. А., Савенко Е. В. Актуальность внедрения робототехники в образовательный процесс 307
Секция 5. «Инновационные образовательные технологии»
Секция 5. Инновационные образовательные технологии 317
Багдасарян Л. Ш., Григоренко В. И., Татаренко В. А. Инновационные технологии в организации и управлении образовательной деятельностью 318
Багдасарян Л. Ш., Козуб А. Ю., Яковенко Ю. А. Информационные технологии в организации и проведении социологического исследования 324
Зверева Л.Г., Петрович М.П. Использование информационных технологий на уроках математики при закреплении учебного материала 331
Кручинин Д.В., Сеитбекова Л.Д., Нугманов Д.Т. Применение игровых методов обучения для закрепления теоретического материала по математическим дисциплинам 337
Оленев А.А., Петрович М.П. Использование СКА Maxima на уроках алгебры при подготовке к ЕГЭ 346
Оленев А.А., Халидова О.Х. Операции с полиномами в системе компьютерной алгебры Maple для учащихся средней школы 354
Шевченко Г. И., Лайпанова Д. М. Информационные технологии в подготовке к ОГЭ по информатике 361
Шевченко Г.И., Джанибекова К.Р. Использование технологии компьютерного тестирования в учебном процессе 369
Шевченко Г.И., Шевелева М.С. Элективные курсы, как способ профильно-дифференцированного обучения информатике 376

Секция 3. «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

Подсекция 1

THE MAIN ASPECTS OF THE USE OF TECHNOLOGY IMPLEMENT THE INTERNET OF THINGS

Sevastianov Sergei Aleksandrovich[1]
drag2662@yandex.ru

Orel Dmitrii Viktorovich[1]
kde.def@gmail.com

Minkina Tatiana Vladimirovna[1]
n.min@mail.ru

Antonov Ilia Vladimirovich[1]
antaunov@gmail.com

[1] North-Caucasus Federal University, Stavropol, 355000, Russian Federation

Abstract

For example, a cloud service receives data of the speed of thousands of cars and builds a map of congestion of the city, helping motorists finding the fastest route.
The bracelet on the foot of a football player tracks his activity during training and sends data to a mobile application or a program on another device to draft statistics and results of the players. Intelligent meters transfer readings online, report leaks, help saving resources and reduce utility bills. What's more, conveyors with intelligent filling warn the operator about the signs of the approaching deterioration of a technological unit and by this way the production is being prevented from halt and repair costs are reduced.
The article deals with the facts about the Internet of things with the help of which people's lives become much easier. 5 aspects about the Internet of things are given and considered, their images are given.

Keywords: Internet of things, IoT, Cisco, report GrowthEnabler, power supplies, solar energy, smart comb.

1 Introduction

As the number of devices connected to the Internet increase the developers are facing a problem on the implementation of the connection between the device and the person [1].

The first Internet of Things device was connected to the internet in 1981 [2]. The term Internet of Things appeared not so long ago, the first Internet of Things device was connected to the Internet much earlier, as the first browser in history was launched.

2 Formulation of the problem

The motivation for launching this innovative technology project was enormous: the engineers at Carnegie Mellon wondered if there was a Coca-Cola drink in the vending machine and what is the cooling temperature of the drinks in the vending machine.

To solve this task they connected the sensors of the machine to the Internet [10] and created a text-based interface, so that any Internet user from anywhere in the world could connected to the machine to see the number of remaining drinks and their temperature.

3 The development of the technology of the Internet of Things

It may sounds a bit trivial but the Internet of Things device illustrates the basic principle behind these technologies. Each time, the number of users of the Internet of Things is growing in the field of information technology to know what is happening in the real world, as well as in cyberspace.

The inflow of users of the Internet of Things, takes its origins in 2008.

Another surprising fact is that the number of IoT devices as an Internet application has exceeded the number of people on the planet.

According to the Cisco IBSG report, the number of devices connected to the Internet exceeded the number of people in 2008, Figure 1 shows the relation graph.

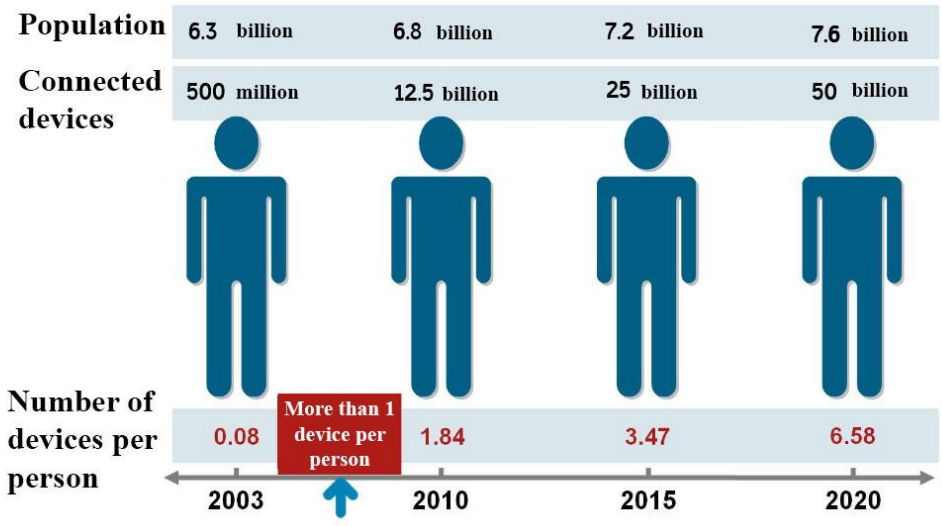

Figure 1. The approximate number of devices for 2018 is 4pcs per person, by 2020 this figure will increase about 1.5 times

Smart City devices take the largest percentage of the Internet of Things.

According to the GrowthEnabler report, on the Internet of Things market, the first 3 positions are taken by: Smart City (26%), industry (24%) and healthcare (20%). Figure 2 shows the chart as a percentage of using the Internet of Things.

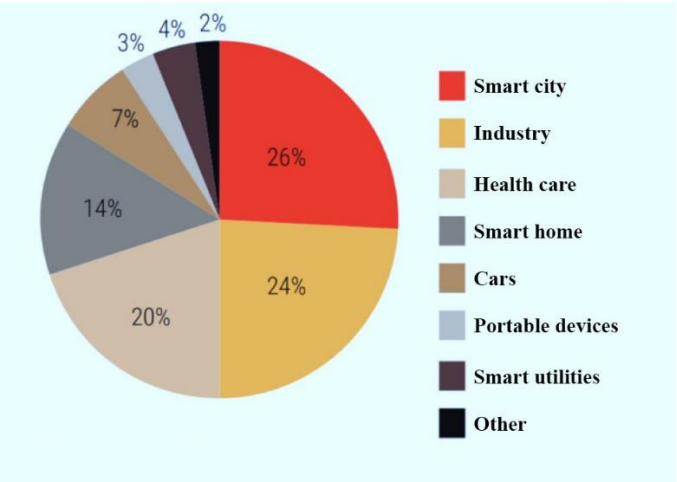

Figure 2. Chart as a percentage of using Internet of Things

Creators and manufacturers should take into account these statistics and adjust their strategies in creating the Internet of Things. Instead of looking for ways to promote devices that have already been manufactured they should strive to integrate them into other devices [5] so that their pairing is compatible.

“Independent” Internet of Things devices are currently in development.

One of the main aspects of the Internet of Things is that the essential sensors for collecting data and sending them over the Internet require a power source. This means that the IoT device must have a wired connection to a power source (which is detrimental to the goal) or it must have a removable or rechargeable power source [9].

Meanwhile the Internet of Things devices that are independent of power sources are already available on the market. These sensors are powered by solar energy (Figure 3 shows the Internet of things with a solar panel), heat, vibrations, or even radio frequencies.

Figure 3. Internet of Things kit using solar energy power source with BLE wireless technology

IoT hairbrush.

Perhaps one of the most interesting devices of the Internet of Things is a hairbrush developed by L'Oréal. Figure 4 shows the hairbrush and the data from the device which is paired with it.

Figure 4. Smart hairbrush and associated application

As the description tells, a smart hairbrush Kerastase Hair Coach, which works with replaceable batteries and does not have a rechargeable battery, is a rather complicated electronic device. Equipped with:

– a microphone that “listens” to the sound of combed hair. Transmits information, allowing you to determine their status and patterns of the process. For example the degree of elasticity, the dryness, the brittleness and the tendency to excision [7];

– 3-axial strain gauges that measure the force applied to the hair and scalp when combing [8];

– an accelerometer and a gyroscope, defining the “combing lines” of hair, counting produced movements - including control and feedback when the user performs the recommendations of the virtual trainer;

– conductivity sensors which determine whether the hair is dry or wet are combined [4]. The body of the comb is protected from moisture and allows brushing the hair after washing, but is not recommended for immersion in water;

– Wi-Fi and Bluetooth modules that send the information collected by the comb sensors into a mobile application on a smartphone [6].

In the application weather factors are taken into account: wind strength, humidity, ambient temperature, ultraviolet radiation power in a given period.

4 Conclusion

And finally, the most important thing. Leading technology companies have not made enough efforts to develop solutions for securing IoT applications.

If the giants of the industry do not take on this crucial task, then responsibilities will come crashing down on many start-up companies which largely ensure the current growth of the IoT sector.

According to the assessment of the consulting company Gartner, in 2017 more than half of the IoT products were produced by small companies that have been operating for less than three years. One can imagine that only a part of these companies are able to ensure a normal level of safety of their products.

5 Discussion

We need to figure out how to help this new generation of developers by equiping them with the knowledge on providing really solid security for IoT devices.

First, manufacturers should be encouraged to cooperate more actively with suppliers of software, hardware, and with the ecosystem of the industry entirely. Senior partners can be a valuable source of experience and knowledge for the application of existing standards and safety elements for novices in the market.

Secondly, it is necessary to develop the education in this field. An example is the creation of security laboratories based on Microsoft, Breed Reply and Indiegogo.

In these laboratories, even small developing companies could access advanced equipment and make their contribution to the development of security systems. People working in these laboratories will find out that safety issues must be top priority at all stages of an IoT project - from idea to mass production and even after and during operation.

In an ideal world there is no security threats. But in our world, more and more things can be connected to the Internet which means the number of things that are potentially in the risk hacking is increasing. We may never solve this fundamental problem but by joining forces we can create the secure Internet of things the world deserves.

List of references

[1] Minkina T., Sorokina N. Social Innovation And Education. *Social and economic innovations: trends, forecasts and perspectives conference proceedings of the Ist International Conference.* Russian State Social University (Stavropol branch); under the editorship of PhD, associate professor O. Yu. Kolosova, PhD, senior lecturer K. V. Bagmet, assistent K. A. Andikaeva. 2015. P. 284-288.

[2] Mandritsa I.V., Stefano S., Mandritsa O.V., Petrenko V.I. Mechanism Of Economic Security Relativelly To Market Agents On Possible Leaks Of Business Information. *Modern Economy Success*. 2016. № 1. P. 19-31.

[3] Nemkov R., Mezentseva O., Mezentsev D., Brodnikov M. Image Recognition By A Second-Order Convolutional Neural Network With Dynamic Receptive Fields. *CEUR Workshop Proceedings 2*. Сер. "YSIP2 2017 - Proceedings of the 2nd Young Scientist's International Workshop on Trends in Information Processing" 2017. P. 147-151.

[4] Dmitrii Orel, Aleksandr Zhuk, Elena Zhuk, Liudmila Luganskaia. A Method of Forming Code Sets for CDMA in Communication, Navigation and Control Systems. *CEUR Workshop Proceedings 2*. Сер. "YSIP2 2017 - Proceedings of the 2nd Young Scientist's International Workshop on Trends in Information Processing" 2017. P. 158-167.

[5] Shlaev D.V., Gaychuk D.V., Rezenkov D.N., Minkina T.V., Durakova A.S. Development The Module Algorithm Of Information System To Face Detection For Smart Environments. *research journal of pharmaceutical, biological and chemical sciences*. 2016. Т. 7. № 6. С. 2299-2302.

[6] Zhuk A.P., Orel D.V., Luganskaia L.A. Method Of Forming Signal Sets With The Required Correlation Properties For Wireless Infocommunication System. *Infocommunication Technologies In Science, Production and Education (Infocom-6)*. Proceedings of the 6th International scientific technical conference. – Stavropol, NCFU Publ., 2014, P. 24-28.

[7] Tebueva F., Kopytov V., Petrenko V., Kharechkin P., Sidorchuk A. Method For Detecting And Eliminating Data Time Series Outlier In High-Speed Process Data Sensors. *International Journal on Communications Antenna and Propagation*. 2017. V. 7. # 7. P. 603-612.

[8] Petrenko V.I., Tebueva F.B., Sychkov V.B., Antonov V.O., Gurchinsky M.M. Calculating Rotation Angles Of The Operator's Arms Based On Generalized Coordinates Of The Master Device With Following Anthropomorphic Manipulator In Real Time. *International Journal of Mechanical Engineering and Technology*. 2018. V. 9. # 7. P. 447-461.

[9] Kopytov V.V., Petrenko V.I., Tebueva F.B., Streblianskaia N.V. An Improved Brown's Method Applying Fractal Dimension To Forecast The Load In A Computing Cluster For Short Time Series. *Indian Journal of Science and Technology*. 2016. V. 9. # 19. P. 93909.

[10] Tebueva F.B., Kopytov V.V., Petrenko V.I., Shulgin A.O., Demurchev N.G. The Identification Of Data Anomalies From Information Sensors Based On The Estimation Of The Correlation Dimension Of The Time Series Attractor In Situational Management Systems. *Journal of Theoretical and Applied Information Technology*. 2018. V. 96. # 8. P. 2197-2207.

РАЗРАБОТКА КОДГРАББЕРА НА ОСНОВЕ ARDUINO NANO ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Сергеев Д. Н.[1]
choma98@mail.ru

Борисов А.П.[2]
alex.borisov84@gmail.com
Кандидат технических наук, доцент

[1] Алтайский государственный технический университет им. И. И. Ползунова, г. Барнаул, 656906, Российская федерация
[2] Алтайский государственный технический университет им. И. И. Ползунова, г. Барнаул, 656038, Российская федерация

Аннотация

Статья посвящена вопросам безопасности на различных предприятиях, промышленных территориях, парковках, многоквартирных домах, гаражных комплексах, где для ограничения доступа используются управляемые по беспроводному каналу шлагбаумы и автоматические ворота. Цель исследования заключается в разработке лабораторного устройства, предназначенного для несанкционированного перехвата передаваемого сигнала и дальнейшего его использования. Для подготовки высококвалифицированных кадров необходимо наличие практических занятий для закрепление теоретических знаний студента, на которых он бы мог детально изучить устройство, предназначенное для перехвата сигнала, передаваемого беспроводным путем, понять принцип его работы, попытаться самостоятельно сконструировать средство по защите от таких перехватывающих сигналы устройств и применить полученные знания и умения на практике в учебных целях.

Помимо этого, специалистам в области информационной безопасности необходимо владеть навыками по взлому и защите охраняемых систем. Такой прибор, как кодграббер может помочь выявить уязвимости различных электронных замков, которые используются как в шлагбаумах, так и в электронных воротах. В условиях современного рынка представлены различные дорогостоящие устройства, позволяющие перехватывать защищенный сигнал, что является их значительным недостатком по сравнению с разрабатываемым лабораторным прибором, позволяющим студентам изучить вопросы безопасности информации.
Выявлена и обоснована необходимость разработки лабораторного устройства.

Abstract

The article is devoted to security issues at various enterprises, industrial areas, parking lots, apartment buildings, garage complexes, where barriers and automatic gates are used to restrict access.
The purpose of the study is to develop a laboratory device designed for unauthorized interception of the transmitted signal and its further use. To train highly qualified personnel it is necessary to have practical training to consolidate the theoretical knowledge of the student, on which he could study in detail the device designed to intercept a signal transmitted wirelessly, understand its principle of operation, try to design a means to protect against such intercepting devices and apply acquired knowledge and skills in practice for educational purposes. In addition, specialists in the field of information security must possess skills to hack and protect protected systems. Such a device as a code grabber can help identify the vulnerabilities of various electronic locks, which are used both in barriers and in electronic gates. In the conditions of the modern market, various expensive devices are presented that allow intercepting a protected signal, which is a significant disadvantage in comparison with a developed laboratory instrument that allows students to study information security issues.
Identified and justified the need to develop a laboratory device.

Ключевые слова: кодграббер, лабораторная установка, система технической защиты информации, беспроводные технологии, перехват сигнала, NRF905, Arduino Nano, разработка средств защиты.

Keywords: code grabber, laboratory installation, technical information protection system, wireless technologies, signal interception, NRF905, Arduino Nano, development of protection tools.

1 Введение

В настоящее время все стремительнее развиваются беспроводные технологии. Почти на каждом предприятии используются устройства, подключаемые и управляемые по воздуху. Невозможно представить нашу жизнь без дистанционных пультов управления, которые во многом облегчают взаимодействие человека с объектами, использующими в своей работе получаемые и отправляемые сигналы.

Ограничение доступа для проникновения актуально как в условиях различных предприятий, так и на защищаемых объектах. Частные и многоквартирные дома, промышленные территории, торговые центры, парковки и гаражные комплексы — эти и многие другие объекты нуждаются в строгом контроле доступа. Одним из самых удобных и надежных способов обеспечить такой контроль является установка шлагбаума или автоматических ворот. Но что, если злоумышленнику потребуется проникнуть на охраняемый объект? Ведь большая часть автоматических запирающих устройств, работающих с пульта, может быть взломана.

2 Постановка задачи

Целью специалистов в области информационной безопасности является защита передаваемой и хранимой информации и поддержание ее целостности. Прежде всего, это связано с использованием технических средств защиты. Техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [2]. Для подготовки высококвалифицированных кадров необходимо наличие практических занятий для закрепление теоретических знаний студента, на которых он бы мог детально изучить устройство, предназначенное для перехвата сигнала, передаваемого беспроводным путем, понять принцип его работы, попытаться самостоятельно сконструировать средство по защите от таких перехватывающих сигналы устройств и применить полученные знания и умения на практике в учебных целях. Помимо этого, специалистам в области информационной безопасности необходимо владеть навыками по взлому и защите охраняемых систем. Такой прибор, как кодграббер может помочь выявить уязвимости различных электронных замков, которые используются как в шлагбаумах, так и в электронных воротах. На рисунке 1 схематично показано устройство электронного шлагбаума:

Рисунок 1. 1 – шлагбаум; 2 - плата управления электронного замка шлагбаума; 3 – антенна, принимающая сигнал от брелока; 4 – брелок, открывающий или закрывающий шлагбаум; 5 – кодграббер, предназначенный для перехвата передаваемого сигнала от брелока.

Принимая во внимание все эти факторы, можно сделать вывод, что студенты, обучающиеся по направлению «Информационная безопасность» должны приобрести навыки по защите от таких устройств, как кодграббер, которые предназначены для перехвата защищенных сигналов. Для подготовки учебного процесса необходимо обеспечить лаборатории соответствующими стендами и оборудованием. Так как оборудование будет использоваться в учебных целях, необходимо детально продумать требования и все аспекты его использования, например: возможность замены его комплектующих элементов, в случае порчи; обеспечить ремонтопригодность устройства; разумную цену комплектующих.

Приобретение готового продукта не будет являться разумным решением в силу того, что большинство производимых на специализированных предприятиях устройств не будут соответствовать вышеперечисленным требованиям. Зачастую готовые решения имеют высокую стоимость и невозможность детального разбора и подробного изучения принципов его работы студентами ВУЗов. Таким образом, возникает необходимость создания кодграббера, предназначенного для перехвата сигналов и макета, для его использования в учебных целях.

3 Разработка методики

Этап разработки начался с создания модели устройства, приведенном на рисунке 2. Данный проект предполагает создание кодграббера, с помощью которого можно перехватить передаваемый сигнал от передатчика приемнику.

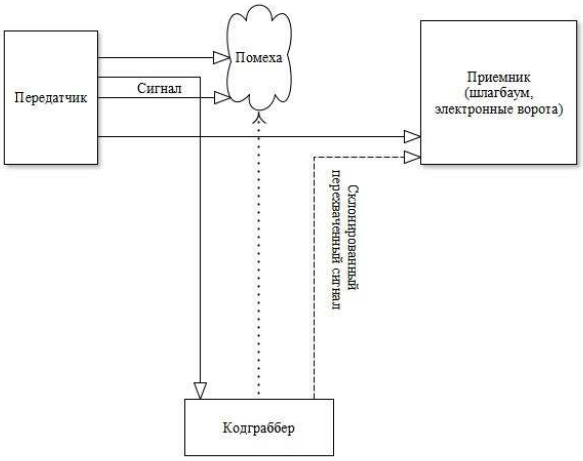

Рисунок 2. Модель устройства.

Следующим этапом стал выбор аппаратной составляющей устройства. Были рассмотрены несколько вариантов плат с собственным процессором и памятью, таких как Arduino Nano, Arduino Uno, а также платы на основе микроконтроллеров Raspberry Pi. Каждый из приведенных продуктов имеет свои преимущества, но в итоге была выбрана плата Arduino Nano [1], т.к на его основе можно относительно просто организовать перехват передаваемого беспроводного сигнала, а также его клонирование и передачу приемнику.

Был собран стенд, состоящий из шлагбаума на сервоприводе SG90, модуля передатчика сигнала с приемником 433 МГц и кодграббера, предназначенного для перехвата передаваемого сигнала. На рисунке 3 приведена схема подключения элементов к блокам управления:

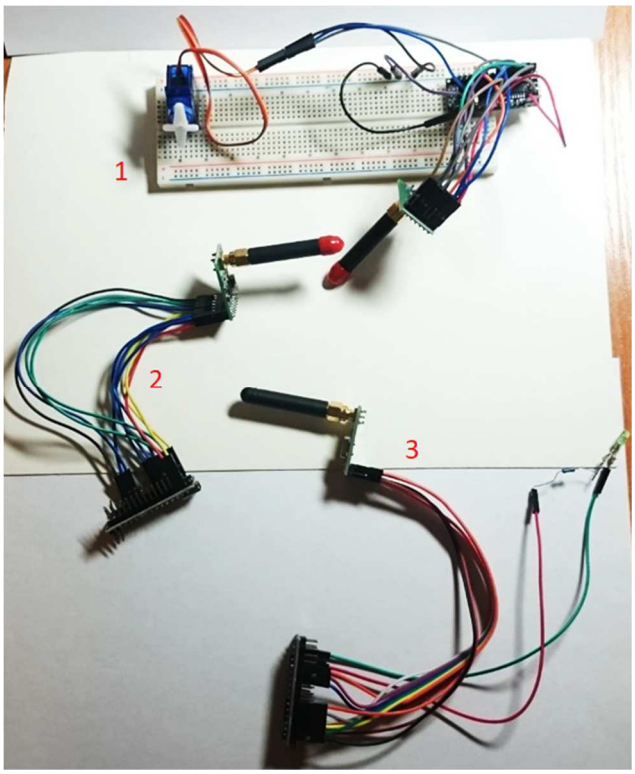

Рисунок 3. 1 – «шлагбаум»; 2 – передатчик; 3 – кодграббер.

Рассмотрим элементы, приведенные на рисунке 3, подробнее.

На рисунке 4 представлена схема, имитирующая работу шлагбаума, который представлен сервоприводом SG90.

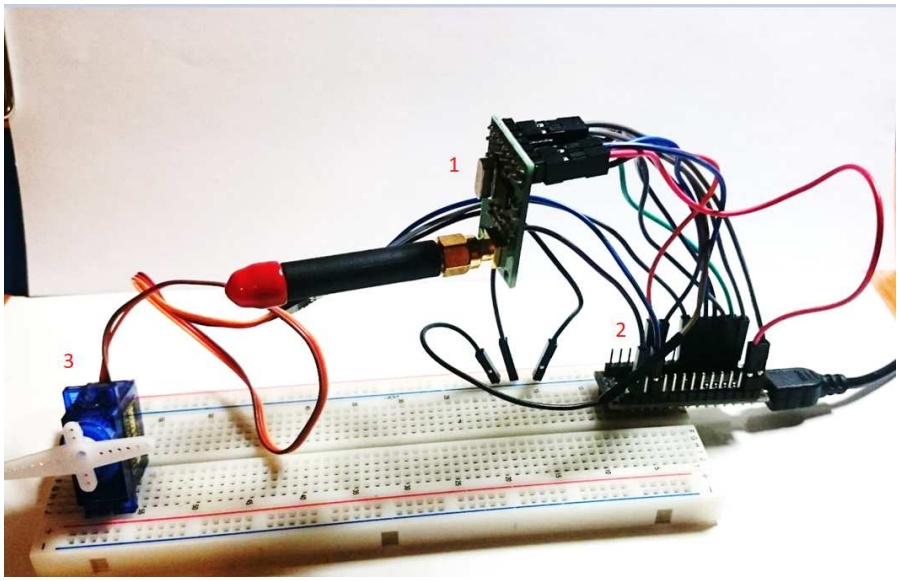

Рисунок 4. 1 – радиомодуль NRF905 с антенной (приемник); 2 - плата управления; 3 – сервопривод SG90 («шлагбаум»).

На рисунке 5 представлен передатчик, выполненный с помощью радиомодуля NRF905 и платы Arduino Nano.

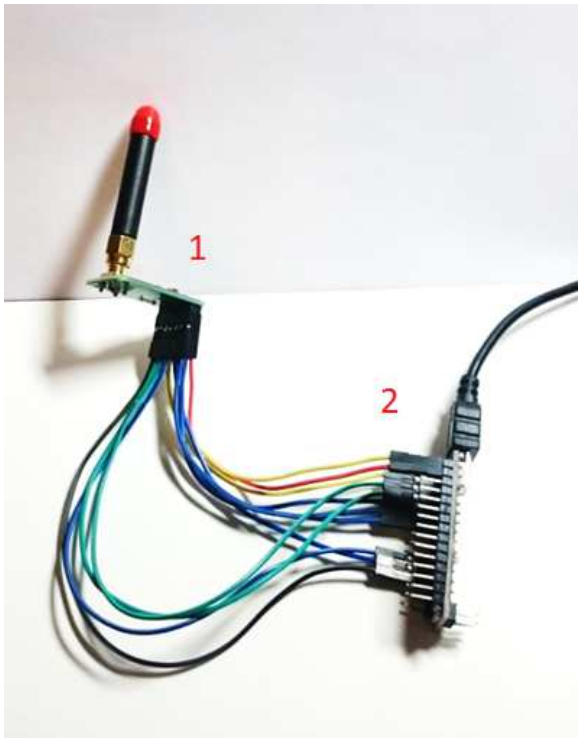

Рисунок 5. 1 – радиомодуль NRF905 с антенной (передатчик); 2 - плата управления.

На рисунке 6 представлен кодграббер, собранный на платформе Arduino Nano.

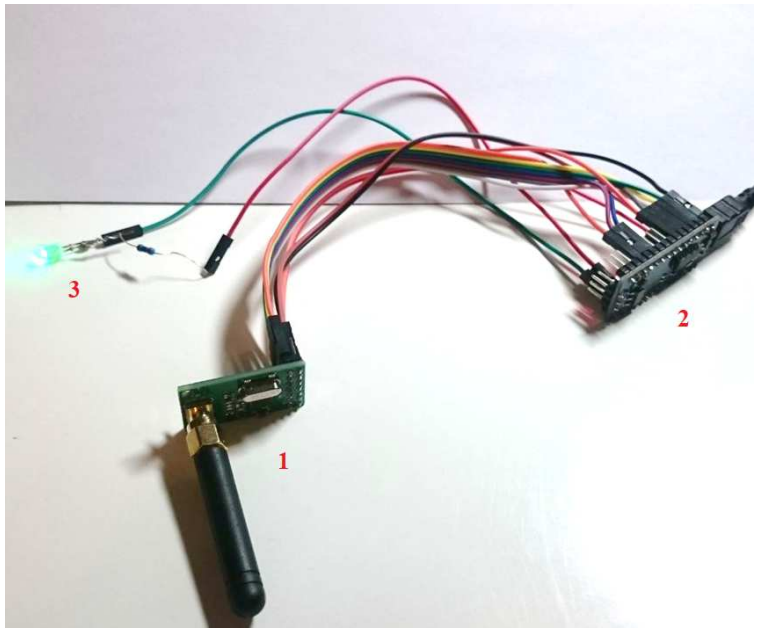

Рисунок 6. 1 – радиомодуль NRF905 с антенной; 2 - плата управления; 3 – светодиод для индикации.

4 Результаты

Принцип работы устройства заключается в следующем: передатчик передает сигнал приемнику, в то время как кодграббер создает помеху исходному сигналу и перехватывает его. Сигнал, дойдя до приемника, заставляет сработать сервопривод SG90, тем самым подняв «стрелу шлагбаума» в вертикальное положение.

После этого кодграббер может использовать перехваченный сигнал для открытия шлагбаума неограниченное количество раз.

Для начала подключаем лабораторный кодграббер к источнику питания. Управляемый радиомодуль NRF905 переключается в режим перехвата сигнала.

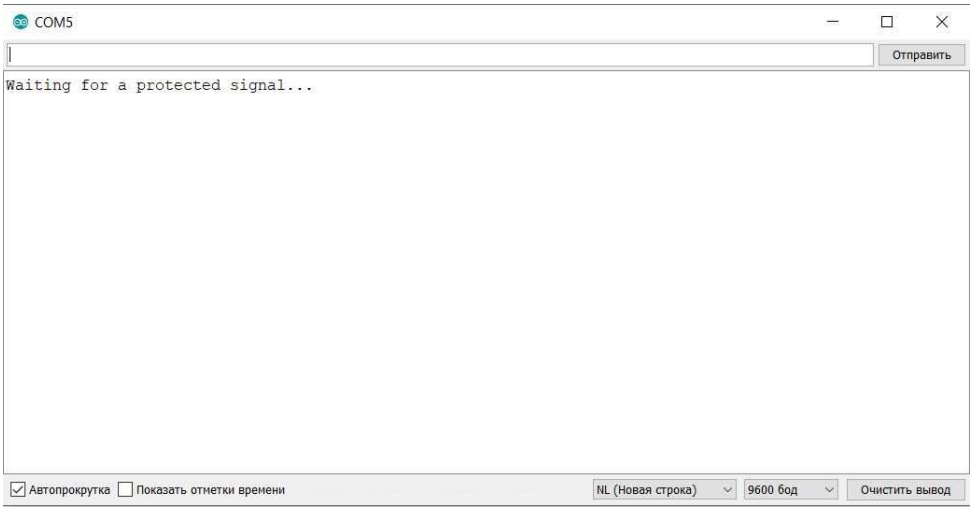

Рисунок 7. Ожидание сигнала для перехвата.

При подключении приемника с «шлагбаумом» радиомодуль NRF905 переключается в режим получения данных.

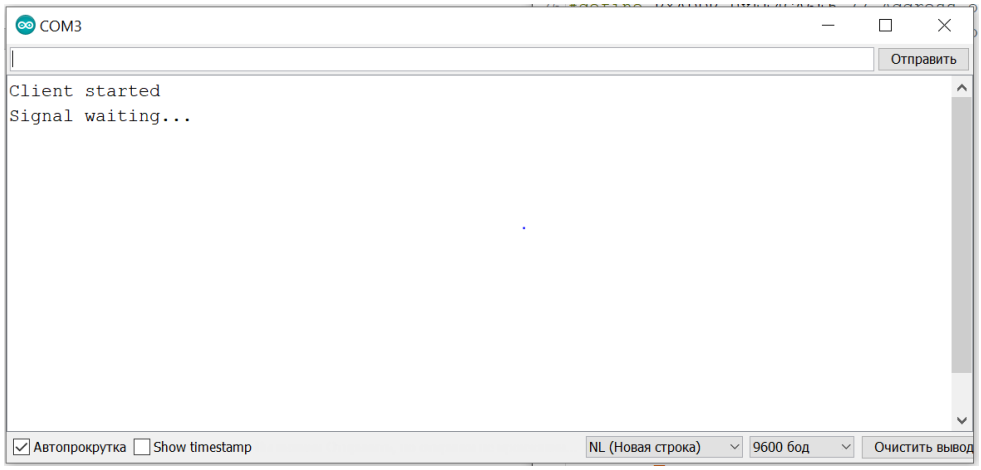

Рисунок 8. Ожидание сигнала от передатчика.

При отправке сигнала с приемника передатчик получает его и дает команду сервоприводу. Затем «стрела» меняет свое положение, тем самым открыв «шлагбаум».

Рисунок 9. Получение сигнала и открытие «шлагбаума».

После того, как кодграббер перехватит и расшифровал сигнал, загорается зеленый светодиод. Далее мы можем использовать этот сигнал его повторно для того, чтобы открыть «шлагбаум».

5 Заключение

Таким образом, созданный лабораторный стенд позволит студентам высших учебных заведений, обучающимся по направлению «Информационная безопасность», ознакомиться с принципами работы кодграббера по перехвату сигналов, разобрать и подробно изучить его, а также применить полученные знания на практике по разработке устройства, предотвращающего перехват передаваемого сигнала. При поломке данного устройства можно легко заменить испорченные радиодетали, а также произвести ремонт. Оно также имеет низкую стоимость, по сравнению с готовыми решениями на специализированных предприятиях.

Список используемой литературы

[1] Arduino Nano [Электронный ресурс] // официальный сайт URL: http://arduino.ru/Hardware/ArduinoBoardNano (дата обращения 13.05.2018).

[2] ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

[3] Максимов А.И., Борисов А.П. Разработка комплекса средств беспроводной передачи информации на базе микроконтроллеров Arduino // Использование цифровых средств обучения и робототехники в общем и профессиональном образовании: опыт, проблемы, перспективы [Текст]: сборник научных статей II Международной научно-практической конференции, Барнаул, 5-6 ноября 2015 г. – Барнаул : Изд-во Алт. Ун-та, 2015, С.107-110

[4] Белый С.С., Борисов А.П. Повышение качества проведения лабораторных работ при помощи устройства передачи данных по радиоканалу // Влияние науки на инновационное развитие: сборник статей Международной научно - практической конференции (28 февраля 2017 г., г. Екатеринбург). - Уфа: МЦИИ ОМЕГА САЙНС, 2017, с.22-24

[5] Литвинская О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М.: КноРус, 2015. - 168 с.

[6] Обзор современных технологий беспроводной передачи данных в частотных диапазонах ISM. [Электронный ресурс] / Беспроводные технологии – Режим доступа: http://wireless-e.ru/articles/technologies/2011_4_6.php

[7] Земор, Ж. Курс криптографии / Ж. Земор. - М.: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2006. - 256 с.

[8] Еремин В.Б., Борисов А.П. Исследование модулей SI4432 в городских условиях // Новая наука: от идеи к результату: Международное научное периодическое издание по итогам Международной научно-практической конференции (22 декабря 2016 г, г. Сургут). / в 4 ч. Ч.3 - Стерлитамак: АМИ, 2016 - с.70-72

[9] Максимов А.И., Борисов А.П. Исследование распространения радиосигналов с частотой 433 МГц в сложных городских условиях // Современный взгляд на будущее науки: сборник статей Международной научно - практической конференции (25 мая 2016 г., г. Томск). В 5 ч. ч.4 / - Уфа: АЭТЕРНА, 2016. – с. 71-74

[10] Белый С.С., Борисов А.П. Программа для передачи дан-ных радиомодемами Si4432 с криптографической защитой // Свидетельство о государственной регистрации программы для ЭВМ №2017663418, заявл. 05.10.17, опубл. 01.12.17

List of references

[1] Arduino Nano [Electronic resource] // official website URL: http://arduino.ru/Hardware/ArduinoBoardNano (access date 13/05/2018).

[2] GOST R 50922-2006 Information Security. Basic terms and definitions.

[3] Maksimov A.I., Borisov A.P. Development of a complex of wireless transmission of information based on Arduino microcontrollers // Using digital teaching aids and robotics in general and vocational education: experience, problems and perspectives [Text]: collection of scientific articles of the II International Scientific and Practical Conference, Barnaul, 5-6 November 2015 - Barnaul: Publishing house Alt. University, 2015, p.107-110

[4] Belyi S.S., Borisov A.P. Improving the quality of laboratory work using a data transmission device over a radio channel // The Impact of Science on Innovative Development: a collection of articles of the International Scientific and Practical Conference (February 28, 2017, Ekaterinburg). - Ufa: MTSII OMEGA SAINS, 2017, p.22-24

[5] Litvinskaya, O. S. Fundamentals of Information Transmission Theory. Tutorial / OS Litvinskaya, N.I. Chernyshev. - M .: KnoRus, 2015. - 168 c.

[6] Review of modern technologies for wireless data transmission in the ISM frequency bands. [Electronic resource] / Wireless technologies - Access mode: http://wireless-e.ru/articles/technologies/2011_4_6.php

[7] Zemor, J. Course of cryptography / J. Zemor. - M .: Regular and chaotic dynamics, Institute of Computer Science, 2006. - 256 c.

[8] Eremin V.B., Borisov A.P. Study of SI4432 modules in urban environments // New Science: from idea to result: International scientific periodical following the International Scientific and Practical Conference (December 22, 2016, Surgut). / in 4 hours. Part 3 - Sterlitamak: AMI, 2016 - p.70-72

[9] Maksimov A.I., Borisov A.P. Study of the propagation of radio signals with a frequency of 433 MHz in a complex urban environment // Modern view of the future of science: a collection of articles of the International Scientific and Practical Conference (May 25, 2016, Tomsk). At 5 am 4 / - Ufa: AETERNA, 2016. - p. 71-74

[10] Belyi S.S., Borisov A.P. The program for data transmission by radio modems Si4432 with cryptographic protection // Certificate of state registration of the computer program №2017663418, declared. 10/5/17, publ. 12/01/17

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ СРЕДСТВ

Галачиев С.М.[1]
joy.kantik@mail.ru

Ванина А.Г.[1]
к.т.н.
hnykina_anna@mail.ru

[1]Северо-Кавказский федеральный университет, Ставрополь, 355000, Россия

Аннотация

В статье рассмотрена возможность взлома различных систем автомобиля при помощи современных информационных технологий. Процесс активной компьютеризации автомобилей является одной из причин возникающих уязвимостей системы. В первую очередь отдельные элементы автоматизации стали объединять в сети промышленных контролеров CAN, а во-вторую, для связи с внешним миром были предложены самые разнообразные телематические системы.

Abstract

The article considers the possibility of hacking various car systems using modern information technology. The process of active computerization of cars is one of the causes of emerging system vulnerabilities. First of all, individual elements of automation began to merge into a network of CAN industrial controllers, and secondly, a wide variety of telematic systems were offered to communicate with the outside world.

Ключевые слова: безопасность, защита информации, кибертерроризм, электронные системы, система управления

Keywords: security, information security, cyberterrorism, electronic systems, control system

1. Введение

Первый в мире автомобиль, задуманный для перевозки человека, появился в 18 веке, вместе с созданием паросиловых машин. В эти времена ученые изобрели следующие двигатели: паровые, электрические, внутреннего сгорания. В начале 20 века появились первые автомобили, подготовленные для автоспорта, мощностью в 100, 200, 250 лошадиных сил. В то время такая мощность считалась очень большой. В автомобилях того времени использовались карбюраторные двигатели.

С 80-х годов 20-го века на автомобилях начали широко применять компьютерные технологии. На смену карбюраторным системам приходят инжекторы. Отличие такого способа подачи горючего основан на том, что главный элемент системы подачи топлива через форсунки - контроллер, сам определяет, когда и сколько смеси топлива с воздухом нужно двигателю, для сгорания топлива. Это был огромный скачок в развитии автомобилестроения. При работе двигателя, контроллер получает различные данные, такие как:

- положение и частота вращения коленчатого вала;
- массовый расход воздуха двигателем;
- температура охлаждающей жидкости;
- положение дроссельной заслонки;
- Объем кислорода в отработавших газах;
- наличие детонации в двигателе;
- напряжение в бортовой сети автомобиля;
- скорость автомобиля;
- положение распределительного вала;
- температура входящего воздуха.

Компьютер, используя сигналы датчиков, управляет следующими системами и устройствами:

- форсунки и электрический бензонасос;
- система зажигания;
- регулятор холостого хода (РХХ);
- система улавливания парами бензина;
- вентилятор системы охлаждения двигателя.

Так же контроллер помогает диагностировать автомобиль на наличие ошибок. При поломке автомобиля, подключается персональный компьютер или ноутбук к микроконтроллеру. Контроллер моментально определяет, что сломано в автомобиле, нам всего лишь понадобится информация о неисправной детали. Нам не нужно лезть под грязную машину, и искать поломанную деталь.

Двигатели 21 века создаются с применением новейших технологий, позволяющими получить от ста сил для бюджетного автомобиля и тысячу сил для спортивного гражданского автомобиля. Немыслимые показатели в сравнении с первыми автомобилями. Применяются следующие технологии: дополнительные системы управления (компьютеры),

турбокомпрессоры, облегченные элементы двигателя с внедрением угле пластика и уникальных сплавов, улучшенные системы подачи топлива.

Создателем механической коробки переключаемых передач был Карл Бенц. Изначально автомобили не имели такого механизма. Существовал единственный способ прямой передачи силы двигателя. Но, инженеры того времени понимали, что необходимо промежуточное звено для регулирования силы двигателя и увеличения скорости передвижения. Так была создана первая коробка переключаемых передач. Технологии развивались далее и в 1903 году немецкий профессор Феттингер запатентовал гидротранформатор.

В семидесятых годах 20 века начали создаваться автоматические коробки передач. АКПП состоит из 3 частей: электрическая, механическая, гидравлическая. Блок управления - основной элемент электрической части КПП. Он отвечает за:

- переключение передач
- корректную работу с двигателем.

В сравнении с механическими коробками передач, автоматические были очень медленными. Автомобиль разгонялся до максимальной скорости в разы хуже, чем на механической КПП. "Автомат не будет переключать передачи быстрее человека" - так утверждали инженеры.

В 2008 году компанией ZF была разработана новая АКПП, включающая восемь ступеней переключения. Сегодня человек не может переключать передачи быстрее АКПП. Всё благодаря новейшим технологиям.

Раньше автомобиль считался простым средством передвижения. Конструкция включала КПП, подвеску, кузов, элементы управления и сиденья. Сегодня недорогой авто включает в себя различные технологические системы. Такие помощники значительно облегчают использование автомобиля. Данные системы я считаю полезными и информационно-безопасными.

Новейшие технологические системы автомобиля

1. Мультимедийная система.

В 70-ых годах 20 века автомобили комплектовались простыми магнитофонами. Сегодня автомобили премиум класса комплектуются многофункциональными мультимедийными системами. Приведу в пример составляющие элементы и функции таких систем:

- связь сотового телефона и автомобиля по протоколу Bluetooth
- сенсорные экраны большого разрешения (могут располагаться по всему автомобилю: на центральной консоли, в подголовниках сидений).
- съемный планшет (BMW 7 серии 2015 модельного года комплектуется съемным планшетом «BMW Touch Command», позволяющий управлять мультимедийной системой, воспроизводить аудио и видео файлы с внешних источников, а также выходить в интернет.
- системы бесключевого доступа
- камеры кругового обзора
- система управления жестами (Впервые появилась на автомобиле BMW 7 серии в 2015 году. С помощью специальных датчиков система распознает определенные жесты и позволяет менять аудио и видео файлы, регулировать громкость, принимать или отклонять телефонные вызовы)
- беспроводное зарядное устройство мобильного телефона

2. Системы управления автомобилем

В современных автомобилях премиум класса, водитель, нажимая определенные кнопки на панели автомобиля, может изменять определенные характеристики. К примеру автомобили BMW имеют несколько запрограммированных вариантов скорости работы автоматической коробки передач, несколько запрограммированных вариантов работы двигателя, несколько запрограммированных вариантов работы ходовой части автомобиля (рулевого управления и работы амортизаторов).

3. Системы автоматической парковки

Современные автомобили премиум класса могут автоматически парковаться. Получая сигналы с датчиков, изображения с камер кругового обзора, программа ищет место на парковке. При обнаружении места, соответствующего габаритам автомобиля, компьютер дает команду на вращение колес и движение автомобиля на парковочное место.

4. Системы безопасности дорожного движения:
   - ассистент распознавания дорожных знаков
   - ассистент контроля полосы (Компьютер контролирует движение автомобиля, предупреждает о наезде на полосу движения, пресекает выезд за ее пределы)
   - ассистент контроля дорожного движения (Компьютер следит за автомобилями, препятствиями и пешеходами, он самостоятельно принимает решение на экстренную остановку автомобиля.
5. Системы движения
   - адаптивный круиз контроль (Автомобиль пристраивается за впереди движущимся транспортом, поддерживает дистанцию и скорость движения)
   - система автономного вождения (Робот самостоятельно управляет автомобилем без участия человека)
6. Системы навигации

Современные автомобили комплектуются средствами навигации. Они обеспечивают отображение местоположения автомобиля, поиск места назначения, мест для отдыха, автозаправочных станции и медицинских пунктов. Система ГЛОНАСС устанавливается на все новые автомобили, продаваемые в РФ. Предназначена для глобального слежения за движением транспорта. С помощью любых устройств, имеющих доступ в интернет, можно контролировать следующие параметры:

- местоположение автомобиля
- его скорость и направление движения в реальном времени
- время включения и выключения двигателя
- стоянка транспорта
- время использования механизмов

2. Постановка задачи

Растущее использование электронных систем в современных автомобилях, грузовиках и других транспортных средствах неизбежно представляет собой новый набор проблем. В первую очередь по соображениям безопасности. Компоненты, узлы, агрегаты, используемые в автомобильных системах, должны быть чрезвычайно устойчивыми к вредоносным атакам.

Поскольку использование электроники становится почти повсеместным в автомобильном мире, неизбежно возникают риски безопасности. Компоненты, используемые в любых транспортных средствах, должны быть чрезвычайно надежными, но они также должны быть чрезвычайно устойчивыми к вредоносным атакам. К примеру, владелец транспортного средства, который, естественно, имеет неограниченный физический доступ к нему, может в некоторых случаях стать частью угрозы. Также растет озадаченность по поводу кибертерроризма, в частности, попытки повлиять на инфраструктуру автомобиля,

завладеть персональными данными собственника. Также злоумышленники могут дистанционно управлять автомобилем, для совершения теракта или создания помех для движения специальной техники.

Связанные с этим риски и присущая им сложность, а также тот факт, что транспортное средство имеет сравнительно долгий срок службы, говорит о том, что обеспечение безопасности информации должно выполняться должным образом!

Две основные области, по которым необходимо решать проблемы информационной безопасности - мы обозначим их как «внешние» и «внутренние». Оба домена имеют тенденцию рассматривать информационную систему транспортного средства как единое целое, хотя на практике он, вероятно, будет состоять из многих отдельных компонентов.

Внутренний домен концентрируется на способности компонентов транспортного средства противостоять локальным атакам. Под «локальными» мы подразумеваем атаки, которые включают в себя физические атаки на различные ИТ-компоненты, а также атаки на интерфейсы между компонентами внутри самого транспортного средства. Атаки API также попадают в эту категорию, где они связаны с эксплуатацией интерфейсов между компонентами внутри транспортного средства.

Внешний домен концентрируется на связях между компонентами транспортного средства и техническими устройствами за его пределами. Он связан с возможными направлениями атаки, которые связаны с использованием ошибок протокола, на сетевом уровне, либо на уровне приложения. Примером внешней атаки может быть использование недостатка протокола для отправки сообщения об опасности дальнейшего движения, которое поступает с придорожной станции, но на самом деле происходит из домашней сети злоумышленника. Также под внешним доменом применяются атаки типа «отказ в обслуживании» через сетевые интерфейсы.

3. Результаты

Ключевое различие между методами, которые могут использоваться для борьбы с внутренними и внешними атаками, заключаются в различных стандартах, применяемых в каждом домене. В частности, безопасность внешнего домена основана на ужесточении протоколов, используемых транспортным средством для связи с другими объектами. Эти протоколы должны быть согласованы на межотраслевой основе, и поэтому работа по обеспечению их целостности должна основываться на высоком и широком уровне. Обеспечение внутренних аспектов автомобильной системы включает в себя проектные решения, которые входят в сферу действия отдельного изготовителя транспортного средства.

Чтобы обеспечить безопасность транспортной информационной системы во внутреннем домене, мы предлагаем стратегию, основанную на использовании набора инструментов.

Проще говоря, архитектура всеобъемлющей системы безопасности транспортных средств должна состоять из следующих компонентов:

Средства обеспечения безопасности базового уровня, обеспечивающие основные функции безопасности, характерные для транспортных сред, встраиваемые приложения, которые используют компоненты мультимедийной системы для обработки данных при использовании транспортных средств.

Поэтому цель инструментов защиты состоит в обеспечении общих функции безопасности на самом высоком уровне.

Элементы обеспечения безопасности:

1. Безопасные обновления.

Программное обеспечение в контроллерах транспортного средства потребуется обновлять несколько раз в течение эксплуатации. Используя средства обновления

приложений, контроллер можно безопасно обновлять, с авторизацией, выполняемой через центральное место в транспортном средстве. Этот помощник несет ответственность за:

- получение подписанных изображений кода и целевых контроллеров;
- подключение к контроллерам для надежной защиты;
- предоставление контроллеров с новым кодом или обновленной информацией; а также
- обновление реестра, для правильной работы после загрузки обновлений.

Для активации систему защиты, приложение должно быть установлено на контроллере. Это позволяет получать и обрабатывать новую информацию о кодах доступа. Невозможно обновить код встроенного программного обеспечения на контроллерах, за исключением подключения к их носителям с помощью других устройств, которые запускают приложение для обновления.

2. Безопасное ведение журнала данных

Цель безопасного ведения журнала – сбор и хранение данных обо всех действиях производимых в автомобиле. Например, приложение может использоваться для:

- записи данных о: скорости вождения, продолжительности пути и маршруте;
- записи данных о проведении технического обслуживания (например, время и показания одометра на сеансах обслуживания, а также информация о неисправностях)

Информация журнала должна быть защищена от несанкционированного доступа. К примеру, автомеханик, который подключает устройство для диагностики к контроллеру, не должен удалять или изменять данные о подключении к автомобилю.

3. Идентификация, аутентификация и авторизация в автомобиле

Система информационной безопасности автомобиля должна определять собственника авто, подтверждать право собственности или право на технические работы, и определять уровень доступа к системам автомобиля.

К примеру: собственник автомобиля будет иметь право заводить двигатель, управлять автомобилем, управлять мультимедийной системой, но у него будут ограничены права на увеличение мощности автомобиля путем чип-тюнинга, так как автопроизводитель запрещает проводить увеличение мощности вследствие уменьшения ресурса двигателя.

4. Контроль за частями автомобиля

Часто конструкция автомобиля подвергается изменению. Согласно постановлению ГИБДД, такие изменения являются небезопасными. Система информационной безопасности автомобиля должна самостоятельно фиксировать такие изменения и сообщать в ГИБДД. Также данные будут передаваться в дилерский центр.

5. Предотвращение краж автомобилей

Для предотвращения краж автомобилей будет использоваться программа, которая будет отключать основные компоненты транспортного средства в определенных сценариях, которые будут указывать на то, что неавторизованное лицо пытается вскрыть автомобиль в целях хищения.

6. Защита от активации функции.

Автомобили продаются по разным ценам в соответствии с их функциями и характеристиками. К примеру 3 серия BMW 2018 модельного года с индексом 320i стоит 2млн 300 т.р, тогда как 330i стоит 2 млн. 700 т.р. На автомобилях установлен один и тот же двигатель, но с разной мощностной прошивкой. Соответственно многие покупают модель 320i, изменяют программное обеспечение и получают как-бы модель 330i. Таким образом система безопасности автомобилей должна защищать автомобиль от таких изменений, так

как компания BMW будет нести убытки. Другой пример: дилер покупает автомобили BMW 320i, изменяет программное обеспечение и продает автомобиль дороже, обманывая тем самым конечного покупателя и компанию BMW. Следовательно, автомобиль должен быть защищен от таких переделок.

4. Обсуждение

В настоящее время тактика хакерских атак на автомобиль отработана. Поскольку подключение к внутренней сети осуществляется через стандартный разъем. Наиболее простым способом входа в систему управления является получение физического доступа к этому разъему. Второй вариант — получение доступа к части функций через различные беспроводные интерфейсы электронных блоков управления.

Для исследования программно-аппаратного окружения существует несколько подходов:

- извлечение отдельных электронных блоков управления из автомобиля и исследование их реакций на передаваемые по шине CAN команды;
- сканирование внутренней сети автомобиля через стандартный порт во время выполнения каких-либо действий (автомобиль при этом ставится на катки для исключения возможных аварийных ситуаций и получения данных во время работы в условиях, приближенных к реальным);
- исследование сети во время движения по дороге.

Современный стандарт связи электронных блоков автомобиля в сеть — шина CAN является достаточно слабым звеном в безопасности, поскольку данные, передаваемые по этой шине физически и логически доступны любому устройству, подключенному к этой сети. Шина CAN достаточно медленна и очень чувствительна к атакам типа «отказ в обслуживании».

Из-за того, что электронные блоки управления должны предоставлять возможности тестирования, считывания данных и обновления программного обеспечения по этой сети для обслуживающего персонала, шина CAN предоставляет богатые возможности для атаки на отдельные электронные компоненты автомобиля [1, 2].

Естественно, в протоколах обмена части устройств предусмотрены ключи доступа для вызывающей и отвечающей стороны, однако их длина составляет всего 16 бит. Согласно стандартам обмена, информацией по сети каждое устройство должно отвечать на запрос менее, чем за 10 секунд, что приводит к тому, что за максимум семь с половиной дней можно получить полный доступ к интересующему вас устройству. Для этого не обязательно быть постоянно подключенным к порту автомобиля — достаточно предоставить возможность для сбора информации одному из легко взламываемых электронных компонентов — скомпрометированный электронный блок управления сделает всю работу за вас.

5. Заключение

Современный автомобиль — высокотехнологичная машина, предоставляющая богатые возможности управления своими компонентами для обеспечения большей физической безопасности и комфорта. К сожалению, за эти возможности в настоящее время требуется платить снижением уровня информационной безопасности. Будем надеяться, что это просто «болезнь роста», и в будущем автомобили будут более защищены от хакеров.

Таким образом, можно сделать вывод о том, что современные автомобили должны быть надежно защищены не только от физических угроз, но и угроз информационной сферы.

6. Список используемой литературы

[1] Беспроводная связь и телематические системы в автомобиле: [Электронный ресурс]. URL: http://hpc.ru/lib/arts/1158/. (Дата обращения 23.11.2018).

[2] Информационная безопасность современного автомобиля: [Электронный ресурс]. URL: https://gblogs.cisco.com/ru/connectedcarssecurity/. (Дата обращения 19.11.2018).

6. List of references

[1] Wireless and telematics systems in the car: [Electronic resource]. URL: http://hpc.ru/lib/arts/1158/. (Accessed 23.11.2018).
[2] Information security of a modern car: [Electronic resource]. URL: https://gblogs.cisco.com/ru/connectedcarssecurity/. (Accessed 23.11.2018).

ВИРУСЫ-МАЙНЕРЫ - СПОСОБЫ ИХ ОБНАРУЖЕНИЯ И УДАЛЕНИЯ

Дёмин К.С[1]
diominkirill@yandex.ru

Выборнова О.Н[1]
кандидат технических наук
olga.vyb.90@gmail.com

[1] Астраханский Государственный Университет, Астрахань, 414056, Россия

Аннотация

Статья посвящена обзору способов обнаружения и удаления вирусов-майнеров. Речь идет о трех основных типах таких вирусов: web, простой и скрытый. Они различаются по способу проникновения и проявления своей активности. В статье рассказывается о вреде данного типа вирусов, о трудности их выявления и ликвидации. Представлены в виде скриншотов примеры подозрительной активности, вызванной заражением вирусом-майнером. Предложены и описаны три метода обнаружения и удаления вируса-майнера. Для каждого типа вируса описаны соответствующие алгоритмы обнаружения и лечения, обладающие большой степенью эффективности. Для web и простого вируса-майнера можно обойтись без дополнительного программного обеспечения, стандартных средств операционной системы будет достаточно для выявления и полной ликвидации данных типов вирусов. Для обнаружения и удаления скрытого майнера рекомендовано использование бесплатных программы, не требующих покупки лицензий. Разработана блок схема программы для автоматизации обнаружения и удаления вирусов-майнеров. Сделаны выводы о необходимости регулярной профилактики и защиты не только от вирусов майнеров, но

и от других угроз, способных навредить ресурсам компьютера.

Abstract

The article is devoted to the review of methods for detecting and removing miner viruses. This is about three main types of such viruses: web, simple and hidden. They differ in the method of penetration and manifestation of their activity. The article describes the dangers of this type of viruses, the difficulty of identifying and eliminating them. Presented in the form of screenshots examples of suspicious activity caused by infection with a miner virus. Three methods for detecting and removing a miner virus have been proposed and described. For each type of virus, the corresponding detection and treatment algorithms with a high degree of efficiency are described. For the web and a simple miner virus, you can do without additional software; standard operating system tools will be sufficient to identify and completely eliminate these types of viruses. To detect and remove the hidden miner, the use of free software that does not require a license purchase is recommended. A block diagram of the program is developed to automate the detection and removal of miner viruses. Conclusions are drawn about the need for regular prevention and protection not only against the miner viruses, but also against other threats that could harm computer resources.

Ключевые слова: информационные технологии, информационная безопасность, майнинг, вирусы, вирусы-майнеры, криптовалюта, веб майнинг, скрытый майнинг

Keywords: information technologies, information security, mining, viruses, viruses-miners, cryptocurrency, web-mining, hidden mining

1 Введение

С середины 2017 года криптовалюта обрела огромный спрос на рынке, цены некоторых из них были больше 20.000$. Начали появляться специальные вирусы-майнеры – скрытые программы, которые добывают криптовалюту, используя ресурсы компьютера «жертвы». По данным Skybox Security, за первую половину 2018 года 32% всех кибератак составляют крипто-майнеры [1]. При этом различается способ проникновения в систему и проявления их активности. Некоторые вирусы-майнеры внедряются в компьютер пользователя через пиратское программное обеспечение и игры; некоторые – размещаются злоумышленниками

на веб-страницы и используют для добычи криптовалюты вычислительные мощности посетителя [2, 3]. При этом, обнаружить вирусы-майнеры довольно сложно, обычный пользователь может не замечать, что его компьютер используется для добычи криптовалюты. Поэтому актуальна задача классификации и формирования методики обнаружения и нейтрализации данного типа вирусов.

Цель статьи – провести классификацию вирусов-майнеров, а также сформулировать рекомендации по их обнаружению и ликвидации.

2 Классификация вирусов-майнеров

Существует три наиболее распространённых вида вирусов-майнеров: web-майнер, простой, скрытый.

Web-майнер размещается на веб-странице или в установленном расширении браузера [4]. Его функционирование проявляется в замедлении работы компьютера во время серфинга по Интернету. По данным AdGuard из 100 тыс. вебсайтов 220 используют web-майнеры [5]. Web-майнер не скрывается, и его легко обнаружить и удалить.

Простой и скрытый вирусы-майнеры размещаются на компьютере пользователя-жертвы. Их функционирование проявляется в замедлении отклика компьютера даже на простые действия пользователя. При этом простой вирус может быть легко обнаружен и удален без применения постороннего программного обеспечения.

Скрытый вирус-майнер скрывается от мониторинговых систем, блокирует работу некоторых антивирусов, отключается, когда компьютер используется, что затрудняет его обнаружение в системе [6]. Кроме того, он создает множество копий, что не дает возможности удалить его обычным способом.

3 Методика обнаружения и удаления вирусов-майнеров

3.1. Обнаружение и удаления web-майнера

Для обнаружения потенциально опасных объектов при использовании Chrome, Opera или Yandex browser необходимо зайти в диспетчер задач браузера и проанализировать запущенные задачи и выполнить следующие действия:

1. Если обнаружено, что какое-то из расширений нагружает центральный процессор (ЦП) на максимум (рис.1), двойным щелчком мыши по названию расширения в диспетчере задач выполнить переход на страницу управления расширениями, где можно удалить данное расширение.
2. Затем перезапустить браузер, в результате чего вирус-майнер будет окончательно удален.
3. Если обнаружено, что веб-страница нагружает систему на максимум (рис. 2), то, с большой долей вероятности, на сайте был установлен скрипт по добыче криптовалюты. Предотвратить запуск скрипта майнера можно с использованием блокировщиков рекламы, таких как AdBlock, AdGuard и др. [7].

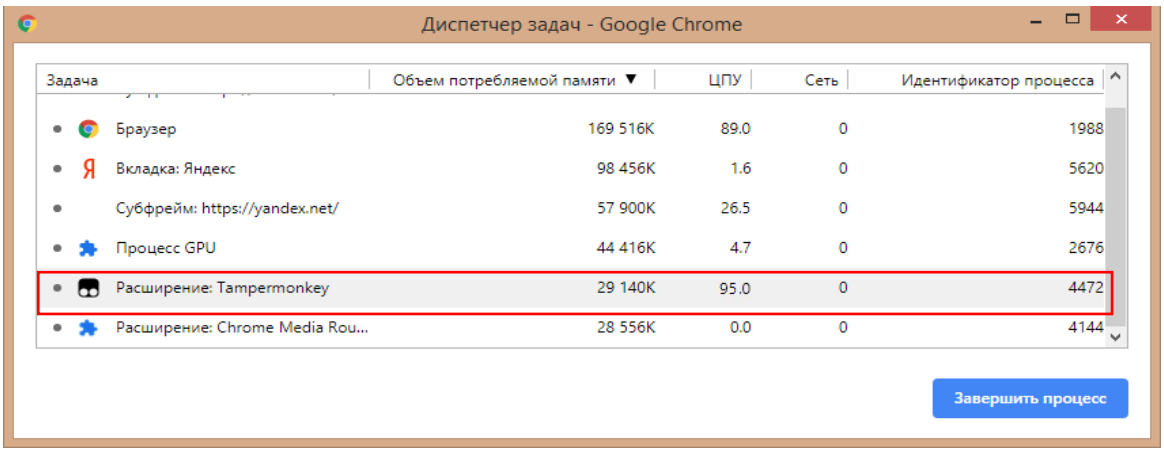

Рисунок 1. Нагрузка на ЦП за счет работы расширения браузера

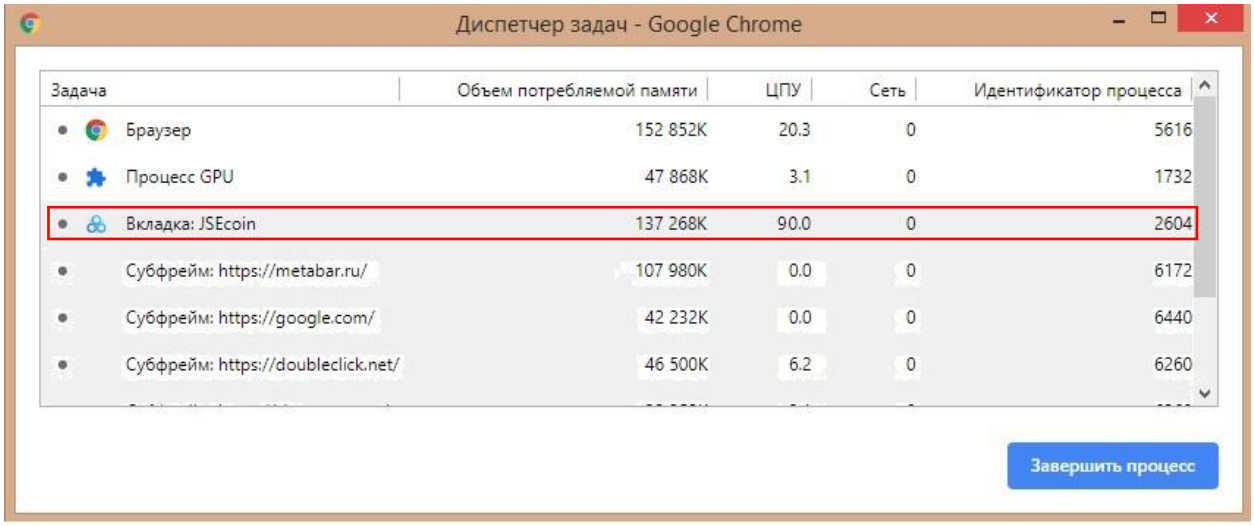

Рисунок 2. Нагрузка на ЦП за счет открытой вкладки браузера

В случае использования браузера, отличного от рассмотренных выше, необходимо:

1. Запустить диспетчер задач Windows или Мониторинг системы для Mac Os.
2. Закрыть все вкладки в браузере. Если загруженность центрального процессора упала, один из сайтов содержал скрипт по добыче криптовалюты. В этом случае для защиты от запуска скриптов по добыче криптовалюты следует использовать указанные выше блокировщики рекламы.
3. Если браузер продолжает нагружать центральный процессор после закрытия вкладок, то вирусом-майнером заражено какое-то из расширений. Для его обнаружения следует зайти во вкладку «Управление расширением» (для каждого браузера разный способ захождения в эту вкладку).
4. Отключить одно из расширений и перезапустить браузер. Если в результате браузер по показателям диспетчера задач перестал нагружать процессор, то данное расширение содержит в себе скрипт по добыче криптовалюты – цель обнаружена.

5. Если диспетчер задач все еще показывает загруженность центрального процесса от браузера, необходимо включить отключенное расширение и перейти к следующему. Повторять пункт 4 до тех пор, пока Диспетчер задач не покажет, что нагрузка на центральный процессор существенно снизилась.
6. Удалить расширение, отключение которого привело к снижению загруженности ЦП.

Описанный алгоритм может быть изображен в виде блок-схемы (рис. 3).

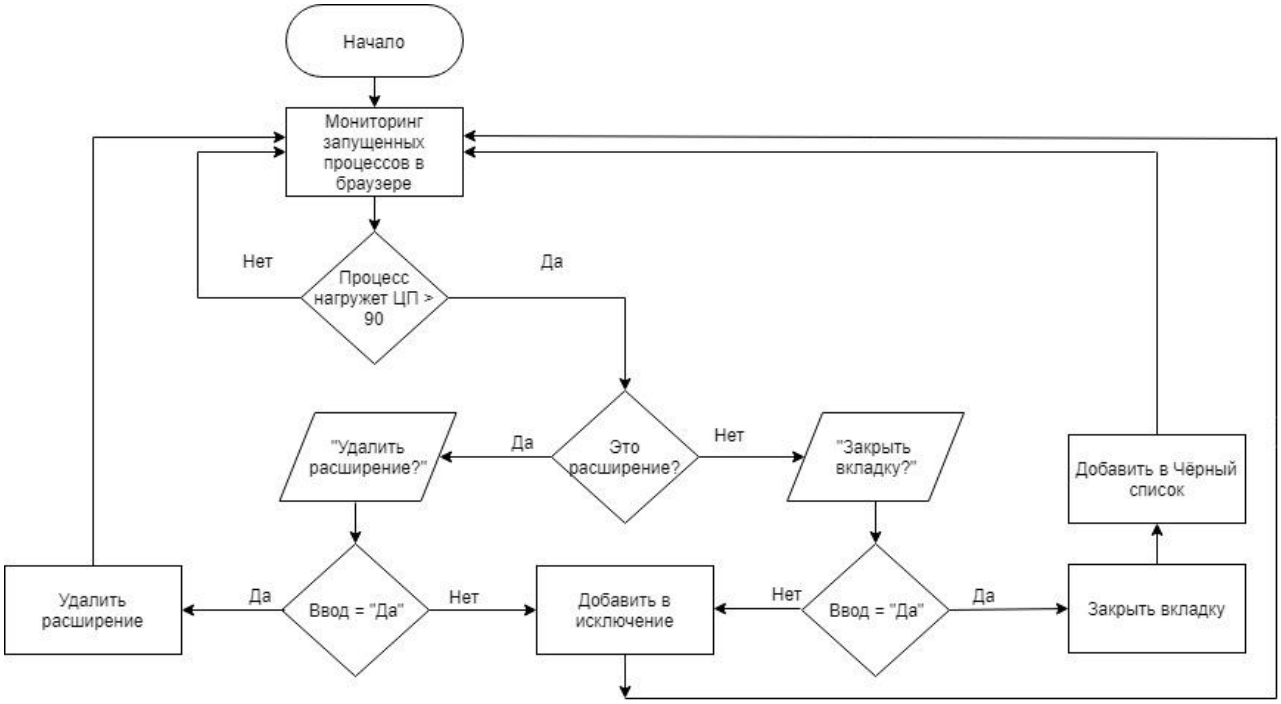

Рисунок 3. Блок-схема обнаружения и удаления web-майнера

3.2. Обнаружение и удаления простого вируса-майнера

Поскольку простой вирус-майнер почти не скрывается, его легко обнаружить, но иногда проблематично удалить. Если замечено существенное замедление работы компьютера и (или) браузер информирует о странной активности, исходящей с компьютера. Рекомендуется выполнить следующие действия, которые помогут обнаружить в системе простой вирус-майнер:

1. Откройте диспетчер задач, зайдите во вкладку «Процессы» и посмотрите, какой процесс больше всего нагружает систему. Часто вирусы-майнеры маскируются под процессы chrome.exe, helper.exe, svchost.exe (рис. 4).
2. Запишите название подозрительного процесса, который нагружает ЦП на максимум, кликните по нему правой кнопкой мыши и откройте «Расположение файла».
3. Если в папке, где располагается подозрительный процесс, не находится сторонних программ, удалите всю папку, если же есть нужная вам программа или файлы, удалите только тот файл, название которого совпадает с процессом.
4. Зайдите в редактор реестра во вкладку «Правка» → «Найти».

5. Введите название процесса и удалите все совпадения.
6. Просканируйте компьютер антивирусом или специальным сканером, таким как Dr. Web Cureit (распространяется бесплатно).
7. В случае обнаружения угроз, необходимо их удалить.

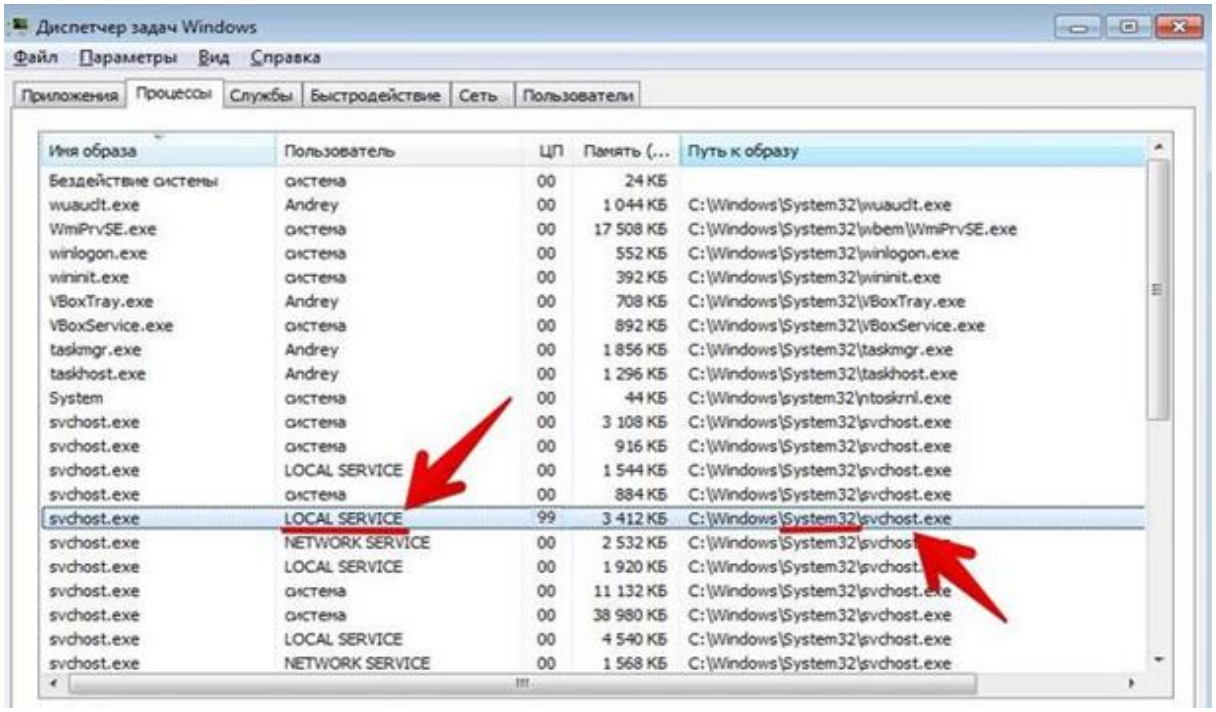

Рисунок 4. Маскировка вирусов-майнеров под легитимные процессы

Блок-схема описанного выше алгоритма приведена на рисунке 5.

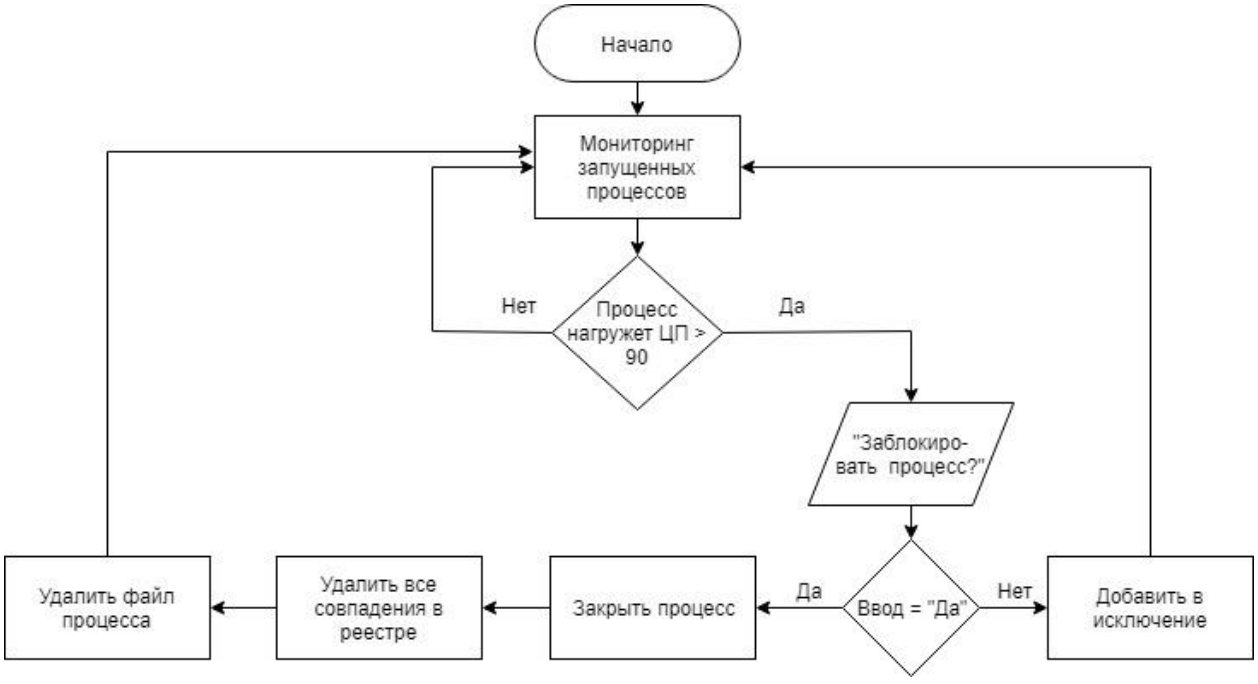

Рисунок 5. Блок-схема обнаружения и удаления простого вируса-майнера

3.3. Обнаружение и удаление скрытого вируса-майнера

Обнаружить скрытый майнер достаточно сложно. Диспетчер задач будет показывать, что компьютер не нагружается, потому что скрытый майнер закрывается при запуске «Диспетчера задач» и некоторых других популярных программ мониторинга системы. Также вирус-майнер может закрываться, когда запускаются программы, требующие много системных ресурсов, чтобы не вызывать замедление работы компьютера и тем самым не обнаружить себя. Новые версии вирусов-майнеров, способные инфицировать устройства под управлением ОС Linux, могут блокировать или полностью удалять работающие антивирусы, а также удалять другие, если такие имеются, скрытые манеры, скрывать файлы в файловой системе, сетевые соединения и запущенные процессы [8].

Если во время простоя компьютера громко работает кулер, или возрастает потребление электроэнергии, возможно компьютер заражен скрытым вирусом-майнером. Для его обнаружения понадобиться стороннее программное обеспечение, например, AnVir Task Manager или System Explorer [9].

1. Скачайте и установите одну из указанных утилит (они распространяются бесплатно).
2. Запустите программу и просмотрите запущенные процессы.
3. Если один из процессов несоизмеримо использует центральный процессор или вызывает подозрение процесс со странным названием (рис. 6), наведите курсор на приложение и правой кнопкой мыши кликните «Детальная информация» → «Производительность» для AnVir Task Manager или «Process Details» → «CPU Usage» для System Explorer.

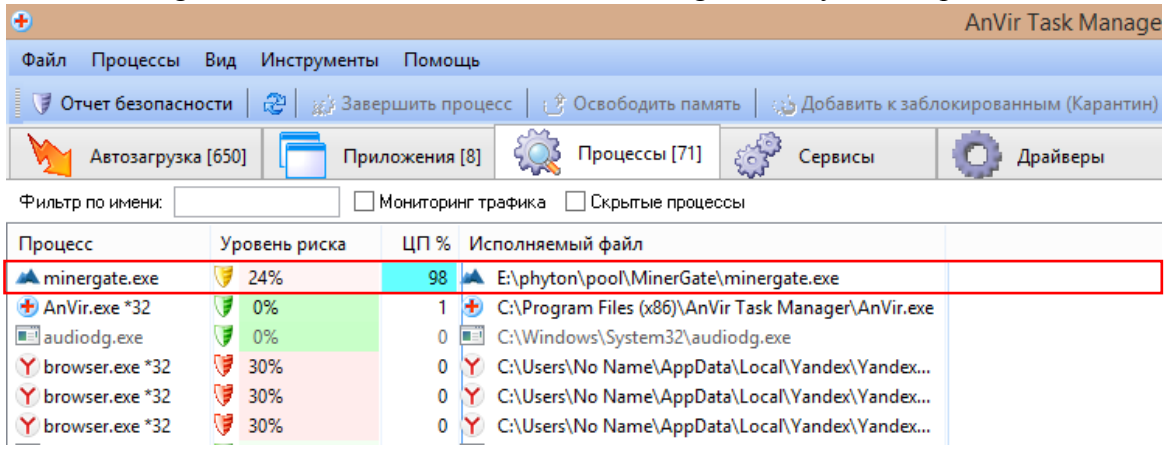

Рисунок 6. Подозрительный процесс

4. Просмотрите нагрузку на компьютер в течении ближайшего часа. Если процесс задействовал системные ресурсы на максимум, запишите его название.
5. Зайдите в редактор реестра во вкладку «Правка» → «Найти».
6. Введите название процесса и удалите все совпадения.
7. Просканируйте компьютер на вирусы с помощью антивируса или бесплатной утилиты Dr. Web Cureit, которая отлично обнаруживает скрытые майнеры.
8. Удалите найденные угрозы и перезагрузите компьютер.

4 Заключение

Вирусы-майнеры очень опасны для аппаратной части компьютера. Из-за повышенной нагрузки центральный процессор или видеокарта могут выйти из строя. Также ограничивается производительность компьютера пользователя. В связи с этим нужно проводить регулярное сканирование системы на вирусы, проявлять бдительность при открытии писем с подозрительными ссылками и вложениями, устанавливать только лицензионное программное обеспечение. Необходимо защищаться не только от вирусов-майнеров, но и от других похожих угроз, чтобы избежать поломки устройства, утерю информации или кражи паролей, номеров карт и т.д. [10].

В дальнейшем возможно проведение исследования вирусов-майнеров, которые влияют на другие системные ресурсы компьютера, рассмотрение более широкого спектра методов и средств обнаружения и нейтрализации данного типа угроз. Приведенные в статье алгоритмы могут быть положены в основу программы мониторинга, способной отслеживать чрезмерную загруженность системных ресурсов, информировать пользователя о подозрительной активности и предлагать пути решения данной проблемы.

Список используемой литературы

[1] Vulnerability and threat trends report 2018 mid-year update [Электронный ресурс]. — Режим доступа: https://lp.skyboxsecurity.com/WICD-2018-07-Report-VT-Trends-MY_03Asset.html, свободный

[2] Скрытый майнинг и ботнеты [Электронный ресурс]. — Режим доступа: https://www.kaspersky.ru/blog/hidden-miners-botnet-threat/18707/, свободный

[3] Cybercrime tactics and techniques: Q1 2018 [Электронный ресурс]. — Режим доступа: https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf, свободный

[4] Веб-майнинг [Электронный ресурс]. — Режим доступа: https://ru.m.bitcoinwiki.org/wiki/Веб_майнинг, свободный

[5] Cryptocurrency mining affects over 500 million people. And they have no idea it is happening [Электронный ресурс]: AdGuard Blog. 12 октября 2017. — Режим доступа: https://adguard.com/en/blog/crypto-mining-fever/, свободный

[6] CryptoMiner, WinstarNssmMiner, Has Made a Fortune By Brutally Hijacking Computers [Электронный ресурс]: Cyber Security News & Current Events | 360 Total Security Blog. 16 мая 2018. — Режим доступа: https://blog.360totalsecurity.com/en/cryptominer-winstarnssmminer-made-fortune-brutally-hijacking-computer/, свободный

[7] Как обнаружить веб-майнер с помощью Диспетчера задач Google Chrome [Электронный ресурс]. — Режим доступа: https://www.comss.ru/page.php?id=4839, свободный

[8] Новый троянец-майнер для Linux удаляет антивирусы [Электронный ресурс]: Новости компании «Доктор Веб» о вирусах. 20 ноября 2018 года. — Режим доступа:

https://news.drweb.ru/show/?i=12942&c=9&lng=ru&p=0&fbclid=IwAR3x2NGLD2gugDi_X0XUM59E5NebMGVIX4Dtshn8E75CYHe40KCgv1R0F7g, свободный
[9] Как найти скрытый майнер на ПК [Электронный ресурс]. — Режим доступа: https://geekon.media/kak-najti-skrytyj-majner-na-pk/?id=4839, свободный
[10] Демина Р.Ю., Ажмухамедов И.М. Методика формирования обучающего множества при использовании статических антивирусных методов эвристического анализа // Инженерный вестник Дона. 2015. № 3 (37) . С. 74.

List of references

[1] Vulnerability and threat trends report 2018 mid-year update [Electronic resource]. – Access mode: https://lp.skyboxsecurity.com/WICD-2018-07-Report-VT-Trends-MY_03Asset.html, free
[2] Hidden mining and botnets [Electronic resource]: Kaspersky Lab Blog. September 11, 2017. – Access mode: https://www.kaspersky.ru/blog/hidden-miners-botnet-threat/18707/, free
[3] Cybercrime tactics and techniques [Electronic resource]. – Access mode: https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf, free
[4] Web mining [Electronic resource]. – Access mode: https://ru.m.bitcoinwiki.org/wiki/Веб_майнинг, free
[5] Cryptocurrency mining affects over 500 million people. And they have no idea it is happening [Electronic resource]: AdGuard Blog. October 12, 2017. – Access mode: https://adguard.com/en/blog/crypto-mining-fever/, free
[6] CryptoMiner, WinstarNssmMiner, Has Made a Fortune By Brutally Hijacking [Electronic resource]: Cyber Security News & Current Events | 360 Total Security Blog. May 16, 2017. – Access mode:https://blog.360totalsecurity.com/en/cryptominer-winstarnssmminer-made-fortune-brutally-hijacking-computer/, free
[7] How to detect web miner using Google Chrome Task Manager [Electronic resource]. – Access mode: https://www.comss.ru/page.php?id=4839, free
[8] A new miner Trojan for Linux removes antiviruses [Electronic resource]: Doctor Web news about viruses. November 20, 2018. – Access mode: https://news.drweb.ru/show/?i=12942&c=9&lng=ru&p=0&fbclid=IwAR3x2NGLD2gugDi_X0XUM59E5NebMGVIX4Dtshn8E75CYHe40KCgv1R0F7g, free
[9] How to find hidden miner on PC [Electronic resource]. – Access mode: https://geekon.media/kak-najti-skrytyj-majner-na-pk/?id=4839, free
[10] Demina R.Ju. , Azhmuhamedov I.M. Formation technique of the training set using static heuristic analisis // Inženernyj vestnik Dona. 2015. № 3 (37). P. 74.

БИОМЕТРИЧЕСКОЕ РАСПОЗНАВАНИЕ ГОЛОСА В СИСТЕМЕ БЕЗОПАСНОСТИ

Карабанова А.Н.[1] 09.nastya.97@mail.ru
Минкина Т.В.[1] n.min@mail.ru
Брехов М.А.[1] brekhov1988@mail.ru
Букреев А.В.[1] artem.bukreev.95@mail.ru

Орёл Д.В.[1]
kde.def@gmail.com

[1] СКФУ, город Ставрополь, 355000, РФ

Аннотация

В статье представлена система распознавания речи, предназначенная для идентификации речи пользователя. При помощи программного обеспечения для кодирования и распознавания речи, созданного в среде MATLAB, может быть распознана речь пользователя. Речевая форма сигнала преобразуется с помощью ключа в параметрический тип представления для дальнейшего анализа и обработки. Существует широкий диапазон возможностей параметрического представления речевого сигнала для системы распознавания голоса, к примеру, Мел-частотные кепстральные коэффициенты. Голосовой сигнал на входе записывается, затем компьютер сравнивает полученный сигнал с сигналом, хранящимся в базе данных. Данная голосовая биометрическая система основана на распознавании одного слова. Пользователь произносит пароль однажды во время обучения, чтобы сохранить его. Во время тестирования пользователь может произнести пароль повторно для того, чтобы проверить его на соответствие. При помощи симулятора в среде MATLAB получаются следующие выходные данные: пользователь либо распознаётся, либо отклоняется.

Abstract

A voice recognition system is designed to identify an administrator voice. By using MATLAB software for coding the voice recognition, the administrator voice can be authenticated. The key is to convert the speech waveform to a type of parametric representation for further analysis and processing. A wide range of possibilities exist for parametrically representing the speech signal for the voice recognition system such as Mel-Frequency Cepstrum Coefficients (MFCC). The input voice signal is recorded and computer will compare the signal with the signal that is stored in the database by using MFCC method. The voice based biometric system is based on single word recognition. An administrator utters the password once in the training session so as to train and stored. In testing session the users can utter the password again in order to achieve recognition if there is a match. By using MATLAB simulation, the output can obtain either the user is being recognized or rejected. From the result of testing the system, it successfully recognizes the specific user's voice and rejected other users' voice. In conclusion, the accuracy of the whole system is successfully recognizing the user's voice. It is a medium range of the security level system.

Ключевые слова: Голосовой сигнал, система распознавания голоса, пользователь, динамическое изменение времени, векторное квантование, Мел-частотные кепстральные коэффициенты, быстрое преобразование Фурье, окно Хемминга, Matlab.

Keywords: Voice signal, voice recognition system, user, dynamic time change, vector quantization, Chalk-frequency cepstral coefficients, fast Fourier transform, Hamming window, Matlab.

1 Введение

В нашем мире все чаще проявляется интерес к технологиям идентификации человеческого голоса. С одной стороны, это объясняется реализацией высокопроизводительных систем, которые могут считать сложные сигналы, к примеру, голоса.

Методы распознавания личности по голосу есть с тех пор, как человек научился говорить. Голос создается из комбинаций поведенческих и физиологических факторов. На сегодня идентификация по голосу реализована для управление доступом в помещения, где объективная оценка степени безопасности не критическая.

Распознавание голоса может использоваться как в системах управления доступом в помещения, так и в системах удалённой аутентификации по каналам связи. Существует

достаточно много способов построения кода идентификации по голосу, как правило, это различные сочетания частотных и статистических характеристик голоса. В последние годы особую актуальность приобретает аутентификация клиентов финансовых учреждений при их обращении по телефону на линию поддержки. Данный вид биометрии основан на анализе характеристик голоса: громкости, скорости, манере речи и др. Помимо знания кодового слова сотрудниками проверяется и принадлежность голоса клиенту. Система распознавания должна установить, принадлежит ли речевой сигнал голосу одного из клиентов.

2 Постановка задачи

В настоящее время многие общественные организации и коммерческие компании используют все виды систем безопасности, чтобы обеспечить свою защиту. К примеру, используются такие идентификаторы как ID пользователя / PIN-код. К сожалению, все эти системы безопасности по сути не защищены, потому что PIN-код можно взломать, ID-карту можно украсть или же сделать копию [9].

В качестве пароля используется биометрическая технология, которая использует параметры так называемых пользовательских особенностей. Эти параметры являются уникальными для каждого пользователя, даже если пользователи – близнецы. Таким образом, система распознавания голоса является вполне безопасной для пользователя. Речь является самым распространённым способом общения между людьми. Целью данной статьи является разработка программы распознавания голоса для идентификации пользователя по определенному произносимому слову [2].

Голосовая биометрическая технология для аутентификации пользователя более удобна и точна, чем многие другие методы. Ведь ничего не нужно помнить и не пугаться, если украдена ID-карта или взломан пароль.

С технологической точки зрения различают два широких типа автоматического распознавания голоса ASR (Automated Speech Recognition): прямой голосовой ввод (DVI) и непрерывное распознавание речи (LVCSR). Эти системы анализируют конкретный голос пользователей и используют его для точной настройки распознавания речи этого пользователя, что приведет к более точной транскрипции [3].

Система распознавания голоса содержит два основных модуля-извлечение признаков и сопоставление признаков. Речевой сигнал и его характеристики могут быть представлены в двух различных областях: временной и частотной [6].

Скрытая марковская модель (HMM) является одним из текстовых зависимых методов. Сначала голос пользователя записывается с помощью микрофона в файл .wav. Затем сигнал поступает в преобразователь A2D, который преобразует аналоговый сигнал в цифровой. Каждое произнесение преобразуется в домен Cepstrum на этапе обучения. Затем из данного домена получают параметры голоса пользователя, которые в последствии сравниваются с эталонным образцом на предмет соответствия. Далее принимается решение: либо голос принимается (если голос соответствует эталонному образцу), либо отклоняется.

Другим методом распознавания голоса является система классификаторов Fusion (слияния), которая использует минимальное количество входных данных для правильного решения. Голос аутентифицированного пользователя выступает в качестве входных данных и будет принят за *x*. В качестве особенностей используются коэффициенты перцептивного линейного предсказания (PLP). Модель S устанавливается как аутентифицированный пользователь. Голос записывается, и параметр функции извлекается с использованием трех разных алгоритмов: обобщенный метод моментов (GMM), метод наиболее благоприятного события (MFN) и метод опорных векторов (SVM). Это три разных алгоритма, используемые для вычисления совпадений между каждым аутентифицированным пользователем. Каждый разный классификатор отображает различные параметры функции пользователя и комбинирует все баллы соответствия, чтобы принять решение о том, принят или отклонен пользователь. Система определяется с помощью ложной скорости приёма (FAR) и ложной скорости отклонения (FRR) [1].

Система распознавания голоса реализована с помощью программы MATLAB (SIMULINK). Для сравнения с пользователем, прошедшим проверку голоса, используется «речевой шаблон». Чтобы распознать голос пользователя, выводится несколько переменных, таких как шаг, динамика и форма волны. Входной голос пользователя будет использоваться для сравнения с речевым шаблоном. Внутри диапазона уровня безопасности появляется логическая «1», в противном случае - логическое «0».

Другим методом, таким как алгоритм динамического временного деформирования (DTW), является измерение сходства между двумя временными рядами, которые могут меняться во времени или скорости. Функция DTW состоит в том, чтобы сравнить два динамических шаблона и измерить его сходство, вычислив минимальное расстояние между пользователями [4].

Два временных ряда Q и C, длины n и m соответственно представлены в уравнениях 1и 2

$$Q = q_1, q_2, \dots, q_i, \dots, q_n \tag{1}$$

$$C = c_1, c_2, \dots, c_j, \dots, c_m \tag{2}$$

Строка n-by-m, в которой элемент матрицы содержит расстояние d между двумя точками qi и cj. Расстояние вычисляется с использованием вычисления евклидовых расстояний в уравнении 3

$$d(q_i, c_j) = (q_i - c_j) \tag{3}$$

Накопленное расстояние рассчитывается с использованием уравнения 4

$$D(i,j) = \min[D(i-1, j-1), D(i-1, j), D(i, j-1)] + d(i,j) \tag{4}$$

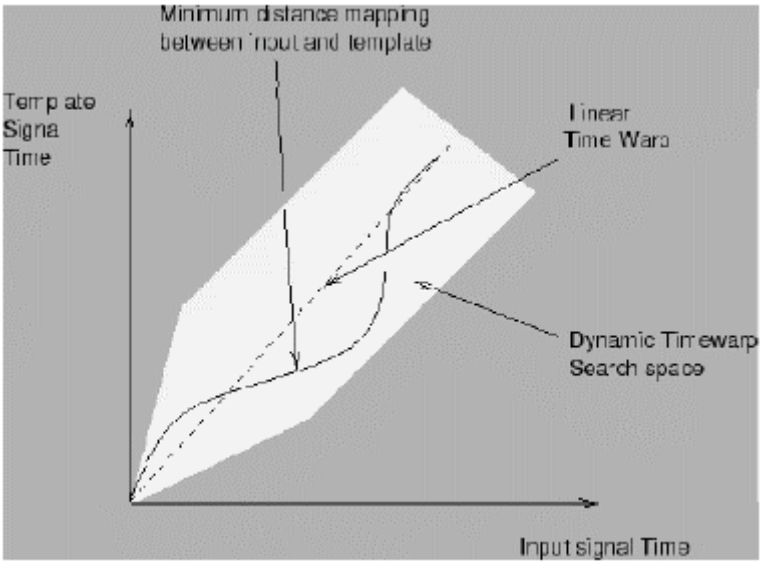

Рисунок 1. Динамическое изменение времени

Метод, который применяется в системе распознавания голоса, представляет собой модель гауссовой смеси (GMM). GMM распознает ключевое слово и делится на два шага, которые изолируют речь от записи произнесения и моделируют статистическое распределение характеристик произнесения статистическим способом. Модель пользователя рассчитывается на этапе обучения и сохраняется в базе данных.

Последний метод в этой статье - векторное квантование (VQ). VQ - процесс отображения векторов из большого векторного пространства в конечное число областей в этом пространстве. Каждая такая область называется кластером. На этапе обучения каждый говорящий будет иметь специальную кодовую книгу VQ. Результатом расстояния от вектора до ближайшего кодового слова называется VQ-искажение. С помощью кодовой книги можно определить идентифицировать говорящего с наименьшими полными искажениями. На рисунке 2 показан пример формирования кодовой книги векторного квантования.

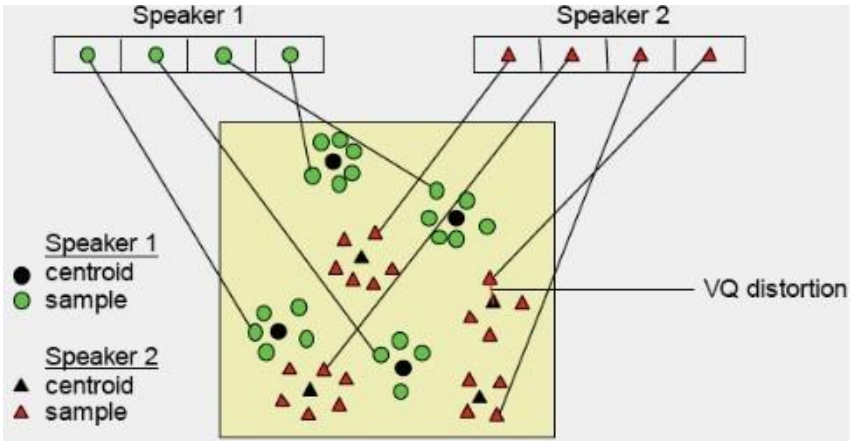

Рисунок 2. Векторное квантование информации в кодовой книге

3 Разработка методики

В этом проекте будут использоваться такое ПО как MATLAB и ARDUINO. Программное обеспечение MATLAB используется для части распознавания голоса, в то время как программное обеспечение ARDUINO фокусируется на части системы связи, например, управляет светодиодным индикатором, ЖК-дисплеем и включением / выключением магнита двери. Во время фазы обучения входной голос от микрофона будет извлечен из фактической произнесенной речи, тишина или отсутствие голоса будет отсеяна. Используя MFCC, энергетическая особенность пользователя извлекается и сохраняется в качестве эталонного шаблона. Голосовой входной сигнал с этапа тестирования будет проверяться, совпадает ли он с эталонным шаблоном или нет, а затем вычисляет его результат. Если результат находится в диапазоне с хранимым шаблоном, тогда голос принимается, в противном случае отвергается [10].

Распознавание голоса делится на две фазы, которые являются фазой тренировки и фазой тестирования [4].

Если результат отклонен, система отобразит «Вы не тот же пользователь», если результат будет принят, система отобразит «Вы тот же пользователь». На рисунке 3 показана произнесенная речь слова «Алло». Данное слово очень часто употребляется при телефонных переговорах.

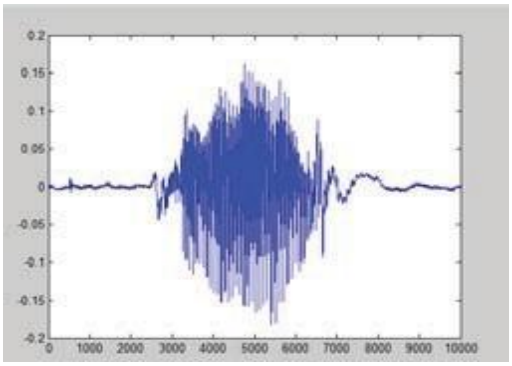

Рисунок 3. Произнесенная речь «Алло»

Выделение функций - это процесс, который извлекает небольшой объем данных из входного речевого сигнала для представления пользователя. Этот модуль преобразует речевой сигнал в некоторый тип параметрического представления для дальнейшего анализа и обработки, используется метод MFCC для расчета коэффициентов. На рисунке 4 приведена блок-схема подхода MFCC к упомянутым вариантам [7].

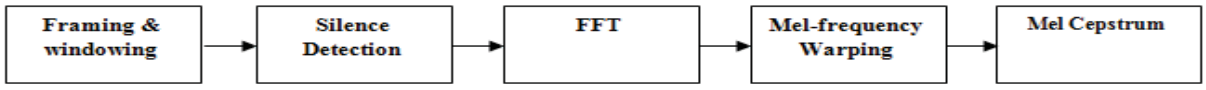

Рисунок 4. Подход MFCC

Более подробно методика обработки голоса представлена в статье Biometric Voice Recognition in Security System [11].

4 Результаты

В данном разделе приводятся два эксперимента для анализа эффективности системы распознавания голоса. Один из экспериментов - это проверка точности собственного голоса, в то время как другой эксперимент проверяет точность голоса других людей, когда голос задан в качестве эталонного шаблона.

Во время произнесенной речи говорящего, его голос будет генерировать сигнал. На рисунке 5 показано слово «Алло», произнесенное пользователем с микрофона.

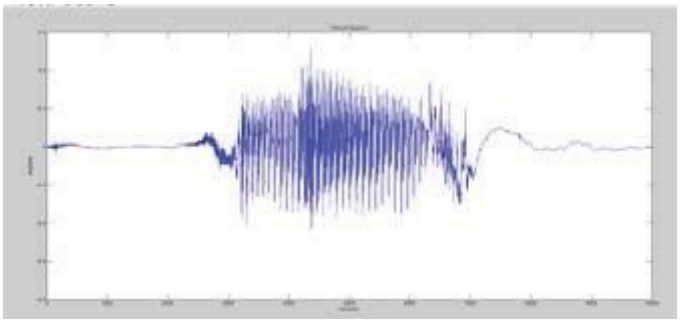

Рисунок 5. Слово «Алло» в качестве голосового входного сигнала

Входной речевой сигнал записывается как 1 секунда, тогда обнаружение тишины будет извлекать только произнесенную речь и игнорировать шумовой сигнал. На рисунке 6 показано слово «Алло» после того, как произошло обнаружение тишины, а шумовой сигнал игнорируется.

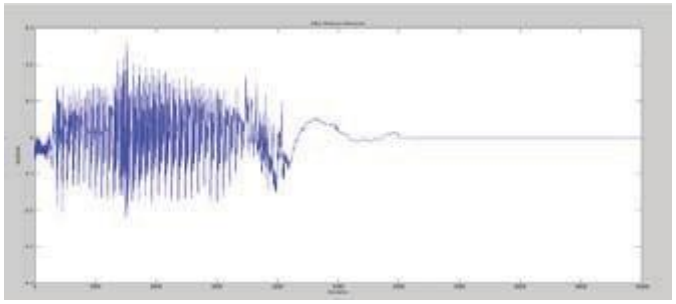

Рисунок 6. Слово «Алло» после обнаружения молчания

После того, как фактический речевой сигнал извлекается отсечением тишины, окно Хэмминга используется для сглаживания входного речевого сигнала. На рисунке 7 показано слово «Алло» после более гладкого окна Хэмминга.

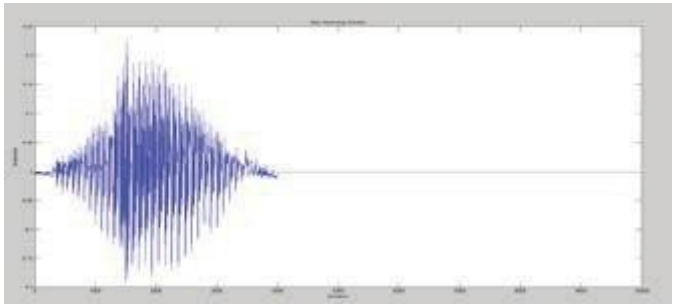

Рисунок 7. Слово «Алло» после использования окна Хэмминга

После более плавного ввода входного речевого сигнала сигнал находится во временной области. Быстрое преобразование Фурье (FFT) изменяет входной речевой сигнал от временной области до частотной области. На рисунке 8 показано слово «Алло» на частотной области.

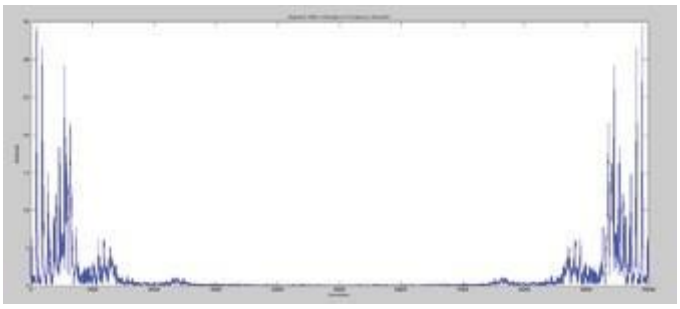

Рисунок 8. Слово «Алло» после FFT

Изменяя от временной области к частотной области, входной речевой сигнал затем вычисляем энергию, используя формулу. Определяем перекрывающееся окно треугольника и энергию в каждом окне. На рисунке 9 показано слово «Алло» после Мел-деформировании.

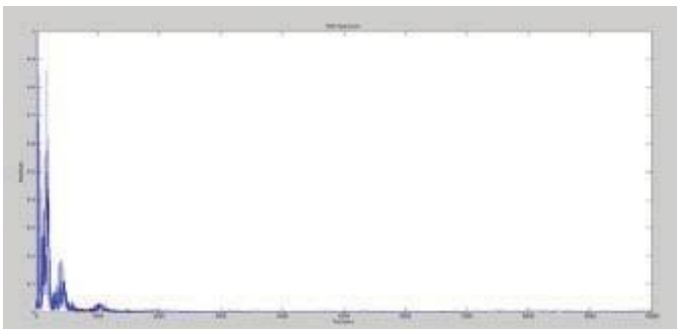

Рисунок 9. Слово «Алло» после Мел-деформирования

5 Обсуждение

Повторяя эксперимент с распознанным голосом администратора 20 раз, в 5-й раз он не смог распознать его голос. Таким образом, наше исследование доказывает 75%-ую точность этой системы распознавания голоса.

Неспособность системы распознать голос аутентифицированного пользователя объясняется изменчивостью энергии речи, произнесенной оратором. Среди 10 человек разного пола и возраста система распознавания голоса может распознать голос зарегистрированного пользователя. Разница между полом и разница в возрастах пользователей помогает осуществить проверку системы на точность распознавания голоса. Несомненно, было бы лучше повысить точность проверки голоса [8].

Неотъемлемым является тот факт, что системы распознавания голоса обладают довольно высоким потенциалом для дальнейшего снижения ошибок распознавания за счет применения все более длинных речевых сообщений, так как в этих сообщениях проявляется индивидуальность акустических характеристик голоса. Аутентификацией по голосу, используемой в системах безопасности, можно воспользоваться и в темноте, и на расстоянии (телефонный канал), т.е. в условиях, когда невозможно получить изображение. Такие системы применяются как в криминалистике, в частности это фоноскопическая экспертиза, так и в различных системах безопасности и управления доступом.

6 Заключение

Система на основе алгоритма распознавания голоса с использованием метода MFCC успешно распознает голос аутентифицированного пользователя и отвергает все остальные голоса. Результат делится на две категории, которые принимаются и отклоняются. Если результат в принятии, то Arduino активирует магнит на двери, чтобы её разблокировать. Если результат в отклонении, то Arduino оставляет дверь заблокированной, и сигнализация будет активирована в течении 1 секунды. Следовательно, в системах аутентификации для борьбы с подделкой голоса путём воспроизведения ранее записанных фраз целесообразно предлагать авторизующемуся лицу произнести определенное слово или фразу. В случае, если произнесенное человеком не соответствует требуемой фразе, отказывать в доступе.

7 Список используемой литературы

[1] Актуальность применения глубокого обучения в современном мире. Хныкина А.Г., Минкина Т.В. В сборнике: Экономические и социальные проблемы регионов в условиях развития информационного общества Сборник материалов Международной научно-практической конференции. 2017. С. 216-219.

[2] Разработка модульного алгоритма информационной системы распознавания лиц для интеллектуальных сред. Шлаев Д.В., Гайчук Д.В., Резенков Д.Н., Минкина Т.В., Дуракова А.С. Исследовательский журнал фармацевтических, биологических и химических наук. 2016. Т. 7. № 6. С. 2299-2302.

[3] Распознавание изображений сверточной нейронной сетью второго порядка с динамическими рецептивными полями. Немков Р., Мезенцева О., Мезенцев Д., Бродников М. В сборнике: Семинар-практикум CEUR 2. Сер. «YSIP2 2017 - Материалы 2-го Международного семинара молодых ученых по тенденциям в области обработки информации». 2017. С. 147-151.

[4] Распознавания речи с помощью алгоритма динамического трансформирования времени. Халимбеков М.А., Колесниченко А.А., Мезенцева О.С. В сборнике: Студенческая наука для развития информационного общества сборник материалов IV Всероссийской научно-технической конференции: в 2-х томах. 2016. С. 235-237.

[5] Разработка системы голосового управления робототехничекими системами. Бадалов Б.М., Ганьшин К.Ю., Попова Н.В., Мезенцева О.С. В сборнике: Студенческая наука для развития информационного общества Сборник материалов V Всероссийской научно-технической конференции. . 2016. С. 563-567.

[6] Методика оценки технической защищённости речевой информации в выделенных помещениях. Сагдеев К.М., Петренко, В.И. Известия ЮФУ. Технические науки. 2012. № 12 (137). С. 121-129

[7] Два подхода к реализации фрактального анализа временных серий. Тебуева Ф.Б. Труды СПбГТУ. 2007. Т. 4. № 2. С. 105.

[8] Исследование уязвимостей информационной безопасности банковских структур РФ. Орёл Д.В., Ивакина Д.А. В сборнике: Студенческая наука для развития информационного общества. Сборник материалов III Всероссийской научно-технической конференции. 2015. С. 52-54.

[9] Анализ компонентов биометрической системы идентификации по трёхмерным моделям лиц. Кузьменко В.В., Орёл Д.В. В сборнике: Студенческая наука для развития информационного общества сборник материалов IV Всероссийской научно-технической конференции: в 2-х томах. 2016. С. 142-144.

[10] Развитие и совершенствование учебно-материальной базы института информационных технологий и телекоммуникаций СКФУ: состояние и перспективы. Чипига А.Ф., Петренко В.И. Информационное противодействие угрозам терроризма. 2015. № 25. С. 408-412.

[11] Mohd Fairus Abdollah, Mohd Fairus Abdollah. Biometric Voice Recognition in Security System. Indian Journal of Science and Technology 7(2):104-112. February 2014.

ПРИМЕНЕНИЕ МЕТОДИКИ ПРОГНОЗИРОВАНИЯ НА ОСНОВЕ ПОЛИНОМИАЛЬНЫХ ТРЕНДОВ ДЛЯ АНАЛИЗА КИБЕРАКТИВНОСТИ В РФ

Заволокина У. В.[1]
zzeseftt@yandex.ru

Унтевский Н.Ю.[1]
untewsky@yandex.ru

Гурчинский М. М.[1]
Gurcmikhail@yandex.ru

Пижевский Д. Е.[1]
Dimapizhevskii@mail.ru

Петренко В.И.[1]
Кандидат технических наук, доцент
vip.petrenko@gmail.com

[1] Северо-Кавказский федеральный университет, Ставрополь, 355009, Российская Федерация

Аннотация

Данная статья посвящена прогнозированию киберативности в РФ для проведения анализа угроз информационной безопасности. Актуальность заключается в необходимости анализа и прогнозирования угроз и рисков в области информационной безопасности при разработке защитной стратегии. В статье приведены основные виды киберугроз. Целью работы является выявление наиболее быстроразвивающихся угроз на основе расчета коэффициентов ускорения изменения количества атак за определенный период. Для этого была применена методика прогнозирования киберативности в РФ на основе построения полиномиальных трендов третьей степени и расчета коэффициента ускорения изменения количества атак за период. Исходными данными методики являются статистические данные за ноябрь 2018 г., представленные на сайте «Лаборатории Касперского». По итогам проведённого анализа результатов применения методики были выявлены наиболее возможные быстроразвивающиеся угрозы на первые числа декабря. Практическая значимость работы заключается в возможности использования предложенной методики при долгосрочном прогнозировании.

Abstract

This article is devoted to predicting cyber activity in the Russian Federation for analyzing information security threats. The urgency lies in the need to analyze and predict threats and risks in the field of information security when developing a defensive strategy. The article presents the main types of cyber threats. The aim of the work is to identify the most rapidly developing threats based on the calculation of the coefficients of acceleration of changes in the number of attacks for a certain period. For this purpose, a method for predicting cyber activity in the Russian Federation was used based on the construction of polynomial trends of the third degree, and the calculation of the acceleration coefficient for changes in the number of attacks over a period. The baseline data of the methodology is statistical data for November 2018, presented on the Kaspersky Lab website. According to the results of the analysis of the results of the application of the methodology, the most likely high-growth threats were identified as of the first days of December. The practical significance of the work lies in the possibility of using the proposed methodology for long-term forecasting.

Ключевые слова: прогнозирование киберугроз, статистика киберугроз в РФ, заражения, сетевые угрозы, спам, веб-атаки, уязвимости.

Keywords: cyber threat forecasting, cyber threat statistics in the Russian Federation, infections, network threats, spam, web attacks, vulnerabilities.

1. Введение

Обнаружение угроз и борьба с ними невозможна без постоянного анализа состояния устройств миллионов пользователей по всему миру. Обеспечение безопасности строится исходя из понимания угроз и рисков, а также из соблюдения правил безопасности [1].

Когда речь заходит о разработке защитной кибер-стратегии, использование мощного статистического инструмента является одним из самых эффективных методов. Анализ векторов атак, которые используются злоумышленниками, и изучение вредоносных программ, проникающих в информационную систему в случае успешного исхода атаки, позволяет прогнозировать, чем все это может обернуться для владельцев устройств.

Целью статьи является выявление наиболее быстроразвивающихся угроз на основе расчета коэффициентов ускорения изменения количества атак за определенный период.

2. Постановка задачи

Задачей данной статьи является применение методики прогнозирования киберактивности в РФ на основе построения полиномиальных трендов третьей степени и расчета коэффициента ускорения изменения количества атак за период. Исходными данными методики являются статистические данные за ноябрь 2018 г., представленные на сайте «Лаборатории Касперского» [2].

Основным объектом изучения является карта киберугроз, которая разрабатывается и поддерживается «Лабораторией Касперского» и позволяет в режиме реального времени получать актуальную статистику об информационных угрозах в различных регионах мира. Статистические данные представлены в виде временного ряда. Источником данных для этой карты является информация от различных компонентов защитных решений «Лаборатории Касперского», установленных на ПК клиентов компании.

В данной статье рассматривается статистика за ноябрь 2018 года. Используемый ресурс предлагает статистику, собранную почти по всему миру, однако в данной статье рассмотрена ситуация в нашей стране.

3. Виды вредоносной активности

Статистика ведется по следующим видам вредоносной активности:

– заражения, которые представляют собой процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.);

– веб-угрозы, под которыми понимаются разнообразные угрозы, поступающие из сети Интернет;

– сетевые атаки – действия, целью которых является обретение контроля над локальной вычислительной системой, либо отказ в обслуживании, а также получение личных данных пользователей этой вычислительной системы;

– уязвимости информационной системы ― это любой недостаток информационной системы, который в своих целях может использовать злоумышленник; как правило, уязвимости создаются разработчиками в процессе производства, администраторами в процессе управления компонентами системы, пользователями в процессе эксплуатации системы;

– спам – массовая рассылка сообщений обычно рекламного характера лицам, не желающим её получать;

– заражённая почта: заражение почтовым вирусом является следствием необдуманных действий пользователей, просматривающих почту, а также возникает из-за ошибок в почтовых сервисах [3].

4. Методика прогнозирования киберактивности в РФ

4.1. Разработка методики

Для достижения поставленной цели и задачи исследования будет применена методика прогнозирования временных рядов на основе полиномиальных трендов третьей степени. Рассмотрим поэтапно применяемую методику.

На первом этапе необходимо отобразить временной ряд количества атак, исходя из статистических данных, представленных на сайте «Лаборатории Касперского».

Второй этап заключается в следующих действиях:

– построение полиномиального тренда третьей степени, т.е. создание приближенной функции, основанное на замене экспериментально полученных данных аналитической функцией, наиболее близко проходящей или совпадающей в узловых точках с исходными значениями;

– построение на его основе пятидневного прогноза количества атак.

Для прогнозирования был выбран период в 5 дней по причине того, что при имеющейся небольшой выборке статистических данных более долгосрочные прогнозы имеют плохую сходимость и большую погрешность [4].

В ходе работы на первых двух этапах будет использована программа Microsoft Office Excel, в которой реализован требуемый инструментарий для проведения расчетов по реализуемой методике.

На третьем этапе производится расчет коэффициентов ускорения изменения количества атак, который является третьей производной от уравнения полиномиального тренда третьей степени, что является физическим смыслом третьей производной, отображающей скорость изменения ускорения [5]. Далее рассчитывается увеличение атак в день в начале декабря по сравнению со средним значением атак в день за прошлый месяц.

Для функции, имеющей вид

$$f(x) = a \cdot x^3 + b \cdot x^2 + c \cdot x + d,$$

где a, b, c — коэффициенты переменной, расчет третьей производной осуществляется по формуле:

$$f'''(x) = 6 \cdot a. \quad (1)$$

Процентное увеличение атак в день p производится по формуле:

$$p = \frac{k}{0.01 \cdot a}, \quad (2)$$

где k — это коэффициент ускорения изменения количества атак, а — среднее арифметическое значение количества атак в день за месяц.

На четвертом этапе необходимо провести анализ прогнозных значений количества атак в день в рассматриваемый период. Для этого выполняется поиск среднего арифметического значения представленного временного ряда и расчет увеличения атак в день по сравнению со средним значением за прошлый временной период [6].

4.2. Реализация методики

Этап I-II. Временной ряд заражений, произошедших в России в период с 1 по 30 ноября, представлен на рис.1.

Рисунок 1. Временной ряд заражений

Прогнозирование показывает, что ближайшее время количество заражений в день ожидает незначительное увеличение.

Временной ряд произошедших за месяц веб-угроз представлен на рис.2.

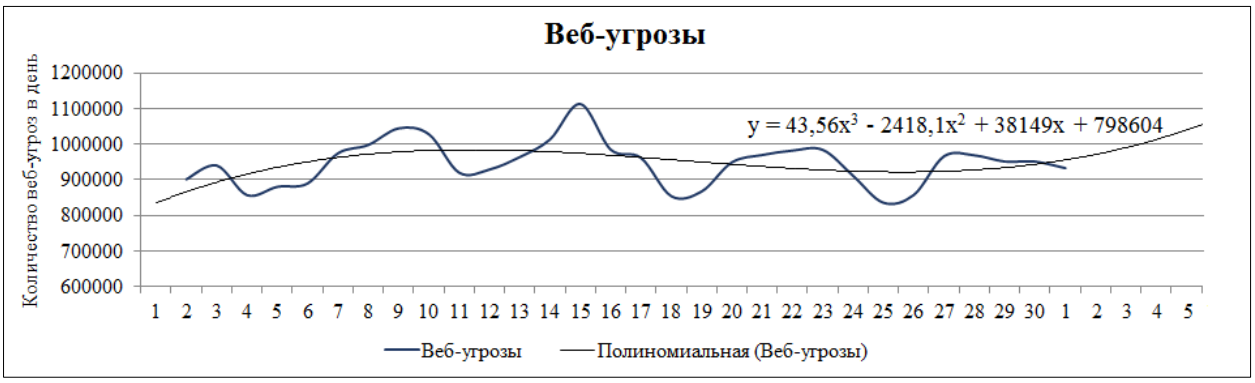

Рисунок 2. Временной ряд веб-угроз

Прогнозирование дальнейшего развития этого вида вредоносной деятельности так же показывает возможный рост количества веб-угроз 1-5 декабря.

Временной ряд, построенный на основе статистики сетевых атак в прошедшем месяце, показан на рис.3.

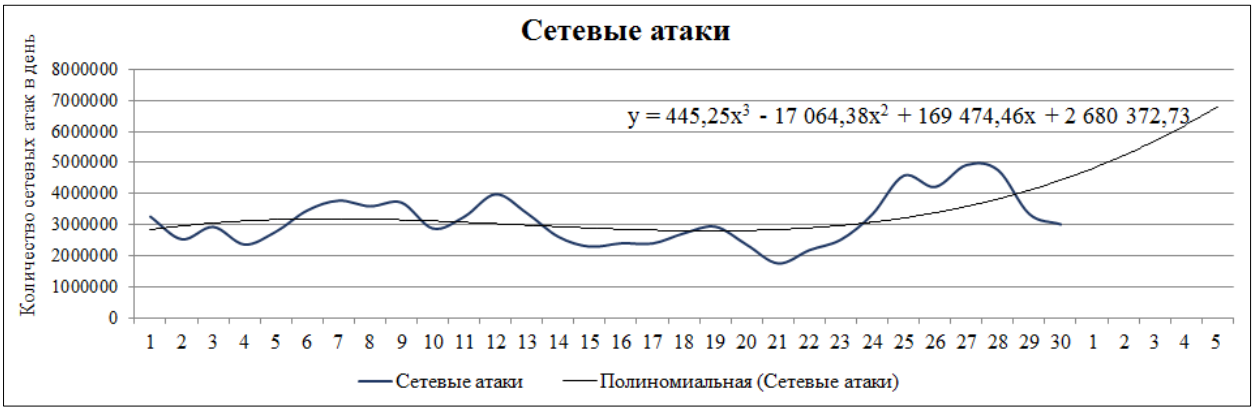

Рисунок 3. Временной ряд сетевых атак

Прогнозы на основании данного графика неутешительны: показатели количества сетевых атак в день в начале декабря будут выше, чем в какой-либо из дней ноября.

Временной ряд, отображающий закономерности выявлений уязвимостей информационных систем в течение месяца, имеет вид, представленный на рис.4.

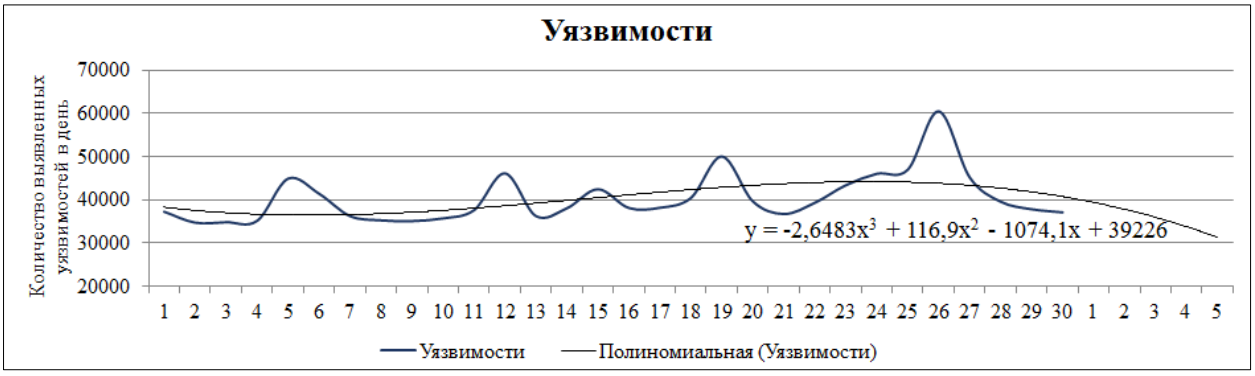

Рисунок 4. Временной ряд выявленных уязвимостей

Это пока что первый обнадёживающий прогноз, показывающий значительное уменьшение количества использования злоумышленниками уязвимостей в начале декабря (на 5000 меньше, чем в самый «спокойный» день ноября).

Временной ряд количества спама в день на протяжении целого месяца представлен на рис.5. Следует отметить, что для этого вида вредоносной деятельности характерны самые высокие показатели по вертикальной оси (количество в день).

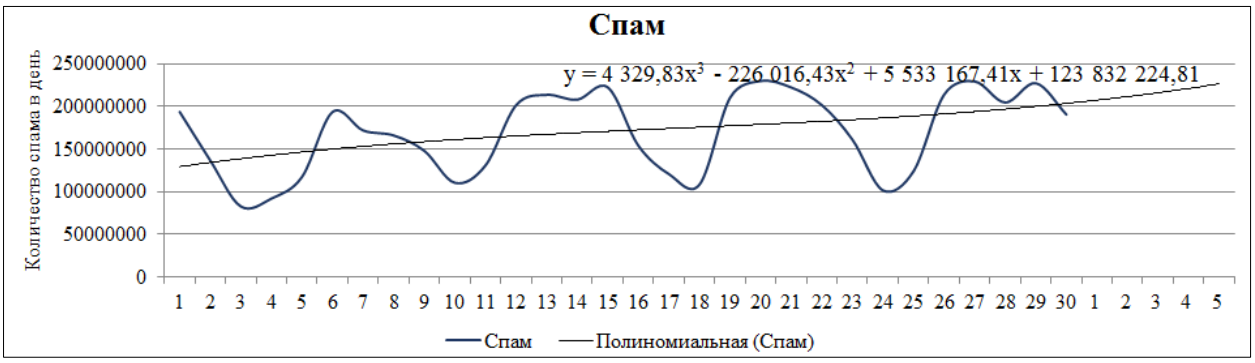

Рисунок 5. Временной ряд, отображающий количество спама в день в ноябре

Можно сделать вывод, что в рассматриваемый для прогнозирования период количество спама не превысит значительно показатели прошлого месяца, однако спада активности спамеров так же ожидать не приходится.

Количество заражений через почту отображено на рис.6.

Рисунок 6. Временной ряд заражений через почту

Исходя из прогнозов, можно сделать вывод о том, что в начале декабря можно ожидать значительное увеличение количества заражений почты в день.

На этапе III были произведены расчеты коэффициентов ускорения изменения количества атак всех видов как третья производная уравнений полиномиального тренда третьей степени по формуле (1):

$$(-5{,}15x^3 + 355{,}24x^2 + 9\,272{,}31x + 2\,584\,565{,}85)''' = -30{,}9$$

$$(43{,}56x^3 - 2418{,}1x^2 + 38149x + 798604)''' = 261{,}36$$

$$(445{,}25x^3 - 17\,064{,}38x^2 + 169\,474{,}46x + 2\,680\,372{,}73)''' = 2671{,}5$$

$$(-2{,}6483x^3 + 116{,}9x^2 - 1074{,}1x + 39226)''' = -15{,}8898)$$

$$(4\,329{,}83x^3 - 226\,016{,}43x^2 + 5\,533\,167{,}41x + 123\,832\,224{,}81)''' = 25978{,}98$$

$$(6{,}2757x^3 - 285{,}8x^2 + 4218x + 6869{,}5)''' = 37{,}6542$$

Этап IV. Результаты использования приведённой методики отображены в таблице 1, угрозы расположены в порядке возрастания процента увеличения атак в день.

Таблица 1. Данные изменения количества кибератак в день на территории РФ

№ п/п	Наименование атаки	Среднее значение за месяц	Коэффициент ускорения (количество/день)	Увеличение атак в день, %
1	Заражения	2803109,567	−30,9	−0,0011
2	Уязвимости	40333,8	−15,8898	−0,0394
3	Спам	169570700	25978,98	0,0153
4	Веб-угрозы	945779,566	261,36	0,0276
5	Сетевые атаки	3138266,4	2671,5	0,0851
6	Заражённая почта	27404,867	37,6542	0,1374

Расчет увеличения атак в день производился по формуле (2).

4.3. Анализ результатов реализации методики

По данным таблицы 1 можно сделать вывод о развитии рассматриваемых видов угроз. Итак, значения в последнем столбце для таких угроз как заражение и использование уязвимостей информационных систем являются отрицательными, что свидетельствует о снижении активности злоумышленников, атакующим по этим направлениям. Процент увеличения спама не значителен и не вызывает опасений.

Наиболее быстрый рост можно ожидать от веб-угроз, сетевых атак и заражений через почту. Причем для зараженной почты показатели самые неутешительные — прирост составляет почти 0,14% и имеет значительный разрыв с предыдущими угрозами.

5. Обсуждение.

Из анализа результатов реализации методики следует, что наиболее быстроразвивающимися являются заражения через почту. Следовательно, ближайшее время надо обратить внимание на существующие методы защиты от данного вида угрозы.

Так или иначе, рассылки по почте по-прежнему остаются очень эффективным способом распространения вредоносного кода. И можно предположить, что в дальнейшем это средство заражения будет использоваться все чаще и чаще, приобретая все более изощренное оформление, используя при этом самую главную уязвимость любой информационной системы — её пользователя.

Рассмотренная методика может применяться и при прогнозировании на более длительные периоды. Например, используя статистические данные по количеству реализаций угроз информационной безопасности за год за год, можно прогнозировать развитие того или иного вида угрозы в следующем месяце.

6. Заключение

В результате проведённого анализа были выявлены наиболее возможные быстроразвивающиеся угрозы на первые числа декабря. Для этого была применена методика прогнозирования киберактивности в РФ на основе построения полиномиальных трендов третьей степени и расчета коэффициента ускорения изменения количества атак за период.

Быстроразвивающимися угрозами были определены веб-угрозы, сетевые атаки и заражённая почта. Именно для них прогнозируется увеличение количества совершений в день.

Практическая значимость работы заключается в возможности использования предложенной методики при долгосрочном прогнозировании. Это будет достижимо при наличии статистических данных за длительный период времени.

Список используемой литературы

[1] Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – 17 с.

[2] Интерактивная карта киберугроз // Лаборатория Касперского URL: https://cybermap.kaspersky.com/ru/stats/ (дата обращения: 22.11.2018).

[3] Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы. // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: 2011. — С. 8-13. — URL https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 02.12.2018).

[4] Юсупова, Н.И. Системное моделирование процесса информационной поддержки разработки паспортов безопасности опасных производственных объектов / Н.И. Юсупова, С.А. Митакович, К.Р. Еникеева // Вестник Уфимского государственного авиационного технического университета. – 2008. – vol. 10, №. 2 – pp. 80-87.

[5] Сагдеев, К.М. Методика оценки технической защищенности речевой информации в выделенных помещениях / К.М. Сагдеев, В.И. Петренко //

Известия Южного федерального университета. Технические науки. – 2012. – vol. 137, no. 12 (137). – pp. 121-129.

[6] Тебуева, Ф.Б. Декомпозиция и прогнозирование временных рядов с долговременными корреляциями / Ф.Б. Тебуева, В.А. Перепелица, М.Ю. Кабиняков // Известия Южного федерального университета. Технические науки. – №. 1 (138). – 2013. – pp. 111-120.

List of references

[1] Doctrine of Information Security of the Russian Federation

[2] https://cybermap.kaspersky.com/ru/stats/ (access date: 30.11.2018).

[3] A. Borshevnikov. Network attacks. Kinds. Ways of struggle. // Modern trends in technical sciences: materials of the Intern. scientific conf. (Ufa, October 2011). - Ufa: Summer, 2011. - p. 8-13. - URL https://moluch.ru/conf/tech/archive/5/1115/ (access date: 02.12.2018) (In Russian).

[4] Yusupova, N.I. System modeling of the process of information support for the development of safety data sheets of hazardous production facilities / N.I. Yusupova, S.A. Mitakovich, K.R. Enikeeva // Bulletin of Ufa State Aviation Technical University. - 2008. - vol. 10, no. 2 - pp. 80-87.

[5] Sagdeev, K.M. Methods for assessing the technical security of speech information in the allocated premises / K.M. Sagdeev, V.I. Petrenko // Proceedings of the Southern Federal University. Technical science. - 2012. - vol. 137, no. 12 (137). - pp. 121-129.

[6] Tebueva, F.B. Decomposition and prediction of time series with long-term correlations / FB Tebueva, V.A. Perepelitsa, M.Yu. Kabinyakov // Proceedings of the Southern Federal University. Technical science. - No. 1 (138). - 2013. - pp. 111-120.

СРАВНИТЕЛЬНЫЙ ОБЗОР МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТ УТЕЧКИ ИНФРМАЦИИ В ЗАДАЧАХ ЦИФРОВОЙ ЭКОНОМИКИ

[1]Кочанов М.С.
Студент кафедры ОТЗИ
smidolty@gmail.com

[2]Павлов А.С.
Аспирант кафедры ПМКБ
losde5530@gmail.com

[3]Петренко В.И.
Канд. тех. наук, доцент
vip.petrenko@gmail.com

[1,2,3] Северо-Кавказский Федеральный университет, г. Ставрополь, 355009, Россия.

Аннотация

В статье проводится анализ методов и принципов информационной безопасности. Рассматриваются такие типы угроз как утечка, модификация и несанкционированный доступ, были рассмотрены методики по решению этих проблем. Проведен сравнительный анализ методов обеспечивающих информационную безопасность от утечки информации в условиях цифровой экономики. В связи с чем подведен итог и предложены рекомендации для обеспечения информационной безопасности. В связи с возникновением нового широкого спектра угроз связанных с утечкой, модификацией и присвоением информации, тема обеспечения информационной безопасности от угрозы утечки информации в условиях цифровой экономики является актуальной и вызывает повышенный интерес. В статье исследованы виды угроз, их специфика и краткое обоснование, а также проведен анализ и выбор критериев эффективности рассмотренных методов в целях повышения информационной безопасности в условиях цифровой экономики. В данной статье проведен сравнительный анализ существующих на данный момент методов обеспечивающих информационную безопасность при утечке информации в условиях цифровой экономики, выявлены сильные стороны каждого из взятых методов, их недостатки.

Abstract

The article analyzes the methods and principles of information security. Such types of threats as leakage, modification and unauthorized access are considered, methods for solving these problems are considered. A comparative analysis of methods to ensure information security from information leakage in the digital economy. In this connection, summed up and proposed recommendations for information security. In connection with the emergence of a new wide range of threats associated with the leakage, modification and appropriation of information, the topic of information security from the threat of information leakage in the digital economy is relevant and is of increased interest. The article investigates the types of threats, their specificity and brief justification, as well as the analysis and selection of criteria for the effectiveness of the methods in order to improve information security in the digital economy. This article provides a comparative analysis of the currently existing methods to ensure information security in information leakage in the digital economy, identified the strengths of each of the methods taken, their shortcomings.

Ключевые слова: информационная безопасность, информационные технологии, защита информации, принципы информационной безопасности, конфиденциальность, целостность, доступность, достоверность и законность.

Keywords: information security, information technology, information protection, principles of information security, confidentiality, integrity, accessibility, reliability and legality.

Введение

Настоящее время принято считать веком информации. С резким внедрением процеса информатизации и высоким уровнем технического развития мы все чаще сталкиваемся с таким понятием как цифровая экономика. Цифровая экономика это отрасль, которая объединяет в себе экономическую, социальную и культурную сферу и непосредственно взаимодействует с обществом посредством цифровых технологий. Россия согласно Распоряжению Правительства полностью пересматривает экономическое взаимодействие в стране и с 28 июля 2017 года постепенно переходит к цифровой экономике[1]. Согласно чему появляется необходимость в введении соответствующих методов обеспечивающих информационную безопасность в условиях цифровой экономики.

«Информационная безопасность – это научная область, которая включает в себя организацию защиты информации от преднамеренных или случайных угроз. [2].»

Под угрозой обычно подразумевают потенциально возможный процесс (явление, событие или воздействие), которое вероятно приводит к нанесению убытка чьим-либо потребностям. Как правило, угрозой информационной безопасности является та угроза, которая нарушает один или несколько установленных принципов информационной безопасности.

На данный момент киберугрозы и киберпреступность в мире по итогам международных данных заняли второе место после техногенных катастроф [3]. В 2016 году произошло более 70 миллионов атак на российские экономические объекты. Ущерб которых составил более 203.5 миллиардов рублей. В 2018 году организованная киберпреступность направленная на кражу персональных данных пользователей увеличилась на 15 процентов с 2015 года. С 2016 года начались активные DDoS атаки направленные на ISO нововведенных криптвалют. Согласно обследованию 237 Российских фирм было выявлено что 40% не имеет стратегий по осуществлению информационной безопасности на предприятии, у 50% отсутствует план реагирования на инциденты связанные с нарушением информационной безопасности.[3].

Постановка задачи

В связи с переходом России в цифровую экономику, возникает необходимость в обеспечении целостной защиты информации от модификации, несанкционированного доступа и утечки информации. В данной статье объектом является утечка информации, где методы обеспечения информационной безопасности в условиях цифровой экономики являются предметом изучения. В связи с большим количеством существующих и разнящихся между собой методов, появляется необходимость провести сравнительный анализ существующих методов, с определением их специфики, сильных и слабых сторон.

Сравнительный анализ методов

В данной статье проведен сравнительный анализ существующих методов обеспечивающих информационную безопасность в условиях цифровой экономики от утечки информации.

Утечка конфиденциальной информации, циркулирующей в программно-аппаратном комплексе, может осуществляться при помощи:

- перехвата конфиденциальной информации за счет побочных электромагнитных излучений и наводок;
- перехвата конфиденциальной информации за счет закладных устройств, установленных в программно-аппаратном комплексе;
- перехвата конфиденциальной информации визуально-оптическим способом;
- несанкционированного доступа к конфиденциальной информации.

Предотвратить утечку можно с помощью пассивных и активных методов и средств защиты. Пассивные методы направлены на снижение побочных электромагнитных излучений и наводок программно-аппаратного комплекса. Снижение происходит с помощью экранирования элементов программно-аппаратного комплекса и заземления. Однако это довольно дорого и нужно уметь правильно экранировать элементы программно-аппаратного комплекса, иначе экранирование не будет действовать в целях защиты. В пассивных методах еще используется защита, основанная на снижение просачивания информационных сигналов в цепи электропитания программно-аппаратного комплекса. Защита осуществляется с помощью фильтрации информационных сигналов.

Активные методы реализуют формирование маскирующих пространственных и линейных электромагнитных помех. Для формирования данных помех используют генераторы шумового сигнала. На сегодняшний день их количество возросло, можно выбрать как отдельный блок генератора, так и отдельную плату, встраиваемую в системный слот программно-аппаратного комплекса. Цена генератора шумового сигнала зависит от диапазона рабочей частоты и от коэффициента качества шума.[4]

В статье [2] предлагается метод обеспечения информационной безопасности от утечки «поиск следа при скрытом активном воздействии».

Для принятия решения о наличии или отсутствии реасобытия в подмножестве используется функция обнаружения, аргументом для которой служит совокупность «тестирующих сигналов». Решение о нахождении следа может основываться на статистическом анализе множества событий подмножества. Отклонение от среднего значения профиля нормального поведения будет свидетельствовать о наличии следа в подмножестве. Например, зафиксирован факт входа сотрудника в информационную систему в нерабочее время, хотя раньше он этого не делал.

Данный подход имеет следующие недостатки:

- относительно высокая вероятность ложных тревог (отклонение от среднего значения профиля нормального поведения не всегда свидетельствует о попытке несанкционированного получения конфиденциальной информации);
- плохая работа, когда действия пользователей не имеют определенного шаблона действий, когда с самого начала пользователи совершают злоумышленные действия (злоумышленные действия типичны), наконец, когда пользователь постепенно изменяет шаблон своего поведения в сторону злоумышленных действий.

Другой подход [3] основывается на использовании «совокупности сигналов» как сигнатур (шаблонов) следов. Они могут быть простыми (строка знаков, соответствующая поиску отдельного условия) или сложными (изменение состояния защиты, выраженное как формальное математическое выражение, последовательность действий или совокупность строк журналов).

Недостатком данного подхода можно считать сложность формирования всего множества сигнатур следов и необходимость его регулярного пополнения. Так как временной фактор принятия решения является в нашем случае некритичным, в сравнении с системами предотвращения утечек информации, работающими в режиме реального времени, то возможно использование обоих подходов.

Для формирования шаблонов выявления следов, присутствия реасобытия в подмножестве могут использоваться следующие критерии: статистические данные, накопленные в организации в результате расследования инцидентов, повлекших утечку конфиденциальных данных; статистические данные, накопленные в сфере ИБ (например, в последние годы преобладающим стал канал утечки информации, связанный с электронным, а не бумажным документом; основным каналом утечки являются вычислительные сети организации и т.д.

В статье [5] приведен эффективный метод борьбы с утечкой информации «фильтр содержимого от утечки информации». Данный метод применим в случае подключения защищенной локальной сети к сети Интернет. Основным преимуществом данного метода является разделение на группы протоколов таких как промышленный интернет;

- протоколы транспортного уровня;
- протоколы сетьевого уровня;
- протоколы прикладного уровня.

Это удобно в случае, если пользователь защищенного сегмента разрешает получить электронную почту, с внешних публичных серверов по протоколу POP3, такой фильтр должен декласифицировать все исходящие IP-пакеты и разрешать TCP-соединение на 110 портах, по которым будутпередаваться определенные команды и идентифицированные данные POP3-серверу в соответствии с RFC 1939.

Опыт широкого применения подобной системы показывает, что они в состоянии гарантировать безопасность при передачи конфиденциальных данных в сеть интернет.

Существенным минусом данного метода является тот факт, что при режиме «быстрой деклассификации» служебной инфрмации в контексте связи «сверху-вниз» нарушается главный принцип модели Белла-ЛаПадула, что влечет за собой риск утечки информации.

В условиях цифровой экономики одним из факторов утечки информации является утечка конфиденциальной информации за счет побочных электромагнитных излучений и наводок[4], осуществляется путем радиоизлучения, возникающего в результате нелинейных процессов в блоках программно-аппаратного комплекса. Предотвратить данную утечку можно с помощью пассивных и активных методов и средств защиты.

Утечка конфиденциальной информации за счет закладных устройств, реализуется при помощи скрытно установленных в программно-аппаратный комплекс электронных устройств. Входными сигналами для них являются электрические сигналы, несущие информационные последовательности, циркулирующие в программно-аппаратном комплексе при обработке конфиденциальной информации. Предотвращение утечки за счет закладных устройств осуществляется путем проведения специальных обследований и специальных проверок элементов программно-аппаратного комплекса.

Специальное обследование осуществляется с помощью визуального осмотра элементов программно-аппаратного комплекса, без использования каких-либо технических средств. Поиск закладных устройств осуществляется по демаскирующим признакам их внешнего вида. Специальная техническая проверка проводится с использованием специальных технических средств. Осуществляется специальная проверка элементов программно-аппаратного комплекса с применением рентгеновских комплексов.

Так же производится организация радио контроля и побочных электромагнитных излучений ПАК. В результате выявление закладных устройств производится их уничтожение. Утечка конфиденциальной информации визуально-оптическим способом, осуществляется с помощью технических средств наблюдения, фотографирования. Утечка конфиденциальной информации в результате несанкционированного доступа, реализуется за счет доступа к информации, нарушающего правила разграничения доступа с использованием штатных средств, предоставляемых программно-аппаратным комплексом.

Заключение

Проанализировав все вышеперчисленные методы обеспечения информационной безопасности от утечки информации в задачах цифровой экономики, можно прийти к

выводу, что в данный момент не существует единой системы методов обеспечения информационной безопасности в задачах цифровой экономики. Все вышеописанные методы являются разрозненными с отличающейся спецификой их применения. В связи с чем следует уделить достаточное внимание разработке системы методов обеспечивающих комплексную защиту информации в условиях цифровой экономики.

Список используемой литературы

[1] Распоряжение Правительства от 28 июля 2017 г. № 1632-р М. 2017.

[2] Учаев Д.Ю., Брумштейн Ю.М., Ажмухадедов И.М., Князева О.М., Дюдиков И.А. Анализ и управление рисками, связанными с информационным обеспечением человеко-машинных асу технологическими процессами в реальном времени. Прикаспийский журнал: управление и высокие технологии. 2016. № 2 (34). С. 82-97.

[3] Удалов Д.В. Угрозы и вызовы цифровой экономики// Экономическая безопасность и качество. №1.30. 2018. С. 12-19.

[4] Пронина Н.Ю. Предотвращение утечки конфиденциальной информации, циркулирующей в программно-аппаратном комплексе обработки и передачи конфиденциальной информации// сборник трудов конференции. 2018. С. 164-167.

[5] Чалдаева Л.А., Килячков А.А. Методы обеспечения информационной безопасности копании: Финансы и кредит. 2002. № 21 (111). С. 55-62.

[6] Зайцев С.Е. Политики информационной безопасности в системах информационной безопасности. Научный вестник Московского государственного технического университета гражданской авиации. 2008. № 137. С. 37-44.

[7] Каратеев Ю.П., Минкина Т.В., Семыкина Е.В. Прикладные аспекты формирования информационной системы предприятия.// Информационно-экономические аспекты бизнес-процессов и финансового развития регионов Материалы Международной научно-практической конференции. 2018. С. 182-186.

[8] Минкина Т.В., Зуб А.В. Опасность хакерских атак и зашита информации в сети. // Материалы II Международной научно-практической конференции, приуроченной ко дню принятия Уголовного Кодекса РФ / 2018.

[9] Тищенко Е.Н., Шарыпова Т.Н. Формализация выбора различных вариантов системы защиты информации от несанкционированного доступа в среде электронного документооборота. Вестник Ростовского государственного экономического университета (РИНХ). 2010. № 3 (32). С. 226-233.

[10] Забокрицкий Е.И., Заводнов В.С., Минкина Т.В. Предпосылки угроз информационной безопасности объекта// «Студенческая наука для развития информационного общества». СКФУ(Ставрополь), 2015 г. С. 181-182.

[11] Кузьминов Ю.В., Мирошников Д.А., Емельянов Е. Проблемы автоматизации. Региональное управление. Связь и автоматика - Паруса-2015 Сборник трудов IV Всероссийской научной конференции молодых ученых, аспирантов и студентов. 2015. С. 85-88.

[12] Vovchenko N.G., Gontmacher M.B., Tishchenko E.N., Epifanova T.V. Electronic currency: the potential risks to national security and methods to minimize them. European Research Studies Journal. 2017. T. 20. № 1. P. 36-48.

List of references

[1] Government Decree of July 28, 2017 No. 1632-r M. 2017.

[2] Uchaev D.Yu., Brummstein Yu.M., Azhmukhadov I.M., Knyazeva OM, Dyudikov I.A. Analysis and management of risks associated with the information support of man-machine asu technological processes in real time. Caspian magazine: management and high technology. 2016. № 2 (34). Pp. 82-97.

[3] Udalov D.V. Threats and challenges of the digital economy // Economic security and quality. №1.30. 2018. pp. 12-19.

[4] Pronin N.Yu. Preventing leakage of confidential information circulating in the software and hardware complex for processing and transmitting confidential information // Proceedings of the conference. 2018. pp. 164-167.

[5] Chaldayeva LA, Kilyachkov A.A. Methods of ensuring information security digging: Finance and credit. 2002. № 21 (111). Pp. 55-62.

[6] S. Zaitsev Information security policies in information security systems. Scientific Bulletin of the Moscow State Technical University of Civil Aviation. 2008. No. 137. S. 37-44.

[7] Karateev Yu.P., Minkina T.V., Semykina E.V. Applied aspects of the formation of the enterprise information system. Information and economic aspects of business processes and financial development of regions. Materials of the International Scientific and Practical Conference. 2018. pp. 182-186.

[8] Minkina T.V., Zub A.V. The danger of hacker attacks and protection of information in the network. // Proceedings of the II International Scientific and Practical Conference, dedicated to the day of the adoption of the Criminal Code of the Russian Federation 2018.

[9] Tishchenko E.N., Sharypova T.N. Formalization of the choice of various options for protecting information from unauthorized access in an electronic document management environment. Bulletin of the Rostov State Economic University (RINH). 2010. No. 3 (32). Pp. 226-233.

[10] Zabokritsky EI, Zavodnov VS, Minkina T.V. Background of threats to information security of the object // "Student science for the development of the information society." SKFU (Stavropol), 2015. P. 181-182.

[11] Kuzminov Yu.V., Miroshnikov DA, Yemelyanov E. Problems of automation. Regional Office. Communication and Automation - Sails-2015 Collection of works of the IV All-Russian Scientific Conference of young scientists, graduate students and students. 2015. P. 85-88.

[12] Vovchenko N.G., Gontmacher M.B., Tishchenko E.N., Epifanova T.V. It is a risk factor to minimize them. European Research Studies Journal. 2017. V. 20. No. 1. P. 36-48.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СРЕДСТВ МОНИТОРИНГА КОМПЬЮТЕРНОЙ СЕТИ

Нечволода В.Э[1]
nechvolodaa@yandex.ru

Смыкова В.Н[2]
zwho@yandex.ru

Рябцев С.С[3]
Nalfartorn@yandex.ru

Петренко В.И.
кандидат технический наук, доцент
vipetrenko@ncfu.ru

[1]Северо-Кавказский федеральный университет (СКФУ), Ставрополь, 355000, Россия

Аннотация

Мониторинг компьютерной сети имеет решающее значения в ИТ – системах.
Стремительное развитие информационных сетей требует высоких показателей доступности, быстродействия и отказоустойчивости. Возникает необходимость постоянного контроля состояния этих показателей с использованием средств мониторинга.
В данной статье описывается средства мониторинга, позволяющие обеспечить безопасность информационной системы, а также представлен сравнительный анализ программ мониторинга компьютерной сети согласно критерию оценки.

Abstract

Computer network monitoring is critical in IT systems. The rapid development of information networks requires high availability, speed and fault tolerance. There is a need for continuous monitoring of the state of these indicators using monitoring tools. This article describes the means and methods to ensure the security of the information system, as well as a comparative analysis of computer network monitoring programs according to the evaluation criterion.

Ключевые слова: Мониторинг компьютерной сети, марковские цепи, программа для мониторинга, информационная система, сетевая безопасность.

Keywords: Computer network monitoring, Markov chains, monitoring program, information system, network security.

1 Введение

Оценка степени защищенности информационных систем является одним из основных направлений деятельности специалиста, занимающегося обеспечением безопасности информации. Широкое применение компьютерных сетей в различных сферах деятельности и высокие требования по обеспечению надежности их работы обусловливают актуальность задачи мониторинга компьютерной сети.

В настоящее время большая нагрузка на компьютерные сети требует минимизации времени простоя, что увеличивает доступность услуг и предотвращения сетевых проблем.

Одним из методов борьбы с сетевыми атаками может служить постоянный мониторинг и наблюдение за аномально поведением сетевого трафика, поскольку резкое увеличение количество передаваемой или принимаемой информации обычно является признаком атаки на сетевой ресурс [1]

Согласно ГОСТу [2] под мониторингом сети понимают процесс постоянного наблюдения и проверки зафиксированных данных о сетевой деятельности и операциях, включая контрольные журналы и предупреждения об опасности, и связанный с этим анализ.

В отличии от системы обнаружения и предотвращения вторжений, мониторинг не только предполагает управление безопасностью, выявляя и не допуская потенциально опасную деятельность несанкционированных пользователей, но и обеспечивает функционирование подсистем управления конфигурацией сети, контроля и анализа производительности и надёжности объектов сети, обработки ошибок и управления устранения неисправностей.

В работах [3,4] описывается процесс мониторинга сети, его основные категории и классификации, а также представлена сравнительная характеристика различных продуктов мониторинга компьютерной сети. Дополнить её можно, использовав критерии оценки, приведённые в данной статье.

В исследовании [5] показаны результаты оценки, проведённые по шести общедоступным инструментам мониторинга, где отбор производился по таким критериям, как масштабируемость, гибкость, надёжность, а также сбор данных и отображения. В результате проведённой оценки выявлены преимущества программного комплекса Zabbix. В работе был представлен подробный анализ программного комплекса Zabbix, но не все средства мониторинга были проанализированы детально.

Согласно основным результатам отчётности по кибербезопасности CISCO [6] растёт сложность, частота и длительность атак методом перегрузки, большинство вредоносных доменов связаны со спам – кампаниями, огромное число организаций подверглись кибератакам на ОТ – инфраструктуру. С помощью карты киберугроз [7] и статистике, которая сделана по России, было выявлено 5794379 сетевых атак за последний месяц. Все вышеперечисленные

факты говорят о необходимости использования различных методов защиты, в том числе мониторинга компьютерной сети, что подтверждает актуальность применения данного способа защиты.

2 Постановка задачи мониторинга

Рассмотрим постановку задачи мониторинга компьютерной сети. В целом задачу мониторинга компьютерной сети можно описать следующим методом. Поскольку события, происходящие в компьютерных сетях и информационных системах, носят случайный характер, то для их изучения наиболее подходящими являются вероятностные математически модели теории массового обслуживания. В данном случае воспользуемся теорией марковский цепей [8].

На начальном этапе моделирования необходимо определить входные данные. В качестве состояний рассматриваемой системы мониторинга сети предлагается рассмотреть события, связанные с обнаружением неисправностей в ходе диагностики и контроля исследуемых системой параметров оборудования в сети.

Исходя из вышеизложенного, опишем возможные состояния в процессе мониторинга параметров сетевого оборудования:

- S_0 – отсутствие неисправностей;
- S_1 – перегрузка сети;
- S_2 – снижение пропускной способности;
- S_3 – недопустимость порта;
- S_4 – физическая недопустимость устройства;
- S_5 – фрагментация пакета;
- S_6 – полный отказ системы.

Описанную цепь событий в ходе мониторинга сети можно представить в виде графа состояний (рисунок 1.)

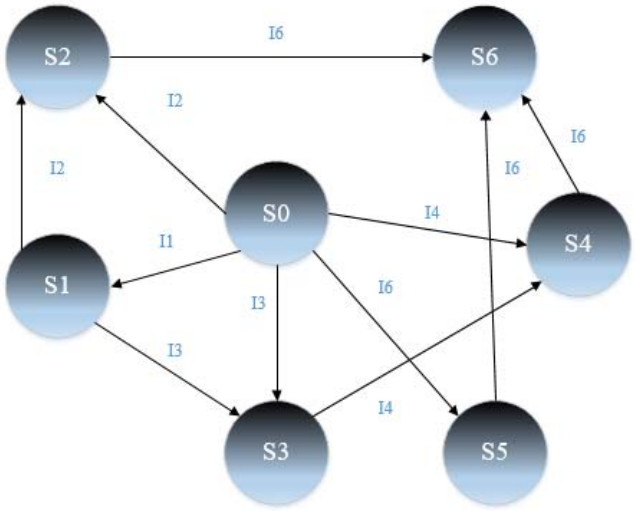

Рисунок 1. Граф обнаружения неисправных параметров в ходе мониторинга сети

Вероятность i -го состояния определяется в данном случае как вероятность нахождения системы в состоянии S_i, то есть вероятность обнаружения системой мониторинга i -го неисправного параметра в сети.

На графе, представленном выше, каждая стрелка соответствует интенсивности того потока событий, который переводит систему из одного состояния в другое. Последовательность опроса определяется назначенным системным администратором приоритетом. Чем выше будет приоритет у параметра сетевого устройства, тем выше интенсивность его опроса. За интенсивности переходов в данном случае принимается I_i – интенсивность опроса i -го параметра в системе мониторинга.

С учётом изложенного материала работы системы мониторинга исходит, что она из состояния S_0 при выполнении опроса сетевых устройств при отказе любого компонента переходит в состояние обнаружения неисправностей S_i с интенсивностью I_i.

По графу (рисунок 1.) составим математическую модель процесса мониторинга сети с учётом вероятностей p_i в виде системы уравнений (1)

$$\begin{cases} \frac{dp_0}{dt} = -p_0 \cdot (I_1 + I_2 + I_3 + I_4 + I_5) \\ \frac{dp_1}{dt} = p_0 \cdot I_1 - p_1 \cdot (I_2 + I_3) \\ \frac{dp_2}{dt} = p_0 \cdot I_2 + p_1 \cdot I_2 - p_1 \cdot I_6 \\ \frac{dp_3}{dt} = p_0 \cdot I_3 + p_1 \cdot I_3 - p_3 \cdot I_4 \\ \frac{dp_4}{dt} = p_0 \cdot I_4 + p_3 \cdot I_4 - p_4 \cdot I_6 \\ \frac{dp_5}{dt} = p_0 \cdot I_5 - p_5 \cdot I_6 \\ \frac{dp_6}{dt} = p_2 \cdot I_6 + p_5 \cdot I_6 + p_4 \cdot I_6 \end{cases} \quad (1)$$

Решение системы дифференциальных уравнений (1) позволяет отследить динамику диагностирования неисправных параметров в процессе сетевого мониторинга путём отслеживания вероятностей в определённые промежутки времени.

3 Анализ программ для мониторинга компьютерной сети

Программы (средства) для мониторинга сети – это незаменимые помощники каждого системного администратора. Они позволяют оперативно реагировать на аномальную деятельность в пределах локальной сети, быть в курсе всех сетевых процессов и, таким образом, автоматизировать часть рутинной деятельности администратора, прежде всего той, что связана с обеспечением сетевой безопасности.

В настоящее время существует множество различных программ мониторинга компьютерной сети. Однако наиболее популярными являются Zabbix, Nagios XI, Cacti.

Проведём анализ особенностей их использования.

Система мониторинга Zabbix [9] – свободная система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования. Zabbix использует гибкий механизм уведомлений, что позволяет пользователям настраивать оповещения по почте практически для любого события. Это даёт возможность быстро среагировать на проблемы с сервером. Zabbix предполагает отличные возможности отчётности и визуализации данных.

Данная программа состоит из четырёх частей:

- Сервер мониторинга (ядро), выполняющий периодический опрос и получение данных, их обработку и анализ, а также осуществляет запуск скриптов для рассылки оповещений. Сервер мониторинга удалённо проверяет сетевые сервисы, является хранилищем, в котором храниться конфигурационные, статистические и оперативные данные.
- Прокси сервер – собирает данные о производительности и доступности от имени Zabbix сервера. Все собранные данные заносятся в буфер на локальном уровне и передаются Zabbix серверу, к которому принадлежит прокси – сервер. Zabbix прокси является идеальным решением для централизованного удалённого мониторинга мест, филиалов, сетей, не имеющих локальных администраторов.
- Агент – специальный демон, который запускается на отслеживаемых объектах и предоставляет данные серверу, осуществляя контроль локальных ресурсов и приложений на сетевых системах, то есть эти системы должны работать с запущенным Zabbix агентом.
- Веб интерфейс – средство визуального предоставления Zabbix, реализован на PHP, для запуска требует наличия веб – сервера.

К основным особенностям Zabbix относят: автоматическое обнаружение серверов и других устройств в сети, распределённый мониторинг с централизованным администрированием через WEB, серверное программное обеспечение для Linux, Solaris, Aix, безопасная аутентификация пользователей, журналы аудита, WEB – интерфейс.

Nagios. В качестве рассмотрения данного продукта была выбрана версия Nagios XI, так как она имеет больше функциональных возможностей по сравнению с Nagios Core.

Nagios XI – это простое в использовании приложение для мониторинга ИТ-инфраструктуры, которое позволяет отслеживать критические серверы, сетевое оборудование, службы и приложения и уведомлять о возникших проблемах.

Nagios XI способен отслеживать сотни различных типов приложений, сервисов, протоколов и компьютерного оборудования, используя встроенные возможности и сторонние расширения и дополнения.

К основным возможностям инструмента Nagios XI можно отнести: мониторинг характеристик с использованием плагинов, простой формат конфигурационного файла (при наличии минимального опыта в программировании можно писать собственные плагины для Nagios), возможность оставлять комментарии с меткой времени, поддержка удалённого мониторинга через шифрованные туннели SSH, возможность проводить анализ сбоев в работе с помощью множества отчётов, предлагаемых веб – интерфейсом системы.

Cacti [10] – инструмент для мониторинга сети с открытым исходным кодом, позволяющий строить графики при помощи RRDtool (набор утилит для работы с циклической базой данных). Cacti собирает статические данные за определённые временные интервалы и позволяет отобразить их в графическом виде. Он обычно используется для сбора данных временных рядов показателей, таких как загрузка процессора и использование пропускной способности сети. Мониторинг сетевого трафика производится путем опроса сетевого коммутатора или интерфейса маршрутизатора через протокол SNMP (Simple Network Management Protocol).

Интерфейс отображения статистики, собранной с устройств, представлен в виде дерева, структура которого задаётся самим пользователем. Как правильно, графики группируют по определённым критериям, причём один и тот же график может присутствовать в разных ветвях дерева. Каждый из графиков можно рассматривать отдельно, при этом он будет представлен за последний день, неделю, месяц и год. Пользователь имеет возможность самостоятельно выбрать временной промежуток, за который будет сгенерирован график.

4 Сравнительная характеристика инструментов мониторинга компьютерной сети

Проведём сравнительную характеристику средств мониторинга компьютерной сети, которые рассматривались в предыдущей главе. Составленная таблица 1 позволит визуально оценить функционал существующих свободно распространяемых систем комплексного мониторинга IT – инфраструктуры.

Таблица 1. Функционал свободно распространяемых систем мониторинга

	Системы мониторинга		
Функциональность	Zabbix	Nagios	Carti
Диаграммы	Да	Да	Да
Отчёты SLA	Да	Через плагин	Да
Логическая группировка	Да	Да	Да
События	Да	Да	Да
Автоматическое обнаружение	Да	Через плагин	Да
Агент	Да	Да	Нет
SNMP	Да	Через плагин	Да
Внешние скрипты	Да	Да	Да
Плагины	Да	Да	Да
Триггеры/тревоги	Через плагин	Через плагин	Нет
Инвентаризация	Да	Динамические и настраиваемые	Через плагин

В качестве дополнительных сведений о продуктах были рассмотрены следующие категории параметров (цена, прогнозирование событий, процесс мониторинга, методы уведомления, создания плагинов, скорость реакции на отказ, функции дополнения).

Цена. Zabbix и Cacti являются бесплатными продуктами, так как они обладают открытом исходном кодом, который свободно распространяется и доступен широкой публике. Nagios Xl – коммерческая система, стоимость которой составляет $1 650 USD. Исходя из этого, пользователи в первую очередь обратят внимания на инструменты, не требующие покупки лицензии.

Прогнозирование событий. При рассмотрении данного вопроса, лидером стала программа Zabbix, в которой есть возможность смотреть историю собранных данных и предсказать, как будут развиваться события в дальнейшем. Второе место Cacti – процесс прогнозирования у него проще, чем у Zabbix. Nagios XI – не имеет такой функции.

Процесс мониторинга. Все системы могут производить мониторинг как на более низких уровнях, так и на высоких. Поэтому в этом случае, все программы имеют одинаковую актуальность.

Методы уведомления. Nagios XI и Zabbix имеют одинаковый набор предупреждений (по электронной почте, SMS, Jabber), по сравнению с Cacti, который обладает только возможностью оповещения по электронной почте.

Скорость реакции на отказ. Наилучшие результаты показал Zabbix, где можно настраивать минимальный интервал в секунду, и это возможно для каждого устройства. Второе место – Nagios XI, в котором интервал реакции на отказ составляет не меньше, чем на минуту. В Cacti не удалось установить интервал индивидуально, так как он имеет только глобальное значение.

Функции дополнения. Zabbix с включённой функцией инвентаризации на основе метода ITIL является единственной системой мониторинга, которая имеет дополнительную функцию.

Создание плагинов. Программные модули, подключаемые к основной программе, предназначенные для расширения, доступны для каждого из продуктов, однако их реализация в Zabbix и Nagios XI происходит проще, чем в Cacti.

Для наглядного представления о том, какое количество пользователей предпочитают тот или иной инструмент мониторинга компьютерной сети, была сделана статистика запросов по ключевым словам на популярном поисковом ресурсе google.com с 2013. (рисунок 2).

Рисунок 2. Статистика запросов в поисковой системе google.com за последние 5 лет

Статистика показывает, что в 2013 году лидирующую позицию занимал Nagios. В 2015 году Zabbix и Nagios имели практически одинаковое количество запросов, а уже ближе к 2018 году

программа Zabbix имеет наибольший интерес среди других средств мониторинга компьютерной сети.

5 Обсуждения

В качестве средств мониторинга компьютерной сети были рассмотрены Zabbix, Nagios XI, Cacti, на основе которых производилась сравнительная характеристика, позволяющая выявить принципиальные различия каждой системы.

Лидером стал Zabbix, имеющий преимущества над другими средствами мониторинга. Достоинством является то, что Zabbix – это открытый продукт, и у него нет никаких закрытых версий. Он является решением «всё в одном», то есть пользователю не нужно строить систему мониторинга из разных отдельных блоков, Zabbix сам визуализирует, обнаруживает проблемы и собирает информацию различными способами. Это делает Zabbix идеальным инструментом для планирования и масштабирования.

Результаты, полученные в данной статье, можно использовать при выборе средств мониторинга и решений обеспечения безопасности сети, так как зная функциональные особенности каждого, легко выбрать подходящий продукт для той или иной цели.

6 Заключение

В данном исследовании рассматривалась проблема мониторинга компьютерной сети, её важность с точки зрения защиты информации. Описан математический метод мониторинга сети на основе теории цепей Маркова, позволяющий отследить неисправные параметы в процессе сетевого мониторинга путём отслеживания вероятностей в определённые промежутки времени.

Проанализированы основные средства мониторинга, такие как Zabbix, Nagios XI, Cacti. Оценка качества выполнения функций различных инструментов мониторинга сети привели к выбору Zabbix в качестве оптимального кандидата.

Список используемой литературы

[1] И. М. Ажмухамедов, А. Н. Марьенков. Обеспечение информационной безопасности компьютерных сетей на основе анализа сетевого трафика. Ж: Вестник Астраханского государственного технического университета, серия: управление, вычислительная техника и информатика, 2011, 137-141 с.

[2] ГОСТ Р ИСО/МЭК 27033-1—2011. - Методы и средства обеспечения безопасности, Москва, Стандартинформ, 2012.

[3] Marik, O., & Zitta, S. (2014). Comparative analysis of monitoring system for data networks. 2014 International Conference on Multimedia Computing and Systems (ICMCS). doi:10.1109/icmcs.2014.6911307.

[4] Hernantes, J., Gallardo, G., & Serrano, N. (2015). IT Infrastructure-Monitoring Tools. IEEE Software, 32(4), 88–93. doi:10.1109/ms.2015.96.

[5] Telesca, A., Carena, F., Carena, W., Chapeland, S., Barroso, V. C., … Costa, F. (2014). System performance monitoring of the ALICE Data Acquisition System with Zabbix. Journal of Physics: Conference Series, 513(6), 062046. doi:10.1088/1742-6596/513/6/062046

[6] Годовой отчёт по кибербезопасности CISCO за 2018 год. URL: https://www.cisco.com/c/ru_ru/products/security/security-reports.html

[7] Интерактивная карта киберугроз. URL: https://cybermap.kaspersky.com/ru

[8] Зорин А.В., Пройдакова Е.В., Федоткин М.А.: Учебно-методическое пособие – Нижний Новгород: Нижегородский госуниверситет, 2013. – 51с.

[9] Андреа Далле Вакке. «Zabbix. Практическое руководство. Второе издание». 2016г, 356 с.

[10] The Cacti Manual. Ian Berry, Tony Roman, Larry Adams, J.P. Pasnak, Jimmy Conner, Reinhard Scheck, and Andreas BraunPublished 2017 Copyright © 2017 The Cacti Group, 97 с.

[11] Linikova O. E., Monitoring of server hardware and applications. Master's thesis. Ural Federal University named after the fi rst President of Russia B. N. Yeltsin. – Ekaterinburg, 2014. – 123 c. (In Russ.)

List of references

[1] I.M. Azhmukhamedov, A.N. Marienkov. Providing information security of computer networks based on network traffic analysis. W: Bulletin of the Astra-Khan State Technical University, series: control, computer technology and computer science, 2011, 137-141 p.

[2] GOST R ISO IEC 27033-1—2011. - Methods and means of ensuring security, Moscow, Standardinform, 2012.

[3] Marik, O., & Zitta, S. (2014). Comparative analysis of the monitoring system for data net-works. 2014 International Conference on Multimedia Computing and Systems (IC-MCS). doi: 10.1109 / icmcs.2014.6911307.

[4] Hernantes, J., Gallardo, G., & Serrano, N. (2015). IT Infrastructure-Monitoring Tools. IEEE Software, 32 (4), 88–93. doi: 10.1109 / ms.2015.96.

[5] Telesca, A., Carena, F., Carena, W., Chapeland, S., Barroso, V. C., ... Costa, F. (2014). ALICE Data Acquisition System with Zabbix. Journal of Physics: Conference Series, 513 (6), 062046. doi: 10.1088 / 1742-6596 / 513/6/062046

[6] CISCO cybersecurity annual report for 2018. URL: https://www.cisco.com/c/ru_ru/products/security/security-reports.html

[7] Interactive map of cyber threats. URL: https://cybermap.kaspersky.com/ru

[8] Zorin A.V., Proidakova E.V., Fedotkin M.A .: Educational-methodical manual - Nizhny Novgorod: Nizhny Novgorod State University, 2013. - 51 p.

[9] Andrea Dalle Vacca. "Zabbix. A practical guide. Second Edition. 2016, 356 s.

[10] The Cacti Manual. Ian Berry, Tony Roman, Larry Adams, J.P. Pasnak, Jimmy Conner, Reinhard Scheck, and Andreas BraunPublished 2017 Copyright © 2017 The Cacti Group, 97 p.

[11] O. E. Linikova, Monitoring of server hardware and applications. Master's thesis. Ural Federal University named after President B. N. Yeltsin. - Ekaterin-burg, 2014. - 123 p. (In Russ.)

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ СОЗДАНИЯ SIEM-СИСТЕМ НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ ПОКАЗАТЕЛЕЙ КОМПРОМЕТАЦИ

Родин Д. А.
26drodin07@gmail.com

Бесланеева Е. Ю.
miss.ekaterina1997@yandex.ru

Лапина М. А.
norra7@yandex.ru

Емельянов Е. А.
kenwood078@yandex.ru

[1] Северо-Кавказский Федеральный университет, Ставрополь, 355009, Российская Федерация

Аннотация

В настоящее время все большую популярность набирают SIEM системы, однако высокая стоимость внедрения развитие их рынка. Эту проблему возможно решить, используя систему на основе открытых источников показателей компрометации. В статье описаны общие возможности SIEM – систем, их функционал и состав, проведен анализ современного рынка SIEM систем, а также проведен анализ открытых источников показателей компрометации.

Abstract

Currently, SIEM systems are gaining more and more popularity, but the high cost of implementation is the development of their market. This problem can be solved using a system based on open sources of indicators of compromise. The article describes the general capabilities of the SIEM systems, their functionality and composition, analyzes the current market for SIEM systems, and analyzes the open sources of compromise indicators.

Ключевые слова: мониторинг событий ИБ, SIEM, защита информации, централизованный мониторинг, КОМРАД, показатели компрометации.

Keywords: monitoring of information security events, SIEM, information security, centralized monitoring, COMRAD, compromise indicators.

1. Введение

1.1 Обзор нормативной базы

SIEM (Security information and event management) — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информационной безопасностью, и SEM (Security event management) — управление событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами или услугами, применяется кроме того с целью для журналирования данных и генерации отчетов в целях совместимости с другими бизнес-данными. [1]

Существует большое количество стандартов и руководств, регламентирующих вопросы управления инцидентами информационной безопасности. В таблице 1.1 представлены актуальные версии стандартов, затрагивающих вопросы управления инцидентами ИБ.

Таблица 1.1 Актуальные версии стандартов, описывающих вопросы управления инцидентами ИБ

Категория	Стандарты	
	Международные	Российские
Специализированные по инцидентам ИБ	ISO/IEC 27035-1:2016	ГОСТ Р ИСО/МЭК 18044-2007
	ISO/IEC 27035-2:2016	
По системе менеджмента информационной безопасности	ISO/IEC 27000:2016	ГОСТ Р ИСО/МЭК 27000-2012
	ISO/IEC 27001:2013	ГОСТ Р ИСО/МЭК 27001-2006
	ISO/IEC 27002:2013	ГОСТ Р ИСО/МЭК 27002-2012
	ISO/IEC 27011:2016	ГОСТ Р ИСО/МЭК 27011-2012
По информационной безопасности	ISO/IEC 27033-1:2015	ГОСТ Р ИСО/МЭК 27033-1-2011
Для управления и обслуживания IT сервисов	ISO/IEC 20000-1:2011	ГОСТ Р ИСО/МЭК 20000-1-2013
Отраслевые	–	СТО БР ИББС-1.0-2014

Так ГОСТ Р ИСО/МЭК 27000-2012 вводит определения:

— событие информационной безопасности – выявленное состояние системы, услуги или состояния сети, указывающее на возможное нарушение или отказ мер и средств контроля и управления или прежде всего неизвестная ситуация, которая может иметь значение для безопасности [1];

ГОСТ Р ИСО/МЭК 27001-2006 «Информационные технологии – Методы безопасности – Системы управления информационной безопасностью – Требования» устанавливает общие требования к построению системы управления информационной безопасности, относящиеся в том числе и к процессам управления инцидентами. В рамках настоящего стандарта также выдвигаются требования к процессу реагирования на инциденты: своевременное выявление удавшихся и неудавшихся попыток нарушения инцидентов информационной безопасности, помощь в обнаружении событий безопасности путем использования индикаторов, и. т. д [2].

ГОСТ Р 53114-2008 вводит следующие определения [4]:

— угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
— уязвимость информационной системы – свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

1.2 Общий функционал SIEM-систем и архитектура

Функциональность SIEM-систем:

— Агрегация данных: данные поступают из различных источников: сетевые устройства и сервисы, датчики систем безопасности, серверы, БД, ПО; обеспечивается объединение и структурирование данных с для упрощения поиска критических событий.
— Корреляция: поиск общих сигнатур, объединение событий в кластеры. Корреляция является типичной функцией SEM
— Оповещение: автоматизированное исследование коррелирующих событий и отправка оповещений о текущих нарушениях. Оповещение может отображаться в как консоли управления так и отправляться на email или по sms.
— Средства отображения (информационные панели): создание диаграмм и графиков помогающих обнаружить поведение отличное от стандартного.
— Совместимость: применение приложений для автоматизации сбора данных, формированию отчетности для адаптации агрегируемых данных к существующим процессам управления информационной безопасностью и аудита.
— Хранение данных: применение долговременного хранилища данных в историческом порядке для корреляции данных по времени и для обеспечения трансформируемости. Долговременное хранение данных критично для проведения компьютерно-технических экспертиз, поскольку расследование сетевого инцидента вряд ли будет проводиться в сам момент нарушения.

— Экспертный анализ: возможность поиска по множеству журналов на различных узлах; может выполняться в рамках программно-технической экспертизы.
— Задачи, которые решает система
— Оперативное обнаружение, реагирование и контроль обработки инцидентов ИБ.
— Возможность оперативного контроля состояния ИБ для высшего руководства компании.
— Создание единого центра мониторинга ИБ компании.
— Определение прав, обязанностей и разграничение зон ответственности персонала компании в области управления инцидентами ИБ.
— Мониторинг соответствия отраслевым стандартам: PCI DSS, IT Governance, NERC CIP и другим.

На рисунке 1 представлена типовая архитектура SIEM-системы

Рисунок 1. Типовая архитектура SIEM системы

2. Постановка проблемы

1.3 Источники данных SIEM-системы

SIEM служит для сбора и анализа данных. Эта система получает информацию из различных источников — таких, как:

- Access Control, Authentication. Применяются для мониторинга контроля доступа к информационным системам и использования привилегий.
- Системы предотвращения утечек. Данные о попытках внутренних утечек, нарушении прав доступа.
- Системы обнаружения и предотвращения вторжений. Передают информацию о атаках в сети, изменениях конфигурации сетевого оборудования и попытках доступа.
- Антивирусные приложения. Составляют отчеты о работе ПО, БД, внесения изменений в политики и конфигурации, вредоносном ПО.
- Журналы серверов и рабочих станций. Применяются для контроля доступа, обеспечения непрерывности, контроля соблюдения политик информационной безопасности.
- МСЭ. Сведения об атаках, вредоносном ПО.
- Сетевое активное оборудование. Используется для контроля доступа, аудита сетевого трафика.
- Сканеры уязвимостей. Данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры.
- Системы инвентаризации и asset-management. Поставляют данные для контроля активов в инфраструктуре и выявления новых.
- Системы веб-фильтрации. Предоставляют данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов.

1.4 Источники данных SIEM-системы

Рассмотрим существующие на рынке решения

Таблица 1.2 Сравнительный анализ существующих SIEM-систем

Наименование SIEM	Производитель	База индикаторов	Наличие сертификата ФСТЭК	Стоимость
1	2	3	4	5
MaxPatrol SIEM	Positive Technologies, Россия	Собственная, закрытая	№ 3734 до 12.04.2020	От 3 млн. руб.
IBM Qradar	IBM, США	Собственная, закрытая	№3354 до 02.03.18	От 3 млн. руб.
HP ArcSight	HP, США	Собственная, закрытая	№3605 до 12.08.2019	От 4 млн. руб.
SearchInform SIEM	SearchInform, Россия	Собственная, закрытая	Нет	От 1,7 млн. руб.
Security Capsule	ИТБ, Россия	Собственная, закрытая	№3649 до 09.11.2019	От 700 тыс. руб.
KOMRAD Enterprise SIEM	Эшелон, Россия	Собственная, закрытая	№3498 до 13.01.2019	От 900 тыс. руб.
RuSIEM	РуСИЕМ, Россия	Собственная, закрытая	Нет	От 600 тыс. руб.
AlienVault OSSIM	AlienVault, США	Собственная, открытая	Нет	бесплатно

Продолжение таблицы 1.2

Splunk Enterprise	Splunk, США	Собственная, закрытая	Нет	От 1 млн. руб.
RSA Netwitness Suite	RSA, США	Собственная закрытая	Нет	От 1,8 млн. руб.
McAfee SIEM	McAfee, США	Собственная, закрытая	№3353 до 18.02.18	От 3 млн. руб.

Из анализа рынка SIEM-систем видно, что большинство решений используют собственные базы индикаторов и не поддерживают подключение сторонних баз индикаторов компрометации.

Дороговизна SIEM-систем с закрытыми базами данных индикаторов, а также невозможность проверить достоверность таких баз данных являются проблемами, решение которых будет рассматриваться в данной статье

3. Разработка методики

Для создания базы данных компрометации возможно использовать открытые источники такие как www.alienvault.com; http://mirror1.malwaredomains.com/; http://malc0de.com/database/; и другие

Анализ информации из открытых источников позволяет выделить более 50 ресурсов, сведения которых могут быть использованы как описание показателей компрометации с разной степенью полноты и достоверности. [5]

Для формирования комплексной базы показателей компрометации определен набор характеристик источников информации:

- формат представления данных;
- способ получения доступа к данным;
- состав предоставляемых данных.

Таблица 2.1 Анализ открытых источников показателей компрометации

Адрес ресурса в сети Интернет	Формат представления данных	Способ получения доступа к данным	Состав предоставляемых данных
1	2	3	4
www.alienvault.com	CSV, OpenIOC, STIX	API, TAXII, agents, download	IP, DNS, hosts, e-mail, URL, URI, Хеши файлов: MD5, SHA1, SHA256, PEHASH, IMPHASH Правила CIDR Имя MUTEX Номер CVE

Продолжение таблицы 2.1

1	2	3	4
www.malware-domains.com/files/	XML, TXT	download	DNS
www.malwaredomainlist.com/mdl.php	TXT, CSV, RSS	download	IP, DNS
feodotracker.abuse.ch/blocklist/	TXT	download	IP, DNS
zeustracker.abuse.ch/blocklist.php	TXT	download	IP, DNS
malc0de.com/database/	XML, TXT	download	IP, DNS
www.spamhaus.org/bgpf/	TXT	download	IP
feeds.dshield.org/block.txt	TXT	download	IP
support.clean-mx.de/clean-mx/phishing.php	XML, TXT	download	IP, DNS, e-mail, URL
www.projecthoneypot.org	TXT	download	IP
www.nothink.org/honeypots.php	TXT	download	IP, DNS
www.iblocklist.com	TXT	download	IP
www.circl.lu/services/passive-dns/	TXT	REST API	IP, DNS
www.c1fapp.com	JSON, CSV	API, Python plugin	IP, DNS, URL, URI
www.talosintelligence.com/reputation_center	TXT	API, download	IP
hosts-file.net/	TXT	download	IP
www.phishtank.com/phish_search.php?page=3&active=y&verified=u	CSV, JSON, XML, PHP	download	URL
www.blocklist.de/ru/export.html	TXT	download	IP
osint.bambenekconsulting.com/feeds/	TXT	download	IP, DNS, URL
ransomwaretracker.abuse.ch/feeds/	TXT, CSV	download	IP, DNS, URL
urlhaus.abuse.ch	CSV, STIX	download, API	URL

Для реализации получения данных от сервиса Vulners возможно использовать Vulners REST API. Vulners REST API обеспечивает поиск в базе данных, получение информации о бюллетени безопасности по идентификатору, поиск общедоступных эксплойтов, получение уязвимостей и эксплойтов по имени и версии программного обеспечения, а также загрузку базы данных в формате CVE. Для загрузки базы данных CVE достаточно составить GET-запрос с нужными параметрами, ответ предоставляется в формате JSON.

Для получения базы показателей компрометации из AlienVault OTX, а также определения злонамеренных URL, IP, DNS будет использоваться OTX Python SDK API.

Для реализации последовательного синтаксического анализа информации в файлах формата TXT, CSV необходимонаписать скрипты на языке программирования PHP, основной задачей которых будет выделение IP и DNS из файла и занесение записи в БД.

Записи в базе данных компрометации будут содержать следующие данные:

– IP в сети интернет распространяющие вредоносное ПО;
– DNS - доменные имена узлов распространяющих вредоносное ПО;
– URL – адреса вредоносных страниц
– Страна
– Достоверность – количество повторений IP в различных источниках

Для хранения можно выбрать любую бесплатную современную СУБД, такую как: SQLite, MySQL, PostgreSQL

4. Результаты

Была разработана методика создания базы данных компрометации на основе информации из открытых источников для SIEM – системы, приведен список открытых источников показателей компрометации и планируемое содержимое базы данных компрометации.

5. Заключение

Большинство SIEM-систем используют собственные базы индикаторов и не поддерживают подключение сторонних баз индикаторов компрометации, не смотря на наличие большого количества открытых источников показателей компрометации. Вследствие этого на выявление и внесение в собственные базы разными решениями одних и тех же данных тратится большое количество времени и ресурсов. Автоматически пополняемая из различных источников база могла бы существенно сократить данные расходы

Список используемой литературы

[1] Алексеев Д.М., Иваненко К.Н.,Убирайло В.Н. Принципы Функционирования SIEM – Систем. Новая наука: Современное состояние и пути развития, 2016, 10(2), 154-155.

[2] ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

[3] ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования

[4] ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

[5] Емельянов Е.А., Антипов А.С. Самокаева Т.А. Анализ открытых источников показателей компрометации для формирования базы знаний SIEM-систем // Студенческая наука для развития информационного общества: сборник материалов VII Всероссийской научно-технической конференции. Часть I – Ставрополь: Изд-во СКФУ, 2018. – 544 с

List of references

[1] [Alekseev D.M., Ivanenko K.N., Cleaned V.N. Principles of Functioning SIEM - Systems. New science: The current state and ways of development, 2016, 10 (2), 154-155.

[2] GOST R ISO / IEC 27000-2012 Information Technology (IT). Methods and means of security. Information security management systems. General overview and terminology

[3] GOST R ISO / IEC 27001-2006. Information technology. Methods and means of security. Information security management system requirements

[4] GOST R 53114-2008 Information Security. Ensuring information security in the organization. Basic terms and definitions.

[5] Yemelyanov, EA, Antipov, AS Samokaeva, T.A. Analysis of open sources of indicators of compromise for the formation of a knowledge base of SIEM-systems // Student science for the development of the information society: a collection of materials of the VIIth All-Russian Scientific and Technical Conference. Part I - Stavropol: SKFU Publishing House, 2018. - 544 p

Защита шаблонов в биометрических системах аутентификации

Автор - Степанян Н.Э.
nerses_stepanyan@mail.ru

Автор – Минкина Т.В.
Кандидат технических наук, доцент кафедры ОТЗИ
n.min@mail.ru

Автор - Орел Д.В.
Кандидат технических наук, доцент кафедры ОТЗИ
kde.def@gmail.com

Степанян Н.Э. - Северо-Кавказский федеральный университет, Ставрополь, 355045, Россия
Минкина Т.В. - Северо-Кавказский федеральный университет, Ставрополь, 355055, Россия
Орел Д.В. – Северо-Кавказский федеральный университет, Ставрополь, 355035, Россия

Аннотация:

В данной статье были рассмотрены основные средства защиты шаблонов в биометрических средствах аутентификации. Были рассмотрены статистические и динамические средства аутентификации и такие их виды, как аутентификация по отпечатку пальца, по сетчатке глаза, по радужной оболочке глаза, по геометрии руки, по геометрии лица, по термограмме лица, по резонансу черепа, по голосу, по клавиатурному почерку, по рукописному почерку. Для каждого вида были выявлены особенности, преимущества и недостатки. Были рассмотрены способы кодирования шаблонов. Исследованы уязвимости средств аутентификации и атаки злоумышленников, рассмотрены средства, обеспечивающие защиту биометрических шаблонов. Исследованы условия и требования для создания схем защиты биометрических шаблонов. Рассмотрены существующие угрозы шаблонам, их уязвимости и ограничения. Были поставлены задачи, которые бы могли преодолеть ограничения при создании схем защиты. Рассмотрены принципы защиты биометрических шаблонов, их особенности, преимущества, ограничения и недостатки. Проанализировав данные, были предложены два метода генерации защищённого эскиза. Рассмотрен метод

позволяющий преодолеть ограничения, связанные с генерацией защищённого шаблона. Сделан вывод об эффективности алгоритмов, которые частично устраняют проблемы безопасности.

Abstract

This article discusses the basic means of protecting patterns in biometric authentication tools. Statistical and dynamic means of authentication and their types such as fingerprint authentication, retina authentication, iris authentication, hand geometry, facial geometry, face thermogram, skull resonance, voice, keyboard handwriting, handwriting were considered. Features, advantages and disadvantages were identified for each species. Ways of coding patterns were considered. Vulnerabilities of authentication means and attacks of malefactors are investigated, the means providing protection of biometric templates are considered. The conditions and requirements for the creation of protection schemes of biometric templates are investigated. The existing threats to templates, their vulnerabilities and limitations are considered. Tasks were set that could overcome the limitations in the creation of protection schemes. The principles of protection of biometric templates, their features, advantages, limitations and disadvantages are considered. After analyzing the data, two methods of generating a protected sketch were proposed. The method is considered to overcome the limitations associated with the generation of a protected template. The conclusion is made about the effectiveness of algorithms that partially eliminate security problems.

Ключевые слова: аутентификация, биометрические шаблоны, биометрические системы, средства, безопасность, биометрический сканер, данные, пользователь, злоумышленник.

Keywords: authentication, biometric templates, biometric systems, tools, security, biometric scanner, data, user, intruder.

В наше время обеспечение безошибочной проверки подлинности довольно важная проблема, ведь в связи с обширным развитием сетевых технологий мы повсеместно используем биометрические средства аутентификации.

Для подтверждения подлинности личности авторизующегося пользователя ведётся сравнение полученного шаблона с тем, который находится в базе шаблонов. И именно эти

шаблоны являются целью злоумышленников, поэтому необходимо обеспечивать достойную защиту для всех шаблонов из базы.

Перед тем, как приступить к описанию методов защиты шаблонов, стоит разобраться, что же такое биометрические системы аутентификации, какие виды систем существуют, а главное - какие существуют угрозы для этих шаблонов. [7]

Биометрические системы аутентификации – это такие системы, которые проводят процесс доказательства и проверки подлинности имени пользователя через предъявление им своего биометрического образа.[1]

Существует три основных метода аутентификации:

1. При помощи пароля.
2. При помощи ключей (предъявление физического носителя ключа)
3. Биометрическая аутентификация.

Принцип работы последнего метода мы и рассмотрим. Сначала система записывает образец при помощи датчика. После из образца извлекаются индивидуальные черты, которые система сохраняет в виде кода, как шаблон в базе данных. Во время аутентификации пользователь предоставляет ещё один образец, из которого извлекаются индивидуальные черты и сравниваются с имеющимся шаблоном.

Методы биометрической аутентификации делятся на два вида:

1. Статистические, которые основаны на распознавании физиологических черт человека, присущих ему от рождения до самой смерти, при условии, что эти черты не могут быть скопированы, украдены и потеряны.

2. Динамические, основанные на особенностях поведения, которые человек подсознательно демонстрирует во время какого-либо повседневного действия. [1]

Рассмотрим статистические методы.

1.1. По отпечатку пальца (дактилоскопия). Является самой широко распространённой технологией биометрической аутентификации. Использует папиллярные узоры, которые у каждого человека почти никогда не совпадают. Преимуществами являются лёгкость в использовании, удобство, быстрота, универсальность, ну а главное – относительная дешевизна, получаемая за счёт небольших размеров сканера. Всё это помогает использовать сканеры отпечатков пальца, как в бизнесе, так и в быту. К примеру, сканер отпечатков пальца можно встретить в ноутбуках, а также в каждом уважающем себя смартфоне. [1]

Сканеры отпечатков пальца делятся на оптические, полупроводниковые и ультразвуковые сканеры. Самыми дешёвыми и простыми в реализации являются оптические сканеры, поэтому они самые распространённые, хоть и имеют один большой недостаток (неустойчивы к муляжам, оторванным пальцам и т. п.). Самыми эффективными сканерами являются ультразвуковые, которые почти невозможно обмануть, так как они не только сканируют отпечаток пальца, но и регистрируют другие параметры. [2]

1.2. По сетчатке глаза. Надёжность этих сканеров полностью компенсирует их громоздкость и стоимость. Данный вид сканеров используется для защиты хранилищ, секретных документов, доступа в частные кабинеты. Для сканирования применяется

инфракрасное излучение низкой интенсивности, которое направлено через зрачок к сосудам на задней стенке глаза. Из отражённого полученного сигнала получают свыше нескольких сотен точек, которые образуют собой шаблон и сохраняются в базе данных.

В последних моделях сканеров инфракрасное излучение было заменено на лазер мягкого действия. В самых современных сканерах на выполнение процедуры тратится больше минуты, что является самым главным недостатком данного вида сканеров, ведь не каждый такое выдержит. [4]

1.3. По радужной оболочке глаза. В этом методе используется уникальность радужной оболочки глаза, которая начинает формироваться ещё до нашего рождения. А факт того, что у человека правый глаз отличается от левого глаза, делает данный метод одним из самых надёжных. Данная технология была создана для замены навязчивого сканирования сетчатки глаза, которая ко всему прочему может изменяться с возрастом, в то время как радужная оболочка остаётся прежней. [1]

Для получения индивидуальной записи на радужную оболочку направляется слабый свет, а чёрно-белая камера делает 30 записей в секунду. Затем одна из записей преобразуется, отбирая более двухсот точек, и записывается как шаблон в оцифрованном виде. Главным преимуществом является то, что вся процедура занимает несколько секунд. Некоторые модели сканеров могут изменять поток света, идущий от сканера, тем самым изменяя размер зрачка, отсутствие реакции будет свидетельствовать о том, что использовался поддельный глаз. [1]

1.4. По геометрии руки. Используется форма кисти и форма таких её параметров, как изгиб, толщина и длина пальцев, толщина и ширина тыльной сторон руки, расстояние между суставами, а также структура кости. В основном при сканировании используется комбинирование параметров руки и регистрация таких мелких деталей, как, например, морщины на коже. Однако данный метод не является надёжным, ведь к отказу в допуске могут привести ушибы и заболевания. [1]

Но, даже не смотря на это, данный метод довольно популярен. Дело в том, что аутентификации по геометрии рук довольно не занимает много времени, не доставляет никаких неудобств, нет зависимости от температуры, загрязнённости или влажности, а сам размер шаблона не занимает много места (9 байт). Для сканирования руку помещают на ровную поверхность и сканируют с помощью диодов, которые активизируются по очереди (для получения разных проекций), а затем строится трёхмерная проекция. [2]

1.5. По геометрии лица. Данный метод делится на 2D-распознавание лица, которое зашло в тупик и 3D-распознавание лица, чья надёжность сравнима со сканированием по отпечатку пальца. Для определения уникального шаблона используется от 12 до 40 отличительных элементов лица, и в первую очередь такие элементы, которые помогут справиться с изменениями лица, наличия маскировки и т. п. [2]

1.6. По термограмме лица. Самым устойчивым и почти неизменным признаком является изображение кровеносных сосудов. Путём их сканирования мы получаем термограмму, аутентификация по которой в плане надёжности сопоставима с аутентификацией по отпечаткам пальцев. Данная аутентификация способна различать лица

после пластических операций, при ношении масок, при старении и т.п. Из-за того, что качество аутентификации невелико, данный метод слабо распространён. [5]

1.7. Отдельно хотелось отметить один интересный метод аутентификации, который многим мог быть неизвестен – аутентификация по резонансу черепа. Принцип заключается в том, что в наушник, используемый пользователем, вставляется микрофон, который записывает и воспринимает эхо, которое звучит из черепа в ответ на звуки, передаваемые в ухо. Данный параметр является уникальным для каждого человека.

Теперь рассмотрим динамические методы.

2.1. По голосу. Главной особенностью является простота. Для аутентификации хватит лишь микрофона и звуковой платы (подключенного записывающего устройства). К преимуществам также относится удобство, а также возможность к скрытой аутентификации (пользователь будет не в курсе, а значит, что у злоумышленника будут проблемы).

Главной проблемой данного метода является то, что голос может измениться в зависимости от психологического состояния, здоровья, возраста. Кроме того, внешние шумы также могут помешать определить голос. Так как вероятность ошибки относительно высока, аутентификацию по голосу используются на объектах среднего уровня безопасности. Но стоит заметить, что у голосового распознавания есть большие перспективы в будущем. [4]

2.2. По клавиатурному почерку. Описывается скорость ввода, интервалы между нажатиями клавиш, время удержания клавиш, время удержания клавиш и т.п. Лучше всего подходит для аутентификации пользователей с удалённым доступом. Аутентификация проводится по двум способам: ввод старого пароля и ввод нового пароля. Эти способы включают режим включения и режим аутентификации. Главным минусом является то, что особенности написания могут меняться в зависимости от здоровья. [2]

2.3. По рукописному почерку. Этот метод основан на специфике движений руки во время написания подписи, с помощью специальных ручек или же чувствительных к давлению поверхностей. Можно выделить два способа аутентификации с помощью написания подписи: [2]

1) Анализ самой подписи, который проводится человеком или компьютером. Проводится сравнение подписей.

2) Анализ динамических характеристик написания подписи, который включает информацию о самой подписи, о временных и статистических характеристиках.

Минусом данного метода является изменяемость в зависимости от психофизического состояния.

Ну а теперь, когда мы изучили основные методы аутентификации, можно изучить и их уязвимости. Когда система не распознаёт реального пользователя, происходит отказ, а когда злоумышленник неверно идентифицируется в качестве авторизированного пользователя, то происходит вторжение. Причины таких сбоев подразделяют на естественные ограничения и атаки злоумышленников. [9]

Поговорим сначала о естественных ограничениях. Образцы, полученные во время аутентификации и идентификации, редко совпадают, из-за чего система может допускать ошибки 2 видов. Когда два образца, полученные от одного пользователя не совпадают,

происходит ложное несоответствие, и легитимный пользователь получает отказ в обслуживании. Когда два образца, полученные от разных пользователей, практически идентичны, то система объявляет о совпадении, и происходит ложное соответствие, вследствие которого происходит вторжение самозванца, которое носит название атака нулевого усилия. [3]

Теперь поговорим об атаках злоумышленников. Сбой в биометрических системах может произойти в результате инсайдерских утечек: вступление в сговор, халатность, мошеннические манипуляции, злоупотребление исключений. Сбой в системе могут вызвать атаки на пользовательский интерфейс или датчик, модули экстракции. К атакам, направленным на системные модули и их соединение, относятся трояны, “человек посередине” и атаки воспроизведения.[3]

Отдельное внимание заслужили атаки подделки на пользовательский интерфейс и утечка шаблонов из базы, так как они имеют наиболее негативные последствия. [6]

Атаки подделки представляют собой подделку биометрической черты, которую не получили от живого человека. Успешные атаки подделки подрывают фундаментальный принцип биометрической аутентификации, состоящий в том, что хоть сами биометрические признаки не являются секретом, но система защищена, так как признак привязан к живому пользователю. Поэтому было предложено немало методов определения живого состояния.

Утечкой шаблона из базы данных называют ситуацию, когда информация о шаблоне легитимного пользователя становится известна злоумышленнику, вследствие чего повышается опасность подделки путём обратного инжиниринга. И в отличие от украденного пароля, который можно легко поменять на новый, украденный шаблон нельзя заменить новым, так как он существует в единственном экземпляре. [8]

Более наглядно с уязвимостями биометрических систем можно ознакомиться на рисунке 1:

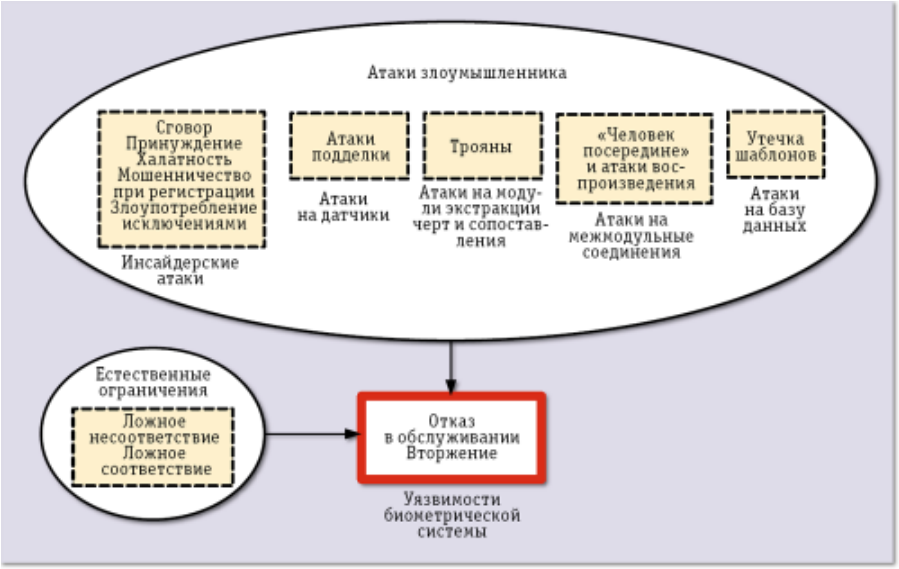

Рисунок 1. Уязвимости биометрических систем аутентификации.

Ну и наконец, получив необходимое представление о биометрических системах и угрозах, связанных с ними, мы можем приступить к вопросу защищённости шаблонов в этих системах, ведь это один важнейших факторов минимизации рисков безопасности.

Главной проблемой при разработке схем защиты биометрических шаблонов является достижение приемлемого компромисса между 3 требованиями: [3]

1) Необратимость. Восстановление биометрических черт из сохранённого шаблона или создание физической подделки должно быть для злоумышленника трудным путём.

2) Различимость. Точность аутентификации не должна быть ухудшена схемой защиты шаблона.

3) Отменяемость. Нужна возможность из одних и тех же биометрических данных создать несколько защищённых шаблонов, которые никак не будут связаны с этими данными, что позволит биометрической системе отзывать выдавать новые шаблоны в случае взлома базы данных. К тому же это позволит сохранять приватность данных о пользователе, в результате предотвращение сопоставления баз данных.

И при обеспечении безопасности ставится задача, которая должна найти компромисс между 3 этими требованиями. На сегодняшний день существует два принципа защиты биометрических шаблонов:[6]

- трансформация биометрических черт;
- биометрические криптосистемы.

При трансформации биометрических черт защищённый шаблон получается благодаря использованию необратимой функции трансформации к оригиналу. Обычно трансформация базируется на индивидуальных параметрах пользователя. Получается так, что во время процесса аутентификации система использует ту же трансформацию к запросу, происходит сопоставление уже для трансформированного образца.

В биометрических криптосистемах хранится лишь часть информации, которая была получена из биометрического шаблона (носит название защищённый эскиз или secure sketch). Этого эскиза не достаточно для восстановления изначального шаблона, но он содержит достаточное количество данных для восстановления биометрического шаблона, при условии наличия другого образца, который похож на исходный образец при регистрации. [10]

Такой эскиз получается путём связывания биометрического шаблона с криптографическим ключом. При этом защищённый эскиз нельзя назвать биометрическим шаблоном, зашифрованным стандартным методом. При обычной криптографии ключ расшифровки и зашифрованный шаблон являются разными единицами, а шаблон будет зашифрован тогда, когда будет зашифрован и ключ. Имея в наличии лишь защищённый шаблон нельзя, нельзя восстановить ни ключ, ни шаблон.

Исследователями было предложено два метода генерации защищённого эскиза:[6]

1)Нечёткое обязательство (fuzzy commitment). Позволяет защитить биометрические шаблоны, которые представлены в виде двоичных строк фиксированной длины.

2) Нечёткий сейф (fuzzy vault). Используется для наборов, которые представлены в виде наборов точек.

Сопоставление в схеме с трансформацией черт обычно происходит напрямую, к тому же возможна разработка функций трансформации, которые не меняют характеристики признаковисходного пространства. Но создать удачную функцию трансформации, которая бы была необратимой и терпимой к изменению биометрических черт, довольно сложно.
Так как представить биометрические черты в формате наподобие двоичных строк и наборов точек довольно сложно, одной из актуальных тем для исследования является разработка алгоритмов, преобразующих изначальный шаблон в эти форматы без потерь информации. [6]

Методы генерации защищённого шаблона имеют некоторые ограничения, в число которых входит неспособность генерировать много несвязных шаблонов из одного и того же набора биометрических данных. Один из способов, который позволяет преодолеть эту проблему – это применение функции трансформации черт биометрического шаблона до того, как шаблон будет защищён биометрической криптосистемой. Такое объединение трансформации с генерацией защищённого эскиза называется гибридным.
Биометрическое распознавание является наиболее надёжным методом аутентификации. Конечно, системы не являются абсолютно неуязвимыми, но ведутся исследования, которые помогут увеличить надёжность. Алгоритмы частично устраняют проблемы, но нужны улучшения перед тем, как применять их в реальных условиях.

Список используемой литературы

[1] http://www.biometrics.ru/news/metodi_biometricheskoi_identifikacii_sravnitelnii_analiz/

[2] https://www.osp.ru/os/2012/10/13033122/

[3] Шаров В. Биометрические методы компьютерной безопасности //"BYTE". –2005. –No 4. –С. 32–35.

[4] Климакин С.П., Петруненков А.А., Черномордик О.М. Эра биометрического общества. – Режим доступа: http: // www.gazeta.ru

[5] Анил К. Джайн, Катик Нандакумар, Биометрическая аутентификация: безопасность системы и конфиденциальность пользователя. Компьютер IEEE, ноябрь 2012 г., IEEE Компьютерная безопасность. С. 122-155.

[6] Kopytov V.V., Petrenko V.I., Tebueva F.B., Streblianskaia N.V. An improved brown's method applying fractal dimension to forecast the load in a computing cluster for short time series/Indian Journal of Science and Technology. 2016. Т. 9. № 19. С. 93909.

[7] Кузьменко В.В., Орёл Д.В. Анализ компонентов биометрической системы идентификации по трехмерным моделям лиц. В сборнике: Студенческая наука для развития информационного общества//сборник материалов IV Всероссийской научно-технической конференции: в 2-х томах. 2016. С. 142-144.

[8] Орел Д.В., Кузьменко В.В.Аналитический обзор биометрических методов распознавания лиц. В сборнике: Студенческая наука для развития информационного обществ//Сборник материалов III Всероссийской научно-технической конференции. 2015. С. 66-68.

[9] Тринкин М.Г., Орёл Д.В., Минкина Т.В. Ссовершенствование метода аутентификации пользователей информационных систем по клавиатурному почерку. В сборнике: Экономическое развитие регионов России в условиях трансформации информационной среды//Сборник научных статей по материалам Всероссийской научно-практической конференции. 2018. С. 184-188.
[10] Лагунов Н.А., Мезенцева О.С.Влияние предобработки изображений на качество обучения нейронной сети для их распознавания. Вестник Северо-Кавказского федерального университета. 2015. № 1 (46). С. 51-58.

Listofreferences

[1] http://www.biometrics.ru/news/metodi_biometricheskoi_identifikacii_sravnitelnii_analiz/
[2] https://www.osp.ru/os/2012/10/13033122/
[3] Sharov V. Biometric methods of computer security //"BYTE". -2005. - No. 4. - P. 32-35.
[4] Klimakin S. P., Petrunenkov A. A., Chernomordik O. M. Era of biometric society. - Access mode: http: // www.gazeta.ru
[5] Anil K. Jain, Kathik Nandakumar, Biometric Authentication: System Security and User Privacy. IEEE Computer, November 2012, IEEE Computer Society.P. 122-155.
[6] Kopytov V.V., Petrenko V.I., Tebueva F.B., Streblianskaia N.V. An improved brown's method applying fractal dimension to forecast the load in a computing cluster for short time series/Indian Journal of Science and Technology. 2016. Т. 9. № 19. С. 93909.
[7] Kuzmenko V. V., Orel D. V. Analysis of components of biometric identification system by three-dimensional models of persons in the collection: Student science for the development of information society//proceedings of the IV all-Russian scientific and technical conference: in 2 volumes. 2016. P. 142-144.
[8] Orel D. V., Kuzmenko V. V. Analytical review of biometric methods of facial recognition in the collection: Student science for the development of the information society//Proceedings of the III all-Russian scientific and technical conference. 2015. P. 66-68.
[9] Trinkin M. G., Orel D. V., Minkina T. V. Improving the method of authentication of users of information systems by keyboard handwriting. In the collection: Economic development of Russian regions in the transformation of the information environment / / Collection of scientific articles on the materials of the all-Russian scientific-practical conference. 2018. P. 184-188.
[10] Lagoonov N. Ah. Mezentseva O. S. influence of image preprocessing on the quality of neural network training for their recognition. Bulletin of the North Caucasus Federal University. 2015. No. 1 (46). P. 51-58.

ОЦЕНКА ПРИМЕНИМОСТИ ОТЕЧЕСТВЕННОЙ КРИПТОГРАФИИ В ПРОТОКОЛЕ MATRIX

Джамиев Н-М.Д.[1]
e-five@mail.ru

Стручков И.В.[1]
selentar@bk.ru

Тебуева Фариза Биляловна[1]
Доктор физико-математических наук, доцент
fariza.teb@gmail.com

[1] Северо-Кавказский федеральный университет, Ставрополь, 355035, Россия

Аннотация

Протокол Matrix позволяет обмениваться текстовыми сообщениями различного формата, файлами, осуществлять голосовые и видео звонки, хранить и передавать данные пользователей на различных серверах (децентрализованность). Данный протокол предоставляет программный интерфейс приложения, осуществляющий передачу сообщений в JSON формате. Для защиты передаваемой информации в протоколе Matrix существуют встроенные механизмы криптографической защиты, однако встроенные модули в реализации данной защиты используют стандарты шифрования несертифицированные в Российской федерации. Поэтому актуально внедрение отечественной криптографии для дальнейшего использования Matrix в отечественных защищенных программных комплексах. Целью данного исследования является оценка применимости отечественной криптографии в протоколе Matrix. В рамках исследования проведен анализ самого протокола Matrix, а именно структуры передаваемых объектов и их параметров, выделены наиболее логичные для защиты параметры, представлена принципиальная криптографическая модель для защиты передаваемых данных и способ задания

зашифрованных блоков в конечный JSON объект для передачи. Также, в рамках исследования произведено сравнение скорости работы криптографической функции хеширования «Стрибог» (длиной хеша 512 бит) с SHA-512 на входных данных различного размера.

Abstract

Matrix protocol allows exchanging text messages of various formats, files, making voice and video calls, store and transmitting user data on different servers (decentralization). This protocol provides an application programming interface that transmits messages in the JSON format. To protect the information transmitted in the Matrix protocol, there are built-in cryptographic protection mechanisms, however, the embedded modules in the implementations of this protection use encryption standards that are not certified in the Russian Federation. Therefore, the introduction of Russian cryptography for the further use of Matrix in Russian secure software packages is important. The purpose of this study is to assess the applicability of Russian cryptography in the Matrix protocol. The study analyzed the Matrix protocol itself, namely the structure of the transmitted objects and their parameters, highlighted the most logical parameters for protection, presented a basic cryptographic model for protecting the transmitted data and a method for specifying encrypted blocks to the final JSON object for transmission. Also, within the framework of the study, a comparison was made of the operation of the Stribog cryptographic hash function (512-bit hash length) with SHA-512 on input data of various sizes.

Ключевые слова: криптография, протокол Matrix, защищенный обмен сообщениями

Keywords: cryptography, Matrix protocol, secure messaging

1 Введение

Современные информационные технологии позволяют мгновенно обмениваться информацией, несмотря на огромные расстояния. Существует множество технологий и различных протоколов для обмена информацией, в частности, протоколы обмена сообщениями, позволяющие обмениваться информацией в удобном формате мессенджеров или чатов. Одним из таких протоколов является протокол Matrix, который выделяется среди

остальных следующими преимуществами: открытость спецификаций и программного кода (как клиентов, так и серверов), фактически неограниченные возможности по масштабированию, универсальность (независимость от реализаций, языка программирования и платформы) [1].

Однако, не всегда такие протоколы обеспечивают надежную защиту от перехвата и чтения передаваемой информации третьими лицами (которые не должны иметь доступ к данной информации). Так, согласно отчетам компании InfoWatch, в первой половине 2017 года зафиксировано в общем количестве утечек 7,78 млрд записей с персональными и платежными данными по всему миру [2].

Для защиты передаваемой информации в протоколе Matrix существуют встроенные механизмы криптографической защиты, однако встроенные модули в реализации данной защиты используют стандарты шифрования несертифицированные в Российской федерации [3]. Поэтому актуально внедрение отечественной криптографии для использования Matrix в отечественных программных комплексах.

2 Постановка задачи

В соответствии с целью данного исследования поставлены следующие задачи:

– изучить структуру передаваемой информации в протоколе Matrix;
– построить криптографическую модель для протокола Matrix.

3 Разработка методики

Протокол Matrix базируется на протоколе прикладного уровня HTTP и является открытым протоколом для мгновенного обмена сообщениями различного формата. Протокол поддерживает передачу сообщений несущих текстовую информацию, файлы, аудио, видео звонки. В качестве формата передачи сообщений используется формат JSON [4]. На рис. 1 показана модель OSI и расположение протокола HTTP (соответственно, и Matrix) в этой модели [5].

Рисунок 1. Протокол HTTP в сетевой модели OSI

Использование JSON в качестве контейнера для передачи данных и REST, как программного интерфейса, позволяют протоколу быть максимально универсальным и независимым от платформы или языка программирования. Таким образом, фактически все современные языки программирования и платформы поддерживают протокол Matrix.

Прежде чем перейти к криптографической модели, рассмотрим структуру протокола и контейнеров данных (JSON).

2.1 Структура передаваемой информации в Matrix

Основными сущностями в протоколе являются «Комната» (Room, далее комната), «Событие» (Event, далее событие) и «Пользователь» (User, далее пользователь). Каждая сущность «Комната» является родительской для сущностей типа «Событие». Отношение событий к комнатам показано на рис. 2. Таким образом, каждая комната является родительским объектом для всех событий, и сами пользователи также привязаны к комнатам (как участники) и могут генерировать события. Текстовые сообщения являются одним из подтипов событий в Matrix.

Для разделения типов объект в Matrix используется параметр type, со значениями в формате «t1.t2.tn», например, «m.room.message».

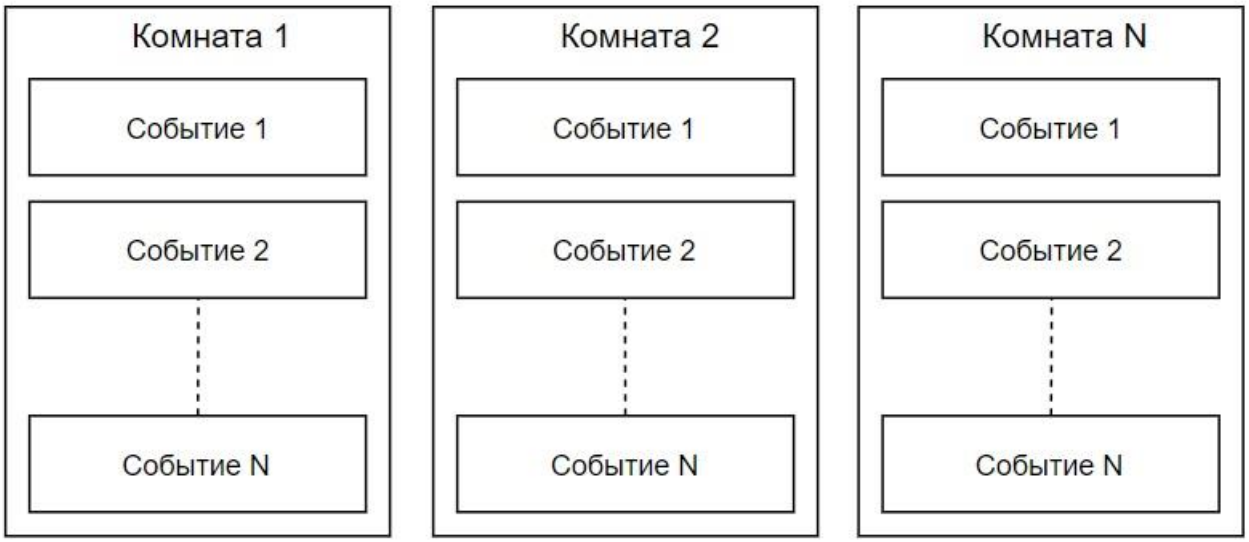

Рисунок 2. Логическая структура комнат в протоколе Matrix

Рассмотрим структуру событий. События в комнатах в протоколе Matrix могут иметь следующие типы:

- «m.room.message» – сообщение;
- «m.room.name» – изменение или создание нового имени для комнаты;
- «m.room.topic» – изменение или создание новой темы для комнаты;
- «m.room.avatar» – изменение изображения для комнаты;
- «m.room.pinned_events» – задание закрепленных событий для комнаты.

Из приведенного списка, наиболее важна защищенная передача событий типа «Сообщение». События данного типа в свою очередь делятся на различные подтипы (текстовые сообщения, аудиосообщения, файлы и т.д.), однако, в рамках начального этапа исследования поставлена задача криптографической защиты текстовых сообщений. Структура JSON объекта текстового сообщения приведена на рис. 3. Данный объект получен клиентов в результате запроса на получение новых событий к серверу (ненужная часть запроса-ответа от сервера не показана на рисунке).

Поля «body» и «formatted_body» содержат текст принятого сообщения в обычном и отформатированном виде, соответственно. Оба поля нуждаются в криптографической защите, так же, как и поля:

- «origin_server_ts» – метка, содержащая дату и время отправки сообщения с точностью до миллисекунд;
- «sender» – уникальные идентификатор отправителя;
- «event_id» – уникальный идентификатор сообщения;
- «age» – время с момента отправки сообщения.

```
{
   "content": {
      "body":"Здравствуйте! Вас беспокоит СКФУ",
      "format":"org.matrix.custom.html",
      "formatted_body":"Здравствуйте! Вас беспокоит <b>СКФУ</b>",
      "msgtype":"m.text"
   },
   "event_id":"$5640752234dPrZf:domain.com",
   "origin_server_ts":1432735924034,
   "room_id":"!jEsURKDJejlrcePyGS:domain.com",
   "sender":"@example:domain.com",
   "type":"m.room.message",
   "unsigned": {
      "age":1234
   }
}
```


Рисунок 3. JSON объект с текстовым сообщением

Разработка криптографической модели для защиты перечисленных полей позволит легко расширить ее и на остальные типы сообщений (или полей).

2.2 Криптографическая модель

В протоколе Matrix для авторизации используется система токенов доступа. Пользователь при аутентификации получает токен и, далее, в каждом запросе должен использовать его как идентификатор и секрет для авторизации.

Так как токен передается при каждом HTTP запросе, его использование в качестве источника ключей для криптографической защиты сообщений может быть небезопасным. Поэтому логично использование протокола Диффи-Хеллмана для создания общего с сервером вторичного ключа, который никогда не будет передан и будет привязан к токену авторизации. Таким образом, злоумышленник, даже получив токен, не сможет расшифровать сообщения от сервера [6, 7].

Упрощенная схема криптографической модели представлена на рис. 4. На рисунке используются некоторые обозначения и сокращения, а именно:

— «Кузнечик» – алгоритм симметричного блочного шифрования [8];
— «Стрибог-512» – алгоритм хеширования с длиной хеша 512 бит [9];
— «Сеансовый ключ, S_k» – вторичный ключ, упомянутый выше;
— «Данные (JSON)» – JSON объект, рассмотренный выше.

Выбор «Кузнечик» обоснован его новизной и улучшенными характеристиками выходного шифротекста (за счёт длины блока). На схеме видно, что в качестве режима

работы шифра используется режим сцепления блоков CBC, ввиду простоты и надежности данного режима.

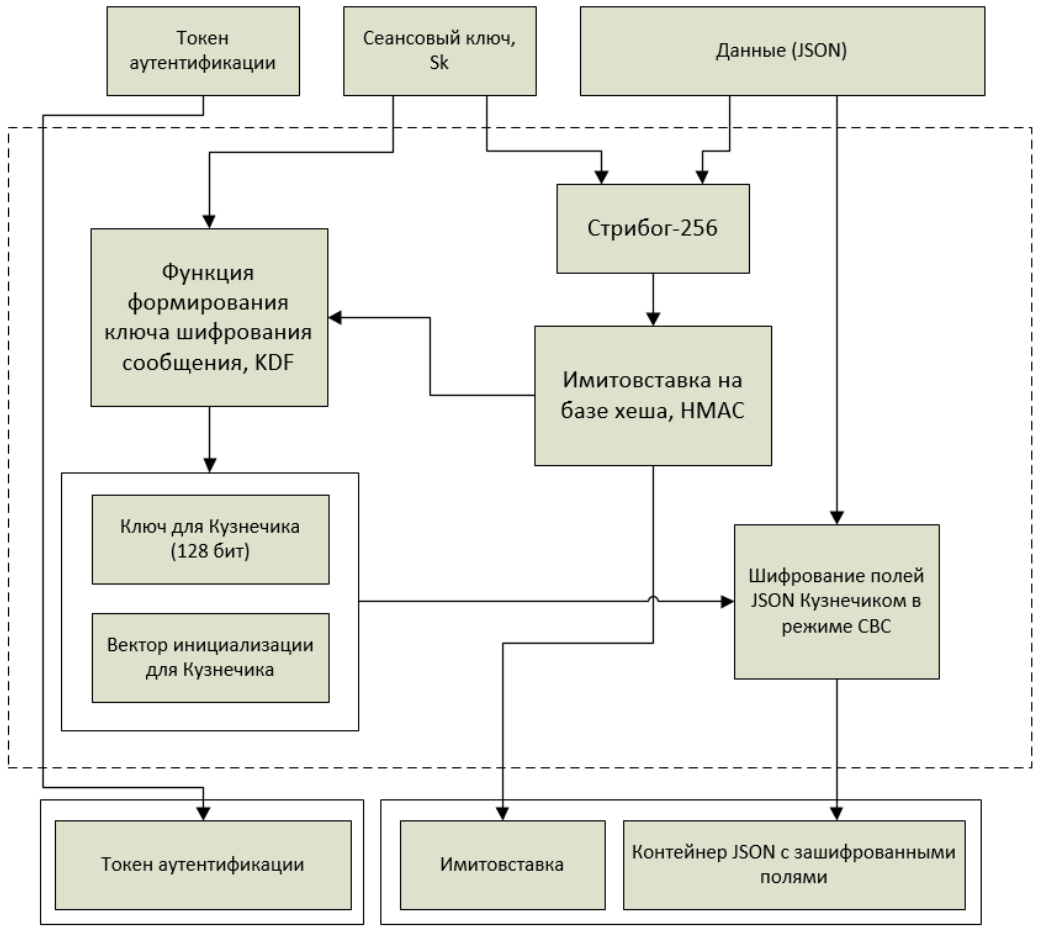

Рисунок 4. Упрощенная схема криптографической модели

Имитовставка выбрана на базе хеша, так как за счет хеширования повышается скорость генерации имитовставки, а сам результат более случаен. Для занесения зашифрованных данных обратно в объект JSON, предлагается преобразовывать зашифрованные блоки данных в формат Base64, который позволяет передавать и хранить зашифрованные данные в строковом виде.

4 Результаты

В рамках исследования проведен анализ протокола Matrix, а именно структуры передаваемых объектов и их параметров, выделены наиболее логичные для защиты параметры, представлена принципиальная криптографическая модель для защиты передаваемых данных и способ задания зашифрованных блоков в конечный JSON объект.

Также, в рамках исследования произведено сравнение скорости работы криптографической функции хеширования «Стрибог». Результаты сравнения с SHA-3 приведены на рис. 5.

Рисунок 5. Зависимость времени выполнения от размера входного сообщения для SHA-3 и «Стрибог»

Результаты сравнения показывают, что «Стрибог» имеет приемлемую скорость обработки для использования в реализации криптографической модели на рис. 4. Скорость работы хеш-функции является одним из решающих параметров при ее выборе, данный показатель будет влиять на скорость обработки запросов серверным модулем [10]. Так как полученные значения скорости работы приемлемы (незначительное замедление по сравнению в SHA-512), хеш-функцию «Стрибог» можно использовать при реализации представленной криптографической модели. Более того, исследования показывают, что при хорошей оптимизации (за счёт таблиц предвычислений), «Кузнечик» также можно значительно ускорить [11].

5 Обсуждение

Реализация полученной модели криптографической защиты позволяет защитить передачу данных в протоколе Matrix, используя стандарты шифрования, сертифицированные в Российской Федерации. Данная реализация также позволит построить на своей основе программное обеспечение для защищенной передачи данных в сети, которое будет обладать всеми преимуществами сторонних клиентов, построенных на протоколе Matrix и при этом соответствовать нормативным стандартам Российском Федерации. Оценка скорости работы «Стрибог» и анализ передаваемых JSON объектов показали возможность данной реализации.

6 Заключение

В данной работе проведен анализ структуры передаваемой информации в протоколе Matrix, а также построена криптографическая модель для данного протокола, позволяющая

построить на своей основе программное обеспечение для защищенной передачи данных в сети, которое будет обладать всеми преимуществами сторонних клиентов, построенных на протоколе Matrix и при этом соответствовать нормативным стандартам Российском Федерации. Оценка возможностей «Стрибог» и «Кузнечик», а также анализ структуры JSON объектов показали, что внедрение отечественной криптографии в протокол Matrix возможно и актуально.

Список используемой литературы

[1] Официальный сайт протокола Matrix [Электронный ресурс]. – Режим доступа: http://matrix.org

[2] Утечки данных. Россия. 2017 год // Аналитический центр InfoWatch. 2018 г.

[3] Nathan Willis. "Matrix: новая спецификация для интегрированного чата реального времени" [Электронный ресурс]. – Режим доступа: https://wikivisually.com/wiki/Matrix_(communication_protocol)

[4] D. Crockford. Json для нотации объектов JavaScript (JSON) – Internet Engineering Task Force, 2006.

[5] Sumit Kumar. Модель osi: обзор семи уровней компьютерных сетей. International Journal of Computer Science and Information Technology Research

[6] Ermoshina, Ksenia; Musiani, Francesca; Halpin, Harry. "Обзор сквозных протоколов обмена сообщениями". In Bagnoli, Franco; et al. Internet Science. INSCI 2016. Florence, Italy: Springer. pp. 244–254.

[7] Бабенко, Л.К. Криптографические методы и средства обеспечения информационной безопасности /Л.К. Бабенко, Е.А. Ищукова. – Таганрог: Таганрогский технологический институт ЮФУ, 2011. – 148с.

[8] ГОСТ Р 34.12-2015. Криптографическая защита информации. Блочные шифры

[9] ГОСТ Р 34.11-2012. Криптографическая защита информации. Функция хэширования

[10] Гавришев А.А., Бурмистров В.А., Осипов Д.Л. Оценка надежности программного обеспечения // Труды северо-кавказского филиала московского технического университета связи и информатики. Ростов-на-Дону: Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования "Московский технический университет связи и информатики", 2013. С. 304-305.

[11] Ищукова Е.А., Кошуцкий Р.А., Бабенко Л.К. Разработка и реализация высокоскоростного шифрования данных с использованием алгоритма кузнечик // AUDITORIUM. 2015. №4 (08). С. 80-88.

List of references

[1] The official website of the Matrix protocol [Electronic resource]. – Access Mode: http://matrix.org

[2] Data leaks. Russia. 2017 year // Analytical center InfoWatch. 2018
[3] Nathan Willis (2015-02-11). "Matrix: a new specification for federated realtime chat". LWN.net. Retrieved 2015-06-28.
[4] D. Crockford The application/json Media Type for JavaScript Object Notation (JSON) – Internet Engineering Task Force, 2006.
[5] Sumit Kumar.The osi model: overview on the seven layers of computer networks. International Journal of Computer Science and Information Technology Research
[6] Ermoshina, Ksenia; Musiani, Francesca; Halpin, Harry (September 2016). "End-to-End Encrypted Messaging Protocols: An Overview". In Bagnoli, Franco; et al. Internet Science. INSCI 2016. Florence, Italy: Springer. pp. 244–254.
[7] Babenko, L.K. Cryptographic methods and means of ensuring information security /L.K. Babenko, Ye.A. Ishchukova. – Taganrog: Taganrogskiy tekhnologicheskiy institut YUFU, 2011. – 148p.
[8] GOST R 34.12-2015. Cryptographic protection of information. Block ciphers
[9] GOST R 34.11-2012. Cryptographic protection of information. Hash function
[10] Gavrishev A.A., Burmistrov V.A., Osipov D.L. Software Reliability Assessment // *Trudy severo-kavkazskogo filiala moskovskogo tekhnicheskogo universiteta svyazi i informatiki.* [Proceedings of the North-Caucasian branch of the Moscow Technical University of Communications and Informatics] Rostov-na-Donu: North-Caucasian branch of the Order of the Red Banner of Labor of the federal state budgetary educational institution of higher education "Moscow Technical University of Communications and Informatics", 2013. p. 304-305.
[11] Ishchukova Ye.A., Koshutskiy R.A., Babenko L.K. Development and implementation of high-speed data encryption using the grasshopper algorithm // AUDITORIUM. 2015. №4 (08). p. 80-88.

СТРУКТУРНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА НА ПРИМЕРЕ КРИПТОВАЛЮТНЫХ СИСТЕМ

Ермолов И.В.[1]
Студент кафедры ОТЗИ
illya.ermoloff@gmail.com

Шутова Ю.А.[2]
Аспирант кафедры ОТЗИ
shutova.job@bk.ru

Тебуева Ф.Б.[3]
Доктор физико-математических наук, доцент
fariza.teb@gmail.com

[1,2,3] Северо-Кавказский федеральный университет, г. Ставрополь, 355009, Российская Федерация

Аннотация

В статье рассмотрены структурные особенности технологии распределенного реестра (блокчейн), связанные с ними уязвимости, риски, угрозы с позиции информационной безопасности не только как защиты конфиденциальности, целостности и доступности информации, но и как защищенности технологии от внутрисистемной преступной эксплуатации. Приведены способы обеспечения целостности, конфиденциальности и доступности. Технология распределенного реестра рассмотрена на примере криптовалюты – наиболее структурно приближенной, распространенной и полно изображающей все этапы функционирования технологии. Целью статьи является анализ вопроса защищенности технологии от манипуляций и атак злоумышленников, соотнесение рисков с мерами их снижения. На основе исследования сформирована реальная состоятельность перехода использующихся сегодня систем на блокчейн. Актуальность проводимого исследования диктуется постулируемой многочисленными пользователями технологии всеобъемлющей её применимостью на все правовые имущественные сферы жизни, а также революционность решения любых конфликтов в узлах системы неким децентрализованным консенсусом. В результате проведенного анализа сделаны комплексные выводы и проведена оценка состоятельности

использования технологии при имеющихся в ней на сегодняшний день уязвимостях.

Abstract

The following article investigates the structural features of the distributed ledger technology (blockchain), associated risks and threats from the perspective of information security not only as of an information's confidentiality, accessibility and integrity, but also as of the technology being secure from attackers and manipulators. Activities towards minimizing the risks will also be stated. The investigation will be executed on the example of cryptocurrency – architecturally closest, most wide-spread and fully depicting every functional step of the technology. Article aims to question blockchain security towards being attacked or manipulated, compare it with the possible measures on lowering the risk. Based on the results of investigation, the real advantages towards the existing systems are rated. Relevance of the study comes from numerous users of the technology proving its total applicability and perfection in solving any inner conflict with decentralized consensus. In the end of the article there the overall conclusions and the rating of using the technology with all its weak points are stated.

Ключевые слова: прикладные информационные технологии, технология распределенного реестра, блокчейн, информационная безопасность, инновационные технологии

Keywords: applied information technologies, distributed ledger technology, blockchain, information security, innovative technologies

Введение

Технология распределенного реестра - технология хранения информации, ключевыми особенностями которой является совместное использование и синхронизация цифровых данных согласно алгоритму консенсуса, географическое распределение равнозначных копий в разных точках по всему миру, отсутствие центрального администратора. Широкая же аудитория больше знакома с подвидом этой технологии - "блокчейном" (англ. Blockchain) – многофункциональной и многоуровневой информационная технологии, предназначенной для надежного учета различных активов. Блокчейн представляет собой технологию надежного распределенного хранения записей обо всех когда-либо совершенных транзакциях в виде цепочки блоков данных, объем которой постоянно растет по мере добавления новых блоков с записями самых последних транзакций, некая хронологическая база данных, в которой каждый блок неразрывно связан с временем его создания и содержимым, т.е. является функцией последних. Данные в связанных между собой в односвязный список блоках представляются последовательностью записей, которую можно дополнять. В основе архитектуры такой сети лежит пиринговая (англ. Peer-

to-Peer, P2P) система - каждый участник является узлом, хранящим весь актуальный массив данных и контактирующим с другими узлами. Узлы могут добавлять новые записи в конец списка и постоянно сообщают друг другу об изменениях списка.

Оригинально произошедшая из идеи пиринговой системы платежей [1] технология распределенного реестра оказалась совершенно самостоятельной и обособленной от “биткоинов” технологией.

Токенизация науки, акции, фонды [2], краудфандинг, страховые свидетельства, кадастровый учет [3], избирательные акции [4], медицина [5, 6] – технология распределенного реестра децентрализует право на обладание, обработку и редактирование всей связанной с некоторой сферой информации, и делает его продуктом общей договоренности между участниками. Все имущественные и неимущественные отношения в том или ином виде уже собраны в базы данных и находятся во владении конкретных лиц. И “блокчейн” не просто устраняет множество расходов на оплату труда лиц, заверяющих, контролирующих, заполняющих статьи данных, но и, теоретически, исключает возможность “неких владельцев” подделать данные, манипулировать ими или вовсе безвозвратно утратить. Любая операция в такой системе тесно сплетается с предыдущими: учет данных ведется с самого создания реестра, и появиться “из ниоткуда” ничто в ней не может (как исключение – операции эмиссии, но и они ограничены и строго контролируются всеми участниками системы). Сам же реестр, хранящий данные обо всех операциях за все время, не занимает много информационного пространства – фиксированные блоки информации, составляющие реестр, будучи верифицированными, представляют из себя лишь небольшой набор данных о предыдущих блоках и продукт хеш-функции с низкой коллизией, аргументами которой являются нужные данные о транзакциях внутри блока с временем создания блока. Эти данные всегда доступны для просмотра любому пользователю, а хотя бы малейшее изменение в содержимом блоков неизбежно повлечет за собой изменение остальных.

Информационный всплеск вокруг технологии блокчейн, поддерживаемый все новыми и новыми идеями её внедрения во все сферы нашей жизни, за последние годы прокатился и по России – что примечательно, ни много, ни мало, а по самым верхушкам. Многочисленные блоги, статьи, обзоры, форумы – трудно найти человека, который ничего слышал о революционных “биткоинах”, не менее трудно – человека, не сытого этим всем по горло. Однако сравнительно мало внимания в “популяризации” технологии уделяется аспекту безопасности. В данной статье рассмотрено, с чем это связано – с утаиванием ли уязвимостей блокчейна или, наоборот, защищенностью настолько абсолютной, что не подлежит и обсуждению.

Постановка задачи

Каким бы ни было будущее развитие технологии распределенного реестра, - общее признание ли, стагнация ли, - имеет смысл составить комплексную оценку существующих уязвимостей технологии и каналов реализации угроз её производительности. Уже на сегодняшний день амбиции технологии распределенного реестра (и блокчейн, в частности) впечатляют - ряд IT-специалистов превозносит её, как беспрецедентную инновацию с претензией на будущее господство в сфере экономики и права. Несмотря на это, до сих пор не было составлено ни одной полной, комплексной оценки защищенности технологии от взломов, мошенничества и манипуляций, основываясь на которой можно было бы сделать взвешенный вывод о состоятельности перехода существующих систем на блокчейн – этому и посвящено приведенное в статье исследование, объектом которого

является блокчейн как прикладная информационная технология, а предметом – аспекты безопасности его структурных компонентов и самой технологии в целом.

Анализ уязвимостей, угроз и средств их профилактики

Существующая технология блокчейн на сегодняшний день наиболее ярко представлена криптовалютными финансовыми системами, на примере которых, суммируя накопленный опыт пользователей и теоретические издержки [7], и будет рассмотрен вопрос уязвимости системы к атакам и ошибкам.

Под “угрозой” будем понимать: совокупность условий и факторов, создающих потенциальную или реально существующую опасность несанкционированного воздействия на информацию пользователей системы или иной её эксплуатации – как правило, в целях собственной выгоды.

Уязвимость системы определим, как свойство объекта информационной системы, которое может быть использовано злоумышленниками.

В соответствии с нормативными и методическими документами в сфере информационной безопасности [10] можно классифицировать угрозы, которым подвержены элементы системы блокчейн, по виду несанкционированного воздействия на информацию:

- угрозы конфиденциальности (хищение, утрата);
- угрозы доступности (блокирование);
- угрозы целостности (модификация, уничтожение, отрицание подлинности, распространение ложных сведений).

Так же необходимо классифицировать способы реализации вышеперечисленных угроз:

- аналитические (через анализ доступной информации);
- социальные (сговор, вербовка, обман);
- организационные (подделка носителей, доступ к ним);
- технические (искажение данных, проходящих по каналам связи, их мониторинг, сбои);
- программно-аппаратные (загрузка специального/вредоносного программного обеспечения, оборудования, перегрузка каналов связи).

Как было указано ранее, в качестве предмета системного анализа технологии распределенного реестра используется структура пиринговой платежной системы биткоин, функционирование которой полностью на ней основано. Тем не менее, также рассмотрены и альтернативы основных процессов, реализованные в поздних аналогах криптовалюты. Различные уязвимости проанализированы на каждом этапе функционирования системы.

Функционирование всей системы блокчейн, представляющей собой последовательное создание и скрепление между собой блоков с реестрами транзакций, можно свести к циклу образования одного блока.

На первом этапе рассмотрим образование структурной единицы блока – транзакции. У каждого пользователя сети имеется биткоин-адрес (открытый ключ), на который/с которого происходят переводы криптовалюты. Биткоин-адрес состоит из 26-35 буквенно-цифровых латинских символов (кроме 0, O, и I). В соответствие ему генерируется приватный, закрытый ключ, управляющий доступом к “кошельку” - на самом деле не хранящем никакой валюты, и являющимся лишь серией подписанных транзакций.

Помимо прямого физического доступа к носителям ключей (подсмотреть запись в блокноте или на стикере), ключи могут быть похищены и дистанционно, как правило, с

помощью вирусов. К примеру, вирус-троян CryptoStealer – программа, в функционал которой входит не только скрытое копирование содержащихся на компьютере файлов-реквизитов (для криптовалют содержатся, обычно, в файле wallet.dat), но и, в случае, если файл зашифрован и доступ к нему производится только с помощью пользовательского пароля, считывает и его через процессы программ работы с криптовалютой, "привязываясь" к функции определения длины строки strlen (библиотека msvcrt.dll), используемой кодом приложения биткоин при вводе пароля.

Кроме угрозы похищения "кошелька", уязвимостью обладает и сам процесс транзакции – злоумышленнику в таком случае нужен доступ не к кошельку пользователя, а к буферу обмена его устройства. Копирование реквизитов получателя в поле ввода занимает куда меньше времени, чем заполнение их ручным вводом – этим и пользуется, к примеру, вирус Trojan.Coinbitclip. Замаскированная под exe-файл карточной игры Hearthstone, программа производит мониторинг буфера обмена на наличие строк, похожих на номер биткоин-кошелька, и подменяет их на номер кошелька злоумышленника при оформлении перевода. Внимательный пользователь сразу заметит отличие нужного номера от введенного, остальные же безвозвратно отправят средства мошенникам.

В конце концов, средства злоумышленник может получить и обычным вымогательством – традиционные вирусы-локеры (например, CryptoWall), которые, попадая на устройство пользователя, быстро распространяются и с помощью специально сгенерированного ключа шифруют файлы ограничивая к ним доступ. Пользователю затем предлагается "спасти" файлы переводом некоторой суммы на кошелек вымогателя. Если пользователь выполняет требования в срок, программа дешифрует файлы и дальше устройство функционирует нормально, в противном случае цена дешифровки увеличивается [8].

Все описанные выше уязвимости легко устраняются избеганием посещения сомнительных сайтов, скачивания подозрительных файлов, установкой и постоянным обновлением антивирусного софта, а также использованием отдельных устройств исключительно для выполнения транзакций.

С биткоин-адресами пользователей системы связана аналитическая угроза анонимности, конфиденциальности личности пользователя, проистекающая из абсолютной прозрачности всех когда-либо совершенных в системе транзакций. Безусловно, при создании биткоин-кошелька от пользователя не требуется никаких персональных данных (как, например, при оформлении банковского счета). Кошелек – лишь некий пронумерованный узел системы. Изначальная, оригинальная информация о совершении пользователем транзакции (адрес отправителя, сумма, адрес получателя) передается от конкретного IP-адреса, но, будучи полученной несколькими пользователями, ввиду особенности peer-to-peer (P2P) архитектуры сети, распространяется дальше между узлами, каждый из которых, в свою очередь, пересылает нескольким другим. Конкретный узел сети хоть и может определить, с какого адреса пришла информация, но не может знать наверняка, создал ли он её или просто перенаправил.

Однако, имея в распоряжении некоторое число узлов, можно, проанализировав каналы поступления транзакции, с относительной точностью указать на её источник. Кроме того, почти ни одна операция обналичивания, депозита, покупки или обмена криптовалюты в сети не может быть проведена без хотя бы частичного раскрытия личности. Совершая покупку в интернет-магазине, как известно, безымянных реквизитов оплаты недостаточно – сервису необходимы сведения о том, кто совершил оплату, хотя бы для того, чтобы знать, куда доставить товар или кому отдать его в руки. Имея доступ к базе данных сервиса или обменника, злоумышленнику ничего не стоит связать биткоин-адрес с реальным

человеком. Пользователь может иметь даже несколько счетов – к примеру, один для получения, второй для хранения, а третий для расчетов биткоинами, - даже это не гарантирует полной анонимности от других пользователей и защиты от кластеризации (аналитического связывания адресов через транзакции). Мерой снижения возможных рисков для приведенных выше примеров могут выступать:

- использование специализированного программного обеспечения, скрывающего IP-адреса (Tor);
- создание нового адреса для каждой новой транзакции;
- использование специализированного программного обеспечения, “перемешивающего” транзакции между пользователями.

Итак, пользователь заполняет реквизиты перевода – сумму и получателя. Дальнейшие операции с переводом делятся на пять этапов:

1. Новая транзакция получает цифровую подпись совершившего её пользователя и отправляется всем узлам пиринговой сети, попадая в пул необработанных данных на узлах.
2. Специально выбранные узлы – майнеры – проверяют валидность транзакции и добавляют её в блок.
3. Системой выбирается майнер, наиболее “заинтересованный” в валидности всех транзакций в блоке.

Подходов к оценке степени вовлеченности в корректное заполнение реестра, в зависимости от реализации рисков потерь майнера, существует несколько:

- проверка работы (блоки создаются узлами с наибольшей вычислительной мощностью)
- проверка ставки (блоки создаются узлами с наибольшим балансом и риском потерь)
- делегированная проверка ставки (блоки создаются «делегатами», которых выбрало большинство пользователей)

В рамках статьи рассмотрим только первый, ставший в некотором роде “классическим”.

Проверка работы (англ. Proof-of-Work) – майнерам ставится сложная криптографическая задача поиска аргумента функции хэширования такого, что результат будет содержать в себе некоторое заданное системой количество нулей. “На страже” решения стоит несимметричный многобитовый алгоритм шифрования, для Bitcoin это – SHA-256. К слову, для приблизительной оценки надежности такого алгоритма защиты хэша от какой-либо технической угрозы конфиденциальности, чтобы найти парольную комбинацию, потребуется, в среднем, около двух в двести пятьдесят шестой степени попыток. Учитывая, что SHA-256 – функция криптографическая, подбор паролей осуществляется исключительно угадыванием. Однако угадывание такого пароля целиком – задача слишком сложная и долгая даже для современнейших суперкомпьютеров, поэтому системой сужается круг валидных комбинаций до наличия некоторого числа нулей в начале.

В то же время, полученную майнером “правильную” комбинацию, в контраст затраченной на её нахождение усилиям, очень легко может проверить любой пользователь сети – просто подставив выдаваемый за правильный аргумент в хэш-функцию.

Для майнеров сдерживающим фактором от мошенничества в этой ситуации является затраченная на поиск нужного хэша вычислительная мощность, которую те рискуют потерять при “вилке” с основным реестром. Стимулирующий фактор – наличие награды, соответствующей затраченной мощности.

Таким образом, существующие методы сдержек в системе блокчейн предписывают ответственным за создание блоков риск потерять полученный трудом ресурс – будь то электроэнергия, валюта или доверие. Это делает в разной степени осуществимой так называемую “атаку 51%”, которая будет рассмотрена ниже.

На данном этапе выбора ответственных узлов риск потери конфиденциальности есть только у подбираемого майнерами хэша, но способов, позволяющих его реализовать быстрее, чем это происходит в самой системе, на сегодняшний день нет.

Подобрав нужный хэш, майнер отправляет блок остальным узлам сети, получая на свой “счет” награду в соответствии со степенью вовлеченности в валидацию – особую эмиссионную транзакцию “из ниоткуда”.

Однако “выигрыш в лотерее” подбора аргументов хэш-функции - лишь условность, показывающая степень заинтересованности майнера, в какой-то степени, доверия к нему, а не его право определять истину в последней инстанции. Майнер, безусловно, может внести в блок ложную транзакцию – например, осуществить перевод средств со счета, на котором их нет - и “поставить свою печать”, но это еще не значит, что она будет одобрена узлами. Получив блок, остальные пользователи проверяют правильность записанных в нем транзакций в отношении их соответствия предыдущему блоку. Как уже было сказано, каждый блок тесно связан с предыдущим – чтобы внести в новый блок невозможный перевод, нужно сделать его возможным блоком ранее, а, чтобы сделать его возможным там, – еще блоком ранее, и так до самого нижнего, “генезис-блока”. Соответственно, децентрализованный консенсус между узлами сети достигается не в пользу сгенерированного мошенником блока, который признается системой бесполезным, как и весь проделанный майнером труд, и отклоняется. При таком развитии событий угрозы целостности реестра транзакций нет.

Отсюда делается несложный вывод: любая хоть сколько-нибудь рациональная атака злоумышленника на блокчейн-систему, во-первых, носит, своего рода, ретроспективный характер, а во-вторых, направлена на некие торговые отношения. Иными словами, просто “вписать” на свой счет в реестре некоторую сумму атакующий не может – система просто откажется принимать такой блок. В таком случае единственный способ злоумышленнику обогатиться и нечестно подзаработать в этой системе – заплатить за некий товар, получить его и “вернуться в прошлое”, когда средства были на его счете, но еще не на счете продавца.

Рассмотрим два случая проведения подобного мошенничества, называемого “двойной тратой”.

В первом, самом простом и близком к реальности случае, так же известном, как “атака-гонка”, злоумышленник одновременно отправляет по двум адресам одну и ту же монету – один из адресов принадлежит продавцу (к примеру, онлайн-магазину видеоигр), второй - злоумышленнику. Обе транзакции расходятся по реестрам, в одних действительной признается одна, в других – другая. Не дожидаясь подтверждения, продавец, получив сообщение о совершении перевода на его счет, отправляет злоумышленнику по электронной почте ключ игры, однако после генерирования следующих блоков выясняется, что большинством узлов, в конце концов, валидной признана операция перевода злоумышленником средств самому себе. Ключевой фактор в этой ситуации – терпение продавца, ведь достаточно образования и двух-трех блоков для раскрытия такой дешевой “вилки” системы. В то же время, обладая некоторыми большими вычислительными ресурсами, злоумышленник в силах некоторое время “убеждать” продавца в том, что тот получил средства. К слову, вскоре “случайная вилка” уже не может соперничать с оригинальной цепью и возвращается в изначальное русло.

Однако, что же случится, если недобросовестный “майнер” обладает ресурсами, внушительными достаточно, чтобы единолично генерировать блоки быстрее остальных пользователей? Не делая ничего “незаконного” вроде проведения заведомо ложных транзакций и совершая немногим больше пятидесяти процентов всех вычислительной работы системы, злоумышленник с большой (~50%) вероятностью обретает монополию на одобрение/блокирование любых транзакций других пользователей (проводить транзакции от лица других пользователей без их криптографической подписи, тем не менее, невозможно), получение 100% прибыли от майнинга (“эгоистичный майнинг”) а также контроль над собственными переводами (вышеупомянутая “двойная трата”).

Что примечательно, осуществление таких сценариев не просто деструктивно в отношении системы (обесценивание криптовалюты, если не полное её уничтожение), но и в высшей степени затратно, особенно для развитых систем с крупным фондом. К примеру, по разным оценкам, принимая во внимание цену на оборудование (берется самая низкая), затрачиваемые электроресурсы (расходующиеся как на хэш-вычисления, так и на охлаждение оборудования) и инфраструктуру, цены на проведение атаки 51 процента (только пятидесяти одного, даже не гарантирующего 100% успех) по разным данным варьируются от $1,006,000,000 до $8,538,842,878. По комплексной оценке [9], даже получая некую условную прибыль от майнинга, пусть, теоретически, не обесцененной криптовалюты, в размере 918 биткоинов ($5,531 на 15.11.2018) в сутки, сможет окупить затраты не раньше, чем через 5 лет. И это только самый оптимистичный сценарий, ведь пользоваться ненадежной, монополизированной и потерявшей свое главное свойство – децентрализованность – криптовалютой никто просто не будет. Делается вывод, что если такая атака и осуществима, то осуществима она:

1) Только силами некой очень влиятельной структуры, как например, государство;
2) Только с целью уничтожения вышеупомянутой криптовалюты.

Тем не менее, защитить блокчейн-систему от такой, на первый взгляд, абсурдной атаки просто невозможно. Причем, невозможно не только потому, что ничто в нашем мире, в принципе, нельзя защитить от влияния неограниченного капитала (как следствие, и власти), но и потому, что уязвимость заложена в самой природе постулируемой блокчейном договоренности, консенсуса. Пятьдесят один процент – и есть большинство, устанавливающее “правила игры”. По достижении консенсуса между узлами сети блок окончательно вносится в реестр.

Обсуждение

Подводя итоги, проведем оценку всех уязвимостей технологии распределенного реестра. За каждым пользователем закреплено его место в системе, доступ к которому уже сейчас, при должной аккуратности пользователя, не требующей сравнительно больших затрат времени или денег, заполучить просто невозможно. Более того, если злоумышленник и проводит некие несанкционированные действия от лица других пользователей, отследить их без труда можно на уровне крупной структуры (например, государства), но никак не на уровне обычного пользователя. Реестр всех операций находится в общем доступе, но всё, что необходимо знать пользователю – это то, что реестр валиден и неправомерных операций в нем нет (что регулируется на техническом уровне). При желании же можно отследить полную историю каждого расчетного элемента системы от самого его создания – даже “разделяясь” на доли или поступая в транзакцию совместно с другим элементом, он сохраняет привязанность к своему “дереву”.

Атаки на систему теоретически возможны, но требуют крайней организованности и влиятельности от атакующих, что исключает случайные глобальные конфликты между узлами. К слову, даже при успешной атаке, система все равно имеет возможность продолжать функционировать в своей собственной “вилке”. В качестве затруднения проведения подобных атак технология вводит собственные системы сдержек и поощрений – ответственным за внесение в реестр транзакций пользователям значительно выгоднее поддерживать здоровое функционирование системы. По сути, рисковать, таким пользователям просто не ради чего – любая захватническая деятельность в блокчейне деструктивна. Небольшая выгода от этой деятельности может быть достигнута в предельно краткосрочной перспективе, но никак не в среднесрочной или долгосрочной.

Профилактика такой атаки очень проста – во-первых, изолировать систему от внешнего воздействия (как, например, покупка блокчейн-валюты за наличные деньги), во-вторых, не допустить сосредоточения значительного объема ресурсов системы в одних руках, т.е. централизации, что возможно только при активном, динамичном обороте этих ресурсов между пользователями без их застаивания, здоровые заработок и трата, а также активная вовлеченность пользователей системы в качественный оборот.

Заключение

Таким образом, при описанных выше уязвимостях и при имеющихся на сегодняшних день препятствиях идеальному функционированию, технология распределенного реестра уже сейчас готова предложить множество решений, нивелирующих колоссальные статьи расходов в области экономики и финансов, избирательных акциях, науке и других сферах деятельности, использующих разные виды заверений, отчетностей и свидетельств правообладания, при этом делая эти сферы абсолютно прозрачными и устойчивыми к ошибкам и махинациям. Очевидно, что снятие миллионов и миллиардов расходов вкупе с надежностью и открытостью системы – очень заманчивая перспектива для целого ряда сфер нашей жизни.

Технология блокчейн, безусловно, имеет большой потенциал, но и знать наверняка, как себя поведет такая система в конкретной сфере и на конкретном этапе развития невозможно. Аппарат системы, её идейный ключ, впечатляют своей революционной природой, ведь, по сути, технология обеспечивает полную автономность оборота денег и активов. Тем не менее, на текущем этапе технологического и правового развития внедрение технологии не представляется возможным.

Список используемой литературы

[1] Nakamoto S. A Peer-to-Peer Electronic Cash System // Bitcoin. -URL: https://bitcoin.org/bitcoin.pdf; Перевод статьи Сатоши Накамото. Биткоин: цифровая пиринговая наличность // Coinspot. URL: http://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/.

[2] Ali R., Barrdear J., Clews R., Southgate J. The economics of digital currencies. Bank of England Quarterly Bulletin, 2014, vol. 54, no. 3, pp. 276-286. URL: http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3dig italcurrenciesbitcoin2.pdf.

[3] Применение блокчейн-технологий в информационных системах в сфере кадастрового учета и регистрации прав на недвижимое имущество. Цыпкин

Ю.А., Кудряшов Ю.Н. Землеустройство, кадастр и мониторинг земель. 2018. № 4 (159). С. 38-42.

[4] “Как голосование на блокчейне находит свое применение в политике и бизнесе” [Электронный ресурс] URL: https://geektimes.ru/company/281122/.

[5] Healthcare rallies for blockchains. Keeping patients at the center. IBM Institute for Business Value. 2017. Available from: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03790USEN.

[6] Unuvar M. Blockchain momentum rallies healthcare. IBM Blockchain: Blockchain in Healthcare. 2017 Jan 06. Available from: https://www.ibm.com/blogs/blockchain/2017/01/blockchain-momentum-rallies-healthcare.

[7] Тищенко Е.Н., Строкачева О.А. Оценка параметров надежности защищенной платежной системы в электронной коммерции. Вестник Ростовского государственного экономического университета (РИНХ). 2006. № 2 (22). С. 115-122.

[8] Ажмухамедов Искандар Маратович. Синтез управляющих решений в слабо структурированных плохо формализуемых социотехнических системах // УБС. 2013. №42. С. 29-54.

[9] Cost of a 51% attack URL: https://gobitcoin.io/tools/cost-51-attack/

[10] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) "Об информации, информационных технологиях и о защите информации"

List of references

[1] Nakamoto S. A Peer-to-Peer Electronic Cash System // Bitcoin. -URL: https://bitcoin.org/bitcoin.pdf; Перевод статьи Сатоши Накамото. Биткоин: цифровая пиринговая наличность // Coinspot. URL: http://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/.

[2] Ali R., Barrdear J., Clews R., Southgate J. The economics of digital currencies. Bank of England Quarterly Bulletin, 2014, vol. 54, no. 3, pp. 276-286. URL: http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3dig italcurrenciesbitcoin2.pdf.

[3] Application of blockchain technologies in information systems in the sphere of cadastral account and registration of rights to real estate Tsypkin Yu.A., Kudryashov Yu.N. Land management, cadastre and land monitoring. 2018. No. 4 (159). Pp. 38-42.

[4] How voting on the blockchain finds its application in politics and business [Electronic resource] URL: https://geektimes.ru/company/281122/.

[5] Healthcare rallies for blockchains. Keeping patients at the center. IBM Institute for Business Value. 2017. Available from: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03790USEN.

[6] Unuvar M. Blockchain momentum rallies healthcare. IBM Blockchain: Blockchain in Healthcare. 2017 Jan 06. Available from: https://www.ibm.com/blogs/blockchain/2017/01/blockchain-momentum-rallies-healthcare.

[7] Tishchenko E.N., Strokacheva O.A. Evaluation of the reliability parameters of a secure payment system in e-commerce. Bulletin of the Rostov State Economic University (RINH). 2006. № 2 (22). Pp. 115-122.

[8] Azmuhamedov Iskandar Maratovich. Control of badly formalizable and poorly structured social engineering systems // Large-Scale Systems Control, 2013, №42. P. 29-54.

[9] Cost of a 51% attack URL: https://gobitcoin.io/tools/cost-51-attack/

[10] Federal law 27.07.2006 N 149-ФЗ (red. et. 19.07.2018) "Of information, information technologies and information security"

АНАЛИЗ МИРОВОЙ ТЕНДЕНЦИИ РОСТА КИБЕРУГРОЗ НА ОСНОВЕ ЛИНЕЙНОЙ АППРОКСИМАЦИИ СТАТИСТИЧЕСКИХ ДАННЫХ ОБ АТАКАХ

Пижевский Д.Е.[1]
Dimapizhevskii@mail.ru

Антонов В.О.[1]
Ant.vl.02@gmail.com

Заволокина У.В.[1]
zzeseftt@yandex.ru

Унтевский Н.Ю.[1]
untewsky@yandex.ru

Тебуева Ф.Б.[1]
Доктор физико-математических наук, доцент
fariza.teb@gmail.com

[1] Северо-Кавказский федеральный университет, Ставрополь, 355009, Российская Федерация

Аннотация

В статье рассмотрены основные типы киберугроз на основе данных за ноябрь 2018 года «Лаборатории Касперского». Приведены потенциально вредоносные средства воздействия на персональные носители информации. Актуальность заключается в изменении количества киберугроз каждый день, что обязывает анализировать эти изменения для предотвращения утечки конфиденциальной информации. Целью статьи является выявлении наиболее прогрессивных киберугроз, для их подавления. По итогам анализа были выбраны самые развивающиеся киберугрозы по типам угроз: локальная угроза, сетевые атаки, веб-угрозы, уязвимость, спам. Практическая часть заключается в использовании предложенного метода для анализа изменения количественного значения киберугроз для разработки рекомендательных мер по защите информации. Для повышения точности определения аналитической зависимости изменения количества угроз возможно использование предлагаемого подхода на большем промежутке статистической выборки.

Abstract

The article describes the main types of cyber threats based on the data for November 2018 of Kaspersky Lab. Potentially harmful means of influence on personal data carriers. The urgency is to change the number of cyber threats every day, which makes it necessary to analyze these changes to prevent the leakage of confidential information. The purpose of the article is to identify the most progressive cyber threats for their suppression. According to the results of the analysis, the most developing cyber threats were identified by a threat level: local threat, network attacks, web threats, vulnerability, and spam. The practical part is to use the proposed method to analyze changes in the quantitative value of cyber threats to develop recommendations for the protection of information. To increase the level of analyticity of the change in the number of threats, you can use the proposed approach over a larger interval of statistical sampling.

Ключевые слова: киберугроза, уязвимости, локальные угрозы, веб-угрозы, сетевые атаки, спам, кибербезопасность.
Keywords: cyber threat, vulnerabilities, local threats, web threats, network attacks, spam, cybersecurity

1. Введение

Киберугроза – это несанкционированный доступ или угроза вредоносного доступа в виртуальное пространство для получения экономических, политических, социальных и других целей. Киберугрозы воздействуют на компьютер, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака, обычно, поражает носителя данных, который предназначен для их хранения, обработки и передачи личной информации пользователя.

Проблема обеспечения кибербезопасности является глобальной проблемой, с которой сегодня сталкивается каждое государство с прогрессивными информационными технологиями. Таким образом анализ тенденций роста киберугроз является необходимым инструментом информационной безопасности [1].

Целью данной статьи является анализ мировой тенденции роста киберугроз на основе линейной аппроксимации статистических данных лаборатории Касперского об атаках за ноябрь 2018 г. [2].

2. Постановка задачи

Для достижения поставленной цели исследования перед автором стоит задача является расчета и анализа изменения синусов углов наклона линейной регрессии, аппроксимирующей статистические данные по типам вредоносной активности в мире.

Под вредоносной активностью понимается любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ [3].

Начальные данные представлены статистикой по следующим видам вредоносной активности, локальные угрозы, веб-угрозы, сетевые атаки, уязвимости, спам.

Основным объектом изучения является статистика киберугроз, которая разрабатывается и поддерживается «Лабораторией Касперского», позволяющая в режиме реального времени получать статистику об информационных угрозах во всём мире. В данной статье рассматривается статистика за ноябрь 2018 года [2].

3. Виды киберугроз

Локальные угрозы – это дистанционное фотографирование; внедрение и использование компьютерных вирусов; использование программ-ловушек; включение в библиотеку программ специальных блоков типа «Троянский конь»; Статистика локальных угроз по всему миру представлена на рисунке.

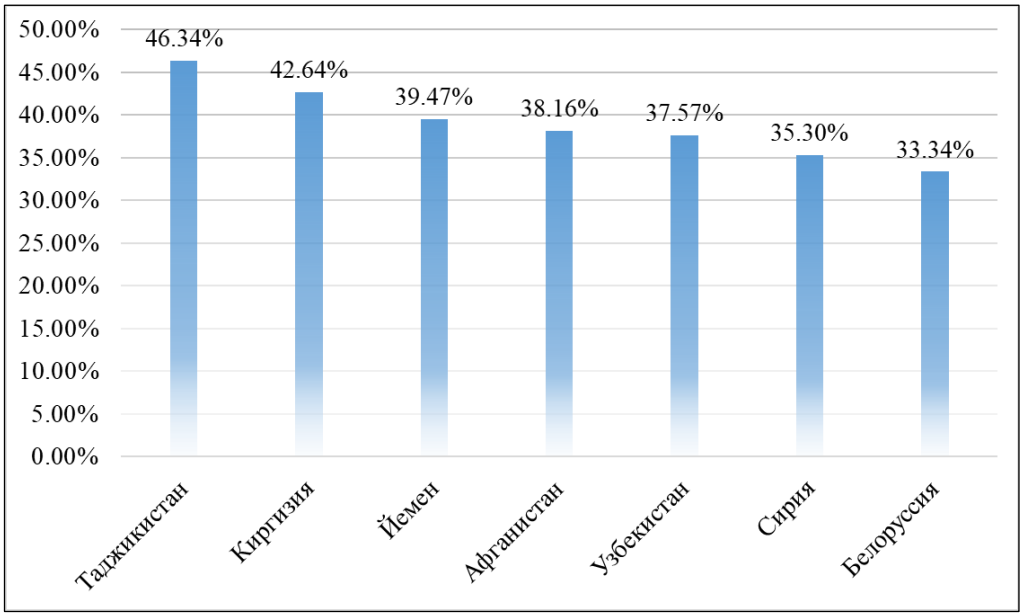

Рисунок 1. Статистика количества локальных угроз

Как показывает статистика, страной с самым высоким уровнем интернет-инцидентов в прошедшем месяце является Таджикистан. Более 46% местных пользователей антивирусных продуктов «Лаборатории Касперского» подвергались в третьем квартале риску заражения, пытаясь перейти на вредоносный сайт. В тройку лидеров вошли еще две азиатские страны Киргизия и Йемен, набравшие около 40% срабатываний антивируса. Из европейских стран риск заражения выше всего в Беларуси (33,34%).

На рисунке 2 изображен график изменения количества локальных угроз по данным Лаборатории Касперского с 01.11.2018 по 30.11.2018.

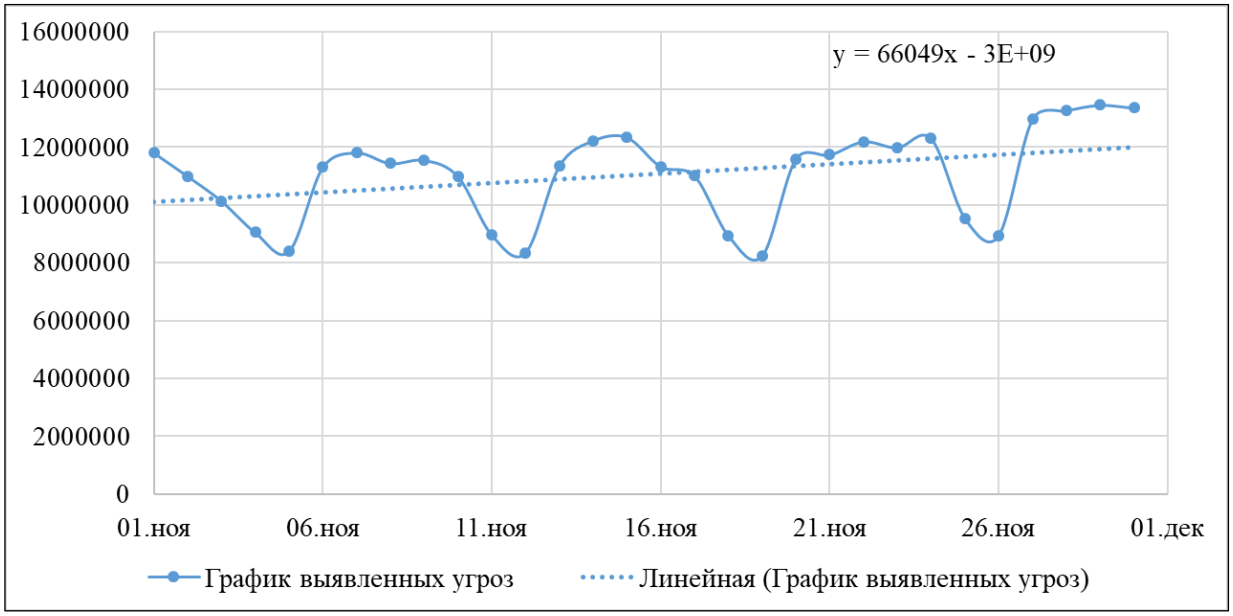

Рисунок 2. График изменения количества локальных угроз

Для последующего анализа построим тренд графика, который показывает, как быстро происходит рост количества локальных угроз. Обратим внимание на уравнение тренда, которое позволит с наибольшей точностью построить линейную зависимость изменения локальных угроз и рассчитать угол наклона линейной регрессии.

Веб-приложения всё больше пользуются популярностью во всех сферах деятельности человека и требуют конфиденциальных данных для их использования, что провоцирует ряд проблем в области безопасности, создавая веб-угрозы.

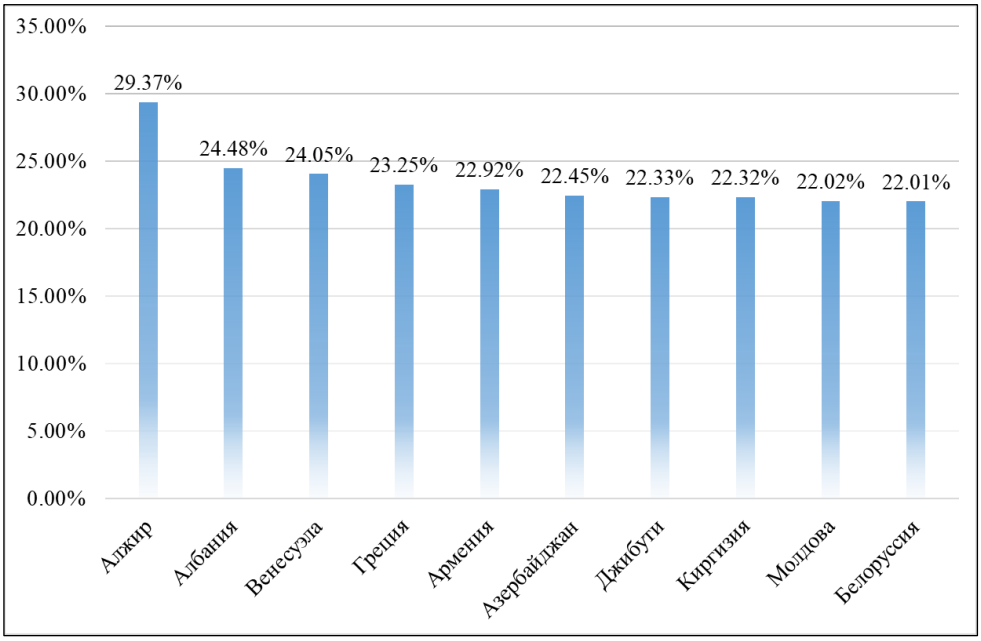

Рисунок 3. Статистика количества веб-угроз

Топ угроз: Trojan.Script.Generic (50,14%); Trojan.Script.Miner.gen (29,54%); Trojan-Clicker.HTML.Iframe.dg (2,76%); Trojan.Script.Agent.gen (1,82%); Trojan-Downloader.JS.Inor.a (1,7%).

По данным статистики наблюдаем, что Алжир лидирует среди других стран по количеству веб-угроз, помимо этого весь топ угроз занимают троянские программы, которые под видом легального программного обеспечения проникают в компьютер и производит утечку информации. Именно поэтому к веб-угрозам надо отнестись с особым вниманием, ведь заметить их крайне сложно.

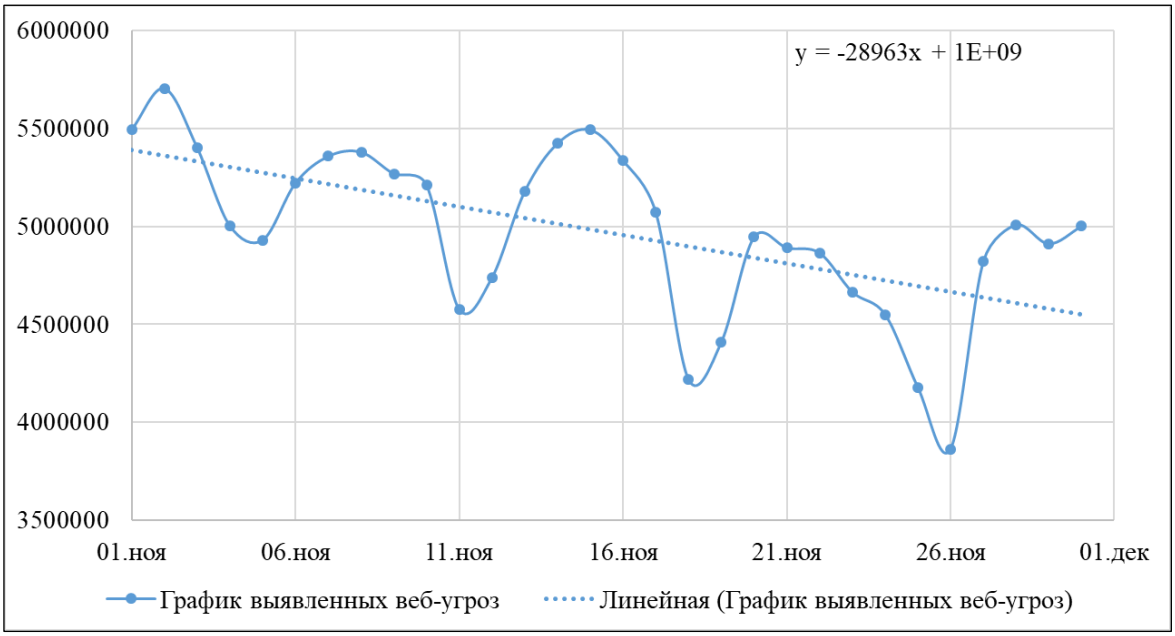

Рисунок 4. График изменения количества веб-угроз

Построив график изменения количества веб угроз и его тренд, мы получили линейное уравнение, которое даёт нам возможность отдельно анализировать линейное уменьшение количества веб-угроз.

Сетевые атаки - это информационное разрушающее воздействие на распределённую вычислительную систему (ВС), осуществляемое по каналам связи.

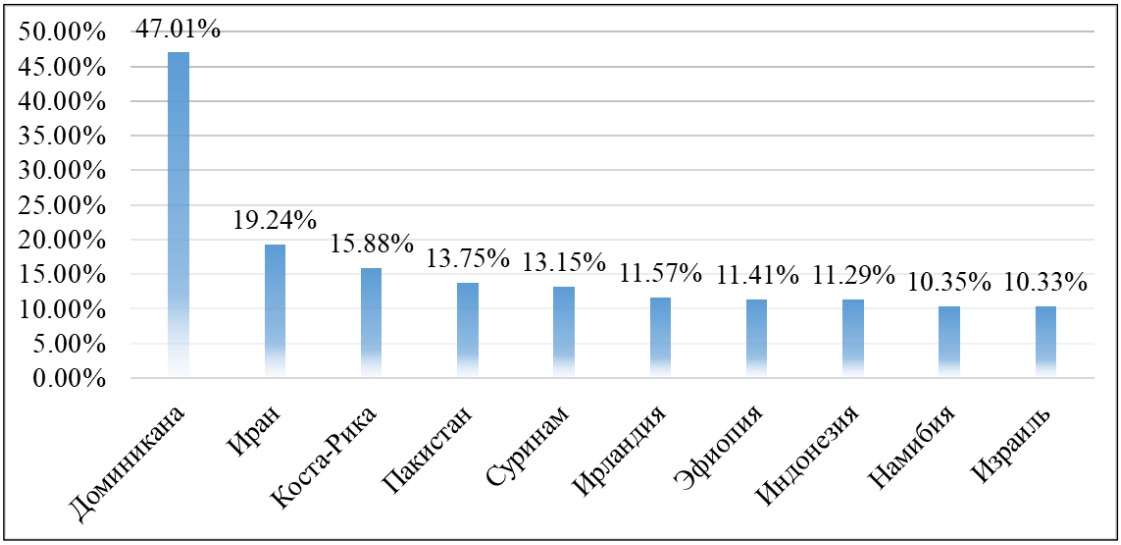

Рисунок 5. Статистика количества сетевых атак

Топ вирусов: Intrusion.Win.MS17-010.o (15,14%); Intrusion.Win.MS17-010.p (3,8%); Bruteforce.Generic.Rdp.a (2,36%); Bruteforce.Generic.Rdp.d (1,64%).

На основе этой статистики можем заметить, что в ноябре значительно изменился состав лидирующих стран. В прошедшем третьем квартале первое место занимали Китай (78%), который сейчас опустился на 17 место (8,75%). Также в прошлом квартале впервые ТОП-10 покинула Южная Корея, на данный момент ситуация не меняется.

Среди топа угроз выделяются такие типы вирусов как Intrusion.Win.MS17-010 и Bruteforce.Generic.RDP, рассмотрим каждый из них:Атака Intrusion.Win.MS17-010.* нацелена на компьютеры под управлением Windows и реализуется в попытке эксплуатировать уязвимости протокола SMB

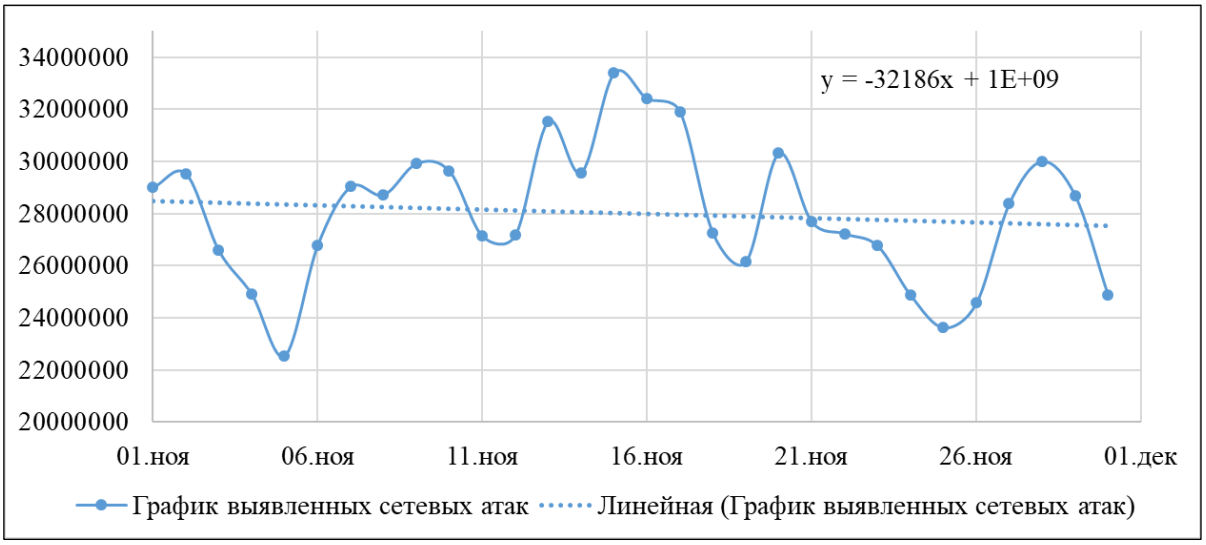

Рисунок 6. График изменения количества сетевых атак

Построив график изменения количества сетевых атак и его тренд наблюдаем небольшое уменьшение угла наклона линейной аппроксимации, о котором будет говорить далее.

Уязвимости – это любые факторы, делающие возможной успешную реализацию угроз. Поэтому для оценки уязвимостей необходимо идентифицировать существующие механизмы безопасности и оценить их эффективность [4]. Другими словами, уязвимости представляют собой слабости защиты, ассоциированные с активами организации.

Топ стран по доле атакованных пользователей:

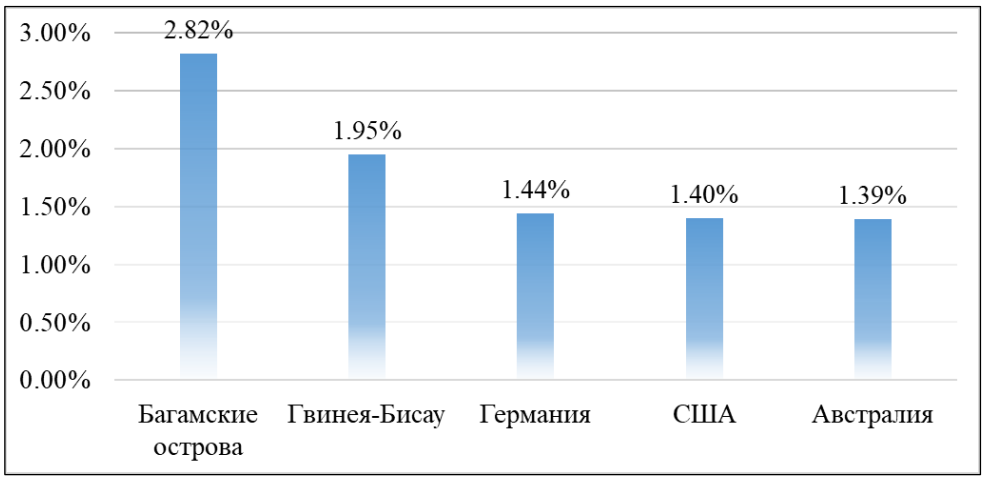

Рисунок 7. График изменения количества уязвимостей

Топ вирусов, воздействовавших за прошедший месяц на уязвимости: Exploit.Win32.CVE-2017-11882.gen (20,82%); Exploit.Win32.CVE-2015-1701 (20,82%); Exploit.Win32.ShadowBrokers.ae (8%); Exploit.Script.Blocker (5,12%); Exploit.Script.Generic (3,16%).

Чаще всего мошенники применяли для нападения уязвимости в Microsoft Office, а также бреши в браузерах [5]. Большинство атак, эксплуатирующих баги программных продуктов, в третьем квартале 2018 года строилось на ошибках пакета Office. И из статистики на момент ноября мы видим, что по-прежнему желанной целью злоумышленников остаются пользователи, не устанавливающие вовремя апдейты безопасности. Например, уязвимость CVE-2017-11882 была закрыта Microsoft еще год назад, однако до сих пор нередко применяется киберпреступниками для проникновения на целевое устройство.

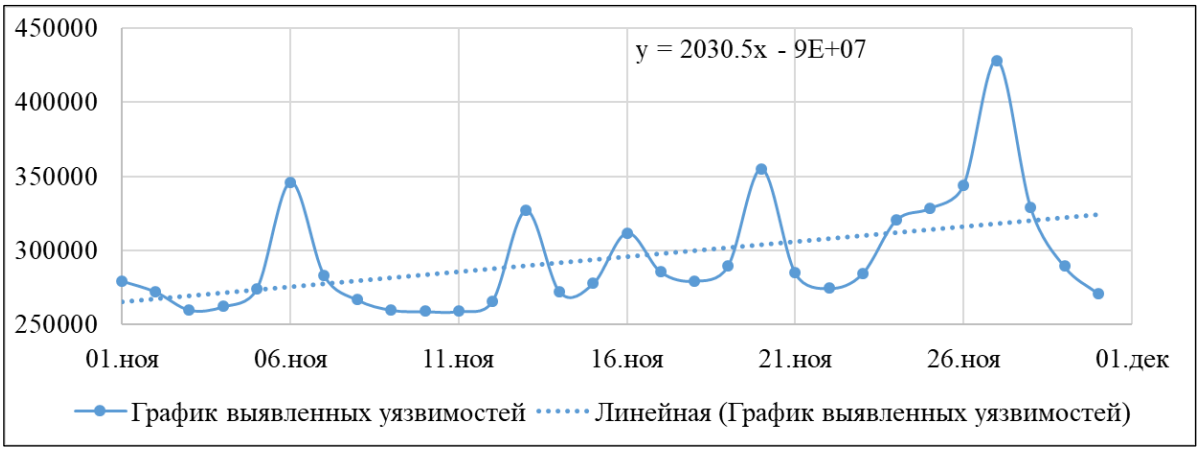

Рисунок 8. График изменения количества уязвимостей

График количества уязвимостей (Рис 8.) наглядно показывает тенденцию роста угроз, что обязывает предпринять меры по обеспечению безопасности компьютера для наименьшей вероятности утечки конфиденциальной информации.

Спам – это сообщения в виде коммерческой, политической и другой рекламы, массово рассылаемые людям, которые не давали своего согласия на их получение.

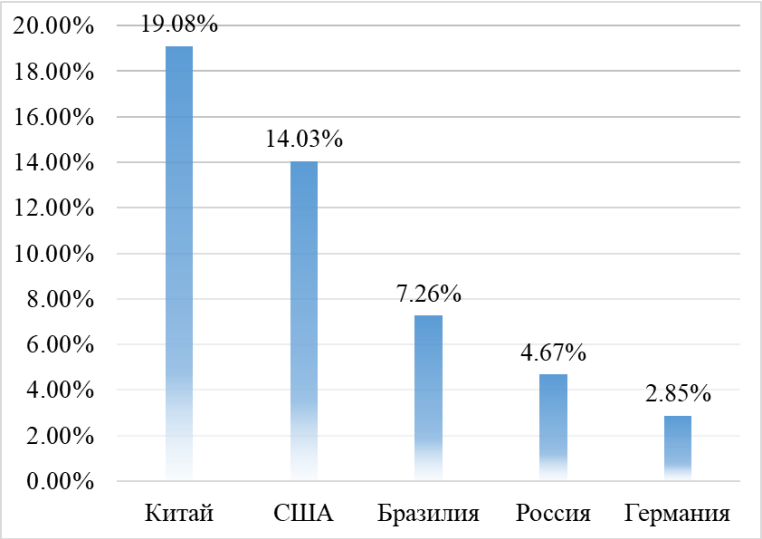

Рисунок 9. Статистика количества спама

Как и ранее, Китай, США и Бразилия опережают другие страны, что можно понять, обратившись к аналитике «Лаборатории Касперского» за второй и третий кварталы 2018 года. Показатели России изменились незначительно, на 0,56 п. п.

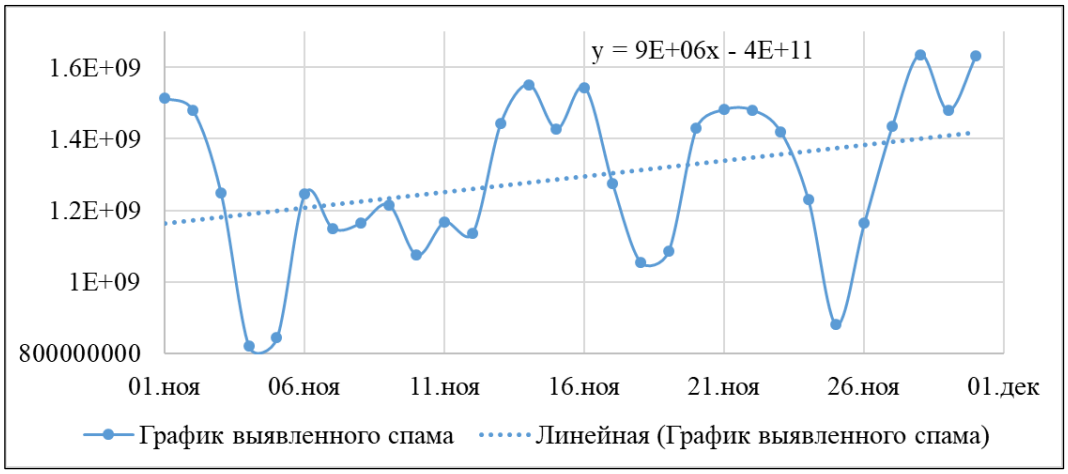

Рисунок 10. График изменения количества спама

На графике наблюдаются частые перепады увеличения и уменьшения спама, но построив тренд делаем вывод о том, что количество спама постепенно возрастает, с чем необходимо бороться с помощью специализированных фильтров.

4. Методика анализа киберугроз в мире

Используя уравнения трендов, изображённых на рисунках 2,4,6,8,10, проведём анализ скорости изменения каждого вида угроз с последующими выводами с помощью нахождения синуса угла линейной аппроксимации [5]. Строим тренд на отдельном графике и достраиваем его до прямоугольного треугольника, где сам он будет являться гипотенузой.

Находим длину прилежащего катета:

$$|a| = \sqrt{a_x^2 + a_y^2} \quad (1)$$

где a_x и a_y координаты вектора $|a|$.

Длину противолежащего катета с помощью формулы:

$$|b| = \sqrt{b_x^2 + b_y^2} \quad (2)$$

где b_x и b_y координаты вектора $|b|$.

После чего находим длину гипотенузы с помощью формулы:

$$c = \sqrt{a^2 + b^2} \quad (3)$$

где a и b катеты треугольника ABC.

Найдя все эти значение мы с лёгкостью можем найти синус угла между гипотенузой (т.е. трендом) и прилежащем катетом (т.е. осью OX), он будет равен:

$$\sin(a) = \frac{b}{c} \quad (4)$$

Далее необходимо провести анализ количества атак в день в течении месяца и сравнить угол отклонения линии.

В таблице 1 представлены результаты проведенного анализа по заданной методике.

Рассмотрев синусы углов тренда к оси OX делаем вывод о том, что активную тенденцию увеличивать количество угроз имеют локальные угрозы, сетевые атаки и спам.

Таблица 1. Результаты анализа мировой тенденции роста киберугроз на основе линейной аппроксимации статистических данных об атаках

№ п/п	Тип угрозы	Уравнение тренда	Синус угла изменения
1	Локальные угрозы	$y = 66049x - 3 * 10^9$	$0{,}0000151403 – (0 - 1)°$
2	Веб-угрозы	$y = -28963x + 1 * 10^9$	$0{,}0000345268 – (179 - 180)°$
3	Сетевые атаки	$y = -32186x + 1 * 10^9$	$0{,}0000310694 – (179 - 180)°$
4	Уязвимости	$y = 2030{,}5x - 9 * 10^7$	$0{,}0004924895 – (0 - 1)°$
5	Спам	$y = 9 * 10^6x - 4 * 10^{11}$	$0{,}0000001111 – (0 - 1)°$

5. Обсуждение

Исходя из построенных графиков трендов можем сделать вывод о том, что количество угроз возрастает у следующих типов:

– локальные угрозы;

– уязвимости;

– спам.

Это значит, что необходимо обратить внимание на эти угрозы, устанавливать на технические средства дополнительное ПО для создания барьера этим угрозам. Так, например, чтобы бороться с локальными угрозами необходимо отказаться от активации незарегистрированного программного обеспечение продукции Microsoft, так как такие программы могут быть использованы в связке с другими вредоносными и нежелательными ПО; вовремя устанавливать апдейты безопасности, иначе уже закрытые уязвимости могут применяться киберпреступниками для проникновения на целевое устройство; устанавливать дополнительные фильтры писем, для более качественной отчистки спама, ведь если этого не делать, то по закону Фридриха Энгельса, количественные изменения могут перерасти в качественные, а это значит, что угрозы перерастут в уязвимости и тогда огромное количество конфиденциальной информации может быть украдено, поэтому с ними надо бороться каждый день, каждый час, каждую минуту, усовершенствовать технологию антивирусов, не заходить на посторонние сайты, не пользоваться посторонним ПО.

6. Заключение

В результате проведённого анализа были выявлены увеличивающие своё количество в мире киберугрозы, которыми являются локальные угрозы, уязвимости и спам. Для этого было применена линейная регрессия и измерен угол отклонения прямой от оси OX.

Практическая значимость работы заключается в возможности использовании предложенной методики исследования киберугроз для оценки количественной характеристики кибератак для принятия соответствующих мер по их отражению.

Рассмотрев киберугрозы, которые имеют интенсивный рост, были получены следующие выводы:

– Необходимо использовать только лицензионное ПО.

– Необходимо использовать эффективные средства антивирусной защиты на всех устройствах.

– Необходимо своевременно обновлять используемое ПО по мере выхода патчей.

Предлагаемый подход возможно использовать на большем промежутке статистической выборки для повышения точности определения аналитической зависимости изменения количества угроз.

7. Список используемой литературы

[1] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) – 17 с.

[2] Мировая статистика киберугроз // Лаборатория Касперского URL: https://securelist.ru/statistics/ (дата обращения: 30.11.2018).

[3] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

[4] Kopytov V.V., Petrenko V.I., Tebueva F.B., Streblianskaia N.V. An Improved Brown's Method Applying Fractal Dimension to Forecast the Load in a Computing Cluster for Short Time Series. Indian Journal of Science and Technology. 2016. Т. 9. № 19. С. 93909.

[5] Тебуева Ф.Б., Сычков В.Б., Огур М.Г. Общая схема системы поддержки принятия решений для оптимизации управления поведением мобильных манипуляционных роботов // Современная наука и инновации. – 2016. – №1 (13). – С. 22-29.

[6] Копытов В.В., Петренко В.И., Сидорчук А.В. Полный одноразрядный сумматор по модулю. Патент №2427027. Бюллетень№23. Опубликован 20.08.2011.

7. List of references

[1] The Doctrine of Information Security of the Russian Federation (approved by Presidential Decree No. 646 of December 5, 2016) - 17 c.

[2] World Cyber Statistics // Kaspersky Lab URL: https://securelist.ru/statistics/ (access date: 11/30/2018).

[3] Federal Law “On Information, Information Technologies and Information Protection” dated July 27, 2006 No. 149-ФЗ.

[4] Kopytov V.V., Petrenko V.I., Tebueva F.B., Streblianskaia N.V. Anslaunches Method for the Short Time Series. Indian Journal of Science and Technology. 2016. V. 9. No. 19. P. 93909.

[5] Tebueva FB, Sychkov VB, Ogur M.G. The general scheme of decision-making support system for optimizing the management of the behavior of mobile manipulation robots // Modern science and innovations. - 2016. - №1 (13). - pp. 22-29.

[6] Kopytov V.V., Petrenko V.I., Sidorchuk A.V. Full one-digit modulo adder. Patent No. 2427027. Bulletin number 23. Published 08/20/2011.

АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПРОДУКТОВ КОМПАНИИ ИНФОТЕКС ПО ЗАЩИТЕ МОБИЛЬНЫХ КОММУНИКАЦИЙ В КОРПОРАТИВНОЙ СРЕДЕ

Автор – Унтевский Н.Ю.
untewsky@yandex.ru

Автор - Минкина Т.В.
Кандидат технических наук, доцент
n.min@mail.ru

Автор - Орел Д.В.
Кандидат технических наук, доцент кафедры ОТЗИ
kde.def@gmail.com

Унтевский Н.Ю.- Северо-Кавказский федеральный университет, Ставрополь, 355045, Россия
Минкина Т.В. - Северо-Кавказский федеральный университет, Ставрополь, 355055, Россия
Орел Д.В. – Северо-Кавказский федеральный университет, Ставрополь, 355035, Россия

Аннотация:

В данной статье подробно рассмотрена процедура защиты мобильных коммуникаций, реализуемая путем применения сразу нескольких продуктов, разработанных на основе флагманской технологии ViPNet. Рассмотрено, по каким критериям данная технология является защищенной VPN сетью. В частности проанализированы два продукта компании ИнфоТеКС: ViPNetClient и ViPNetConnect, также были выявлены их преимущества. Установлено на чем основывается безопасное соединение с сетью интернет через ViPNetClient, и каким образом оно позволяет безопасно обмениваться данными различного типа. Также проанализирован мессенджер ViPNetConnect для устройств, как мобильных, так и стационарных и выявлено, почему оно специализируется для общения в корпоративной среде. Рассмотрены свойства приложения, по которым можно гарантирует безопасную коммуникацию всех пользователей ViPNetConnect, как при голосовых переговорах, так и во время текстового общения. Также рассмотрена эксплуатационная сторона приложения ViPNetConnect. Данная продукция может быть весьма полезным приобретением для большинства организаций, так как отвечает всем актуальным запросам. В статье рассмотрены их преимущества и сделаны выводы о целесообразности их применения в корпоративной среде.

Annotation:

This article describes in detail the procedure for the protection of mobile communications, implemented through the use of several products developed on the basis of ViPNet flagship technology. It is considered by what criteria this technology is a secure VPN network. In particular, two products of the company Infotex were analyzed: ViPNet Client and ViPNet Connect, their advantages were also revealed. Established on what is based a secure connection to the Internet via ViPNet Client and how it allows you to securely exchange data of various types. Also analyzed messenger ViPNet Connect for devices, both mobile and stationary and revealed why it specializes in communication in the corporate environment. The properties of the application, which ensures secure communication between all users of ViPNet Connect as a voice in the negotiations and during the text communication. The operational side of ViPNet Connect application is also considered. This product can be a very useful purchase for most organizations, as it meets all current needs. The article discusses their advantages and conclusions about the feasibility of their application in the corporate environment.

Ключевые слова: ViPNet, конфиденциальность, ViPNetClient, ИнфоТеКС, информация, шифрование, защищённые каналы, ViPNetConnect, корпоративная среда.

Keywords: ViPNet, privacy, ViPNet Client, Infotex, information, encryption, secure channels, ViPNet Connect, corporate environment.

ViPNet VPN — это линейка продуктов компании ИнфоТеКС, включающая программные и программно-аппаратные комплексы, средства защиты информации ограниченного доступа, в том числе персональных данных.

Об этих способах защиты пойдет речь в данной статье, а именно о защите данных, которые хранятся на наших мобильных устройствах и передаются с их же помощью в частности в корпоративной среде. Таким образом целью настоящей работы является проведение анализа функциональных возможностей продуктов компании Инфотекс по защите мобильных коммуникаций в корпоративной среде. [6]

В наши дни довольно часто с помощью мобильных устройств выполняются переговоры между сотрудниками, а не редко и владельцами, различных организаций. Информация, которой они обмениваются, может иметь как маленькую, так и просто неоценимую ценность

для определенного круга лиц, а потенциальный ущерб, который может получить компания, допустив утечку информации, может оказаться катастрофическим. [7]

Следовательно, вопрос о конфиденциальности и защищенности мобильных коммуникаций в корпоративной среде является очень важной темой, как для крупных, так и для начинающих организаций. В таком случае давайте рассмотрим продукты предназначенные для защиты мобильных коммуникаций, предлагаемых компанией ИнфоТеКС: [5]

1. ViPNetClient
2. ViPNetConnect

Именно эти два продукта отлично функционируют вместе, расширяя возможности при их совместном использовании.

1. Начнем мы с ViPNetClient, который позволяет своим пользователям безопасно обмениваться данными и организует их защиту на вашем персональном устройстве, а также надежно защищающий работу с корпоративными данными через Интернет. ViPNetClient также поддерживает работу на компьютерах под управлением таких операционных систем как Windows, Linux и OS X. Данный продукт обеспечивает безопасное пребывание в интернет среде за счёт комплексной защиты, состоящей сразу из нескольких уровней. [4]

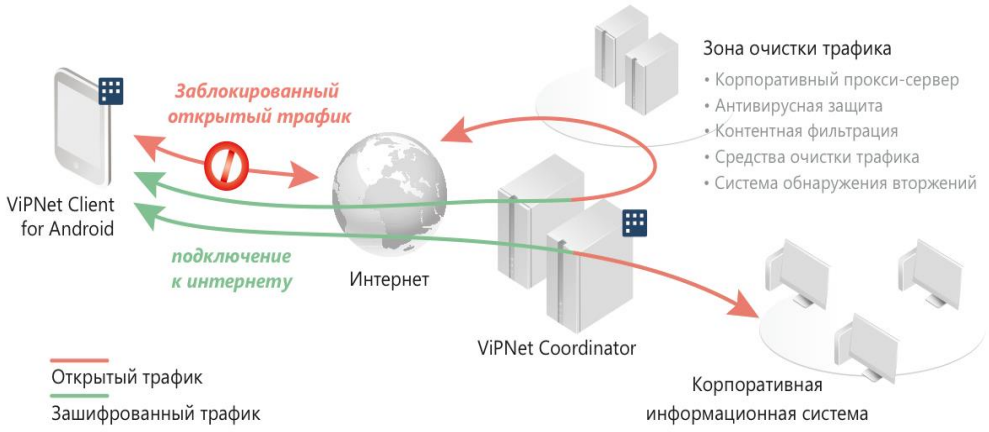

Рисунок 1. Сценарии использования ViPNetClient.

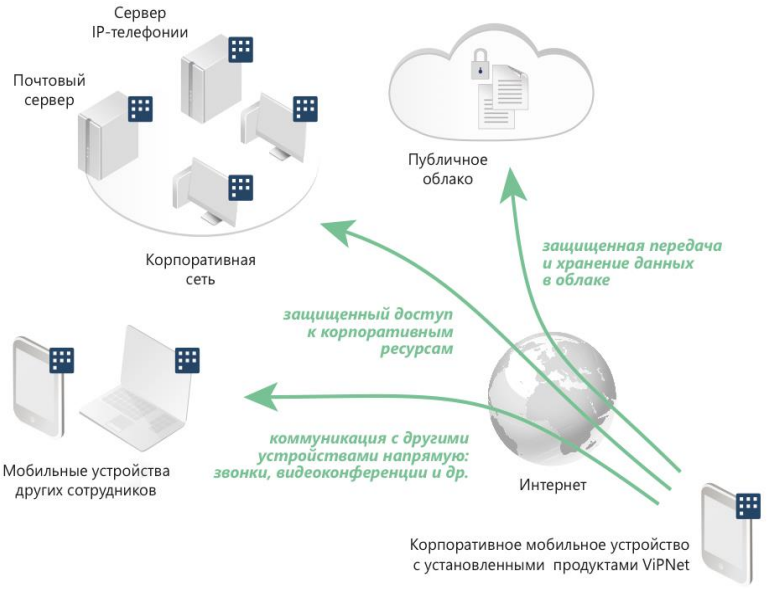

Рисунок 2.Безопасная работа с корпоративными ресурсами через защищенные каналы.

С любыми внутренними данными через интернет можно работать без какой-либо опаски, благодаря шифрованию трафика, в котором используется алгоритм ГОСТ 28147-89 (длина ключа 256 бит).

Безопасная работа в Интернете с централизованной очисткой трафика. [3]

Приложение ViPNetClient имеет функцию блокировки прямого доступа в интернет, даже если устройство в данный момент лежит за пределами корпоративной сети.

При этом доступ в интернет устройство может получить только через корпоративный центр очистки трафика: прокси-серверы, межсетевые экраны и другие средства фильтрации.

Данный подход предоставляет многоуровневую защиту мобильного устройства и дает возможность использовать корпоративные механизмы информационной безопасности с планшетами и смартфонам так же, как и к с обычными офисными компьютерами. Пользователям больше не нужно устанавливать на мобильные устройства специализированные версии средств контроля трафика. [7]

Безопасная коммуникация пользователей

ViPNetClient выполняет множество полезных функций, но они могут быть дополнены и стать еще более полезными при работе вместе с еще одной разработкой компании ИнфоТеКС под названием ViPNetConnect, которая нацелена на обеспечение защищенного общения корпоративных пользователей и также будет рассмотрена в нашей статье.

Фильтрация трафика на устройстве. [8]

ViPNetClient защищает мобильное устройство от сетевых атак с помощью встроенного сетевого экрана, который управляется централизованно администратором защищенной сети.

Мобильное устройство с ViPNetClient обладает встроенным сетевым экраном, доступ к которому имеет только администратор защищенной сети. [9]

Преимущества:

- стабильная и быстрая работа приложения не зависит от качества канала связи. (предварительное соединение не обязательно устанавливать для построения защищенного канала ViPNet);
- защищенное соединение при временных разрывах связи восстанавливается автоматически;
- злоумышленники не имеют возможности встроиться в защищенное соединение и осуществить MITM-атаки, потому что процесс шифрования начинается с первой фазы установления соединения;
- для удаленной защиты устройства используется корпоративный центр очистки трафика снижающий нагрузку обработки трафика;
- прозрачная защита канала для сторонних приложений на устройстве;
- благодаря ViPNetClient платформами iOS и Android можно пользоваться, не обладая правами суперпользователя;
- централизованное управление ViPNetClient . Политика безопасности, обновления ПО, ключи шифрования передаются по защищенному каналу.

Следующий продукт от компании ИнфоТеКС, о котором мы обещали рассказать это ViPNetConnect, являющийся альтернативой публичных мессенджеров для безопасной коммуникации корпоративных пользователей, также это приложение дает возможность контролировать инфраструктуру безопасности по своему усмотрению. [2]

ViPNetConnect функционирует на стационарных компьютерах, ноутбуках и мобильных устройствах и позволяет осуществлять голосовые коммуникации, отправку текстовых сообщений и обмен файлами. Каналы сети ViPNet с шифрованием «точка-точка» обеспечивают защиту и конфиденциальность общения пользователей ViPNetConnect.
Преимущества: [4]

- любая информация передается по защищенным каналам связи, в том числе при передаче в локальной сети;
- удобный интерфейс, который не вызовет у пользователей никаких вопросов и поможет легко освоиться со всеми возможностями приложения;
- администратор сети ViPNet задает адресную книгу ViPNetConnect и пользователь не может изменить ее самостоятельно;
- общение как с пользователями сети ViPNet, так и с пользователями в сетях компаний-партнеров;
- метод шифрования «точка-точка».

Пользователи ViPNetConnect общаются друг с другом напрямую (связь «точка-точка»). Посторонние лица не могут получить доступ к информации, так как отсутствуют промежуточные сервера для хранения или расшифровки данных.

В использовании центрального маршрутизирующего сервера нет никакой необходимости, так как функционирование проходит в режиме «точка-точка» следовательно, можно обойтись без высокоскоростного канала связи. [10]

Исходя из подробного анализа продуктов компании ИнфоТеКС, результатом их применения является высокий уровень защиты мобильных коммуникаций в корпоративной среде, независимо от их разновидностей.

Данная продукция может быть весьма полезным приобретением для большинства организаций, так как отвечает всем актуальным запросам. Она обеспечивает безопасное нахождение в интернете, а также предоставляет настраиваемую и удобную платформу для всех видов коммуникаций в корпоративной среде, включая как видео, так и аудио звонки, а также обмен файлами. [1]

Список используемой литературы:

[1] Kopytov V.V., Petrenko V.I., Tebueva F.B., Streblianskaia N.V. An improved brown's method applying fractal dimension to forecast the load in a computing cluster for short time series/Indian Journal of Science and Technology. 2016. Т. 9. № 19. С. 93909.

[2] Петренко В. И., Мирошников Д. А., Емельянов Е. А.Обзор современных средств сетевой защиты информации//Проблемы автоматизации. Региональное управление. Связь и автоматика («ПАРУСА-2015»), Материалы IV Всероссийской научной конференции молодых ученых, аспирантов и студентов, Геленджик, 2015.

[3] Исупов Т.А., Орел Д.В., Минкина Т.В. Анализ специфики информационных процессов в инфраструктуре открытых ключей (PKI) /В сборнике: Экономическое развитие регионов России в условиях трансформации информационной среды//Сборник научных статей по материалам Всероссийской научно-практической конференции. 2018. С. 110-115.

[4] Orel D., Zhuk A., Zhuk E., Luganskaia L. A METHOD OF FORMING CODE SETS FOR CDMA IN COMMUNICATION, NAVIGATION AND CONTROL SYSTEMS//В сборнике: CEUR Workshop Proceedings 2. Сер. "YSIP2 2017 - Proceedings of the 2nd Young Scientist's International Workshop on Trends in Information Processing" 2017. С. 158-167.

[5] Жук Ю.А., Иванов А.С., Орёл Д.В. Способ передачи информации в системах сотовой подвижной связи с кодовым разделением каналов //Наукоемкие технологии в космических исследованиях Земли. 2010. Т. 2. № 2. С. 18-20.

[6] Тринкин М.Г., Орёл Д.В., Минкина Т.В. Совершенствование метода аутентификации пользователей информационных систем по клавиатурному почерку. В сборнике: Экономическое развитие регионов России в условиях трансформации информационной среды//Сборник научных статей по материалам Всероссийской научно-практической конференции. 2018. С. 184-188.
[7] Лагунов Н.А., Мезенцева О.С. Влияние предобработки изображений на качество обучения нейронной сети для их распознавания. Вестник Северо-Кавказского федерального университета. 2015. № 1 (46). С. 51-58.
[8] Светличная Н.В., Савельев С.В., Минкина Т.В. Роль организационных мероприятии в надежности механизма защиты информации. // Студенческая наука для развития информационного общества сборник материалов V Всероссийской научно-технической конференции: в 2 частях. 2016. С. 347-350.
[9] Nemkov R.M., Mezentseva O.S., Mezentsev D. Using of a convolutional neural network with changing receptive fields in the tasks of image recognition// Advances in Intelligent Systems and Computing. 2016. Т. 451. С. 15-23.
[10] Севастьянов С.А., Гогуля В.А., Палканов И.С. WAN технологии: уникальные возможности использования// Студенческая наука для развития информационного общества сборник материалов VII Всероссийской научно-технической конференции. 2018. С. 282-286.

Listofreferences:

[1] Kopytov V. V., Petrenko V. I., Tebueva F. B., Streblianskaia N. V. An improved brown's method of applying fractal dimension to forecast the load in a computing cluster for short time series/Indian Journal of Science and Technology. 2016. Vol. 9. No. 19.P. 93909.
[2] Petrenko V. I., Miroshnikov D. A., Emelyanov E. A. Review of modern means of network information security//Problems of automation. Regional management.Communication and automation ("SAILS-2015"), Proceedings of the IV all-Russian scientific conference of young scientists, postgraduates and students, Gelendzhik, 2015.
[3] Isupov T. V., Orel D. V., Minkina T. V. analysis of the information specifics processes in the infrastructure of open keys (PKI) /in the collection Of economic Russian regions development in the transformation of the information environment//Collection of scientific articles on the materials of the all-Russian scientific-practical conference. 2018. P. 110-115.
[4] D. Orel, A. Zhuk, Zhuk E., Luganskaia L. A METHOD OF FORMING CODE SETS FOR CDMA IN COMMUNICATION, NAVIGATION AND CONTROL SYSTEMS//proceedings: CEUR Workshop Proceedings 2. Ser. "YSIP2 2017-

Proceedings of the 2nd Young Scientist's International Workshop on Trends in Information Processing" 2017. P. 158-167.

[5] Zhuk Y. A., Ivanov A. S., eagle, D. V., a Method of transmitting information in a cellular mobile communications with code division of channels //science Intensive technologies in space studies of the Earth. 2010. Vol.2. No. 2. P. 18-20.

[6] Trinkin M. G., Orel D. V., Minkina T. V. Improving the method of authentication of users of information systems by keyboard handwriting. In the collection: Economic development of Russian regions in the transformation of the information environment / / Collection of scientific articles on the materials of the all-Russian scientific-practical conference. 2018. P. 184-188.

[7] N. Lagunov.A. Mezentseva O. S. Influence of image preprocessing on the quality of training the neural network to recognize them.Bulletin of the North Caucasus Federal University.2015. No. 1 (46). P. 51-58.

[8] Svetlichnaya N. In. Savelyev S. V., Minkina T. V. the Role of organizational measures in the reliability of the information security mechanism. // Student science for the development of information society proceedings of the V all-Russian scientific and technical conference: in 2 parts. 2016. P. 347-350.

[9] Nemkov, R. M., Mezentseva O. S., Mezentsev D. Using of a convolutional neural network with changing receptive fields in the tasks of image recognition// Advances in Intelligent Systems and Computing. 2016. Vol. 451. P. 15-23.

[10] Sevastyanov, S. A. and Gogola V. A., Polkanov I. S. WAN technology: unique opportunities for use// Student science for development of the information society a collection of materials of VII all-Russian scientific-technical conference. 2018. P. 282-286.

Секция 3. «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

Подсекция 2

РАЗРАБОТКА МЕТОДИКИ ПОСТРОЕНИЯ ПСИХОЛГИЧЕСКОГО ПОРТРЕТА ПОТЕНЦИАЛЬНОГО НАРУШИТЕЛЯ ПУТЕМ АНАЛИЗА ЕГО АКТИВНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Гончаров А.Б.[1]
artur_goncharov_97@mail.ru

Ажмухамедов И.М.[1]
д.т.н.,доцент
iskander_agm@mail.ru

[1] Астраханский государственный университет, г. Астрахань, 414056, Россия

Аннотация

В нашем современном мире, в век прогресса, развития науки и технологий манипулировать людьми становится все проще. Приёмами манипуляции активно пользуются террористы, для вербовки людей в свои ряды, различные мошенники для вымогательства денежных средств жертвы. Если рассмотреть этот вопрос с точки зрения информационной безопасности, то манипуляцию могут применять злоумышленники для вытягивания конфиденциальной информации, либо же, что бы заставить жертву каким-то образом уменьшить уровень защиты. Исходя из этого, выявления людей, которые могут стать жертвами манипулятора, является актуальной задачей, как для организаций, так и для государства в целом.

В данной статье рассматривается методика по выявлению потенциальных нарушителей. Суть данной методики состоит в построение психологического портрета потенциального нарушителя путем анализа его активности в социальных сетях. Описан эксперимент по определению определенных личностных характеристик с помощью корреляционного и регрессионного анализа на основе данных, полученных из социальных сетей. Эксперимент проведен с участием добровольцев. Были выявлены

корреляции между личностными характеристиками и словами, которые наиболее часто встречаются в, понравившихся пользователям, записях. Выявленные корреляции были использованы для проведения регрессионного анализа с целью предсказания личностных характеристик.

Abstract

In our modern world, in the age of progress, development of science and technology to manipulate people is becoming easier. Methods of manipulation are actively used by terrorists to recruit people into their ranks, various scammers to extort money from the victim. If we consider this issue from the point of view of information security, the manipulation can be used by attackers to pull confidential information, or that would force the victim to somehow reduce the level of protection. Based on this, the identification of people who may become victims of the manipulator, is an urgent task for organizations and for the state as a whole.

In this article the technique of identification of potential violators is considered. The essence of this technique is to build a psychological portrait of a potential offender by analyzing its activity in social networks. An experiment to determine certain personal characteristics using correlation and regression analysis based on data obtained from social networks is described. The experiment was conducted with the participation of volunteers. Correlations between personal characteristics and the words that are most often found in the posts that users liked were revealed. The revealed correlations were used for regression analysis to predict personal characteristics.

Ключевые слова: анализ данных, социальные сети, информационный образ, психоэмоциональное состояние, психометрика, социальное взаимодействие.

Keywords: data analysis, social networks, information image, psycho-emotional state, psychometrics, social interaction.

1 Введение

Потенциальный нарушитель – человек, который склонен к манипулированию.

Манипулирование – скрытое управления человеком для достижения, каких-либо определенных целей. В повседневной жизни это понятие встречается довольно часто, потому что желание манипулировать окружающими людьми присуще каждому. Манипуляцию можно сравнить с ножом. Нож сам по себе не плохой и не хороший. Все зависит от того, в чьих руках он находится. В руках хирурга он используется для сохранения жизни, в руках преступника - наоборот. Поэтому и манипуляцию нужно рассматривать в используемом контексте, а также, важны цели, с которыми она применяется. Результаты применения манипуляции могут, как приносить благо, так и наносить ущерб.

Для успешного манипулирования человеком, манипулятор должен найти точки давления на него. Такой точкой может служить эмоциональное состояние, состояние влюбленности, привязанность, обида, депрессия и т.д. Что бы найти эти точки, манипулятор должен собрать как можно больше информации о своей жертве, составить ее психологический портрет.

Раньше для составления психологического портрета, необходимо было, как то контактировать с человеком, чей портрет ты хочешь составить, либо же заставить его пройти психологический тест. Сейчас, с появлением социальных сетей все изменилось.

В последние годы произошла крупная революция в том, как люди взаимодействуют друг с другом через Интернет. Социальные сети являются частью этой революции. Число пользователей социальных сетей растет с каждым годом. Если 2010 году их было примерно 0,97 млрд. человек, то в 2018 эта цифра увеличилось в 2,5 раза [1].

Сегодня почти каждый человек имеет аккаунт хотя бы в одной социальной сети. За счет возрастающей интеграции социальных сетей в повседневную жизнь современного человека, большое количество населения осознанно оставляют значительное количество информации о себе в свободном доступе. Используя эту информацию можно составить достаточно точный психологический портрет человека.

К данным пользователя, размещенным в свободном доступе можно отнести следующие:

- личные данные (пол, возраст, семейное положение, религиозные и политические предпочтения, образование, профессия и т.д.);

- данные об активности пользователя (количественные характеристики дружественных связей; входящих/исходящих комментариев, лайков; периоды активности; геометки;

- посещаемые сообщества и информационные страницы и т.д.)

- генерируемый и используемый пользователем контент:

a) тексты (комментарии, записи со стены, заметки, статусы и т.д.);

b) изображения;

c) аудиозаписи;

d) видеозаписи.

Данные делятся на фактически записанные данные, т.е. те который пользователь выкладывает сам и на информацию, которая может быть предсказана из таких данных.

Люди могут не раскрывать определенные сведения о своей жизни, такие как их сексуальная ориентация или возраст, и тем не менее эта информация может быть предсказана в статистическом смысле из других аспектов их жизни, которые они раскрывают. Например, крупная американская розничная сеть использовала записи покупок клиентов для прогнозирования беременности своих женских клиентов и отправки им своевременных и хорошо ориентированных предложений.

2 Разработка методики

На протяжении десятилетий исследователи психологи работали, что бы понять личность. После обширных работ по изучению личностной модели, исследователи установили связь между характером человека и типом поведения. Отношения были установлены между личностью и психологическим расстройством [2], личностью и родом деятельности [3], личностью и умственными способностями человека [4] и так далее.

С появлением социальных сетей психологов стал интересовать вопрос, могут ли профили в социальных сетях предсказывать черты личности. Было показано, что внешние наблюдатели могут успешно оценивать черты личности пользователей, изучая их страницы в сети Facebook [5]. Аналогичное исследование проводилось и для пользователей социальной сети Twitter [6]. Поведение в Facebook может само по себе быть функцией черт личности. В первую очередь речь идет об экстраверсии. Наличие ее коррелирует, например, с цветовыми предпочтениями фотографий [7], с числом групп, в которые вступает пользователь [8], с числом фотографий, размещенных на странице [9]; со статистическими характеристиками числа друзей, записей на стене (постов) и комментариев, просмотров своих и чужих страниц; замен фотографий профиля, слов в секции «обо мне» [10]. В свою очередь, показатели выраженности нейротизма связаны с частотой использования стены для коммуникаций [8], а добросовестность – с самоотчетным числом отправленных личных сообщений в Facebook [9].

Одним из привлекательных с точки зрения эмпирической психологии свойств социальных сетей является сравнительно простое получение численных показателей поведения индивида и фиксация этих показателей за определенный период времени.

Число исследований поведения пользователей Facebook растет по мере понимания важности научной составляющей социальных сетей, однако исследований такого поведения

в отечественной сети «Вконтакте» практически нет. Таким образом, целью настоящего исследования стало изучения поведения пользователей социальной сети «Вконтакте» для определения черт личности и обнаружения потенциальных нарушителей.

3 Постановка задачи

Целью настоящего исследования стало изучения поведения пользователей социальной сети «Вконтакте» для определения черт личности и обнаружения потенциальных нарушителей.

Исследование основано на использование likes в «Вконтакте». Like - механизм используемый пользователями для выражения положительной связи с онлайн контентом, например фотографиями, обновлениями статуса друзей, спортом, музыкантами, книгами, ресторанами и т.д.

4 Результаты

Поиск респондентов для исследования осуществлялся в группах, социальной сети «Вконтакте», связанных с психологией. В общей сложности в исследовании приняли участие 50 пользователей данной социальной сети. Каждый участник сообщал свои имя и фамилию, что объяснялось для испытуемых необходимостью «избежать ошибок при подготовке и рассылке обратной связи». По окончании исследования участники получали по электронной почте файл с результатами тестирования черт личности. На всех этапах исследования конфиденциальность личных данных испытуемых была обеспечена.

Испытуемые ответили на вопросы личностного опросника «Большая пятерка» [11] для определения следующих черт личности:

- депрессивность – склонность в обычном состоянии проявлять хроническую подавленность и угнетенность настроения; преобладание негативного в самооценке, эмоциональном состоянии;

- доверчивость – склонность принимать какую-либо информацию без критического размышления или анализа, постоянная готовность верить слову, обещанию другого человека или группы.

- мечтательность – сильная склонность относиться к своим мыслям и желаемым образным представлениям, как к значащим большего и заслуживающим большего внимания,

чем окружающая действительность; навязчивое состояние, уводящее в мир иллюзий, несбыточных желаний и грёз;

- тревожность – склонность к чрезмерному беспокойству, к частым и интенсивным негативным переживаниям сильной тревоги, а также в низком пороге её возникновения;

- эмоциональная лабильность – это патология нервной системы, характеризующаяся неустойчивостью настроения, его резкими перепадами без видимых причин.

Средние балы по личностному тесту представлены в Таблице 1.

Таблица 1 – Средние балы по личностному тесту

Черта личности	Средний бал
депрессивность	10
доверчивость	9
мечтательность	12
тревожность	10
эмоциональная лабильность	9

Затем, для каждого пользователя, мы собрали данные его профиля в социальной сети «Вконтакте». Нас интересовали записи, на которые пользователь поставил отметку «Мне нравится» (Like), а также записи, которые пользователь разместил у себя на стене. Для сбора данных со страниц пользователя было написано специальное программное обеспечение с использованием API Вконтакте [12]. Программа была написана на языке программирования Python 3.7.

Предыдущие исследования показали, что лингвистические особенности используется для прогнозирования личностных качеств [13-14]. Существует потенциал для применения этих методов лингвистического анализа, чтобы помочь предсказать личность, анализируя записи человека. Однако в предыдущих исследованиях использовался текст большего объема, чем любая из записей Вконтакте. Исходя, из этого было принято решения объединить полученные записи конкретного пользователя в единый файл.

После того как мы получили файл для каждого пользователя, был проведен частотный анализ распределения слов в этих файлах. Перед началом частотного анализа необходимо осуществить следующие действия:

- привести текст к нижнему регистру;

- удалить «стоп слова»;

- удалить цифры;

- удалить знаки препинания;

- провести нормализацию слов.

В результате частотного анализа были получены слова с наибольшей частотой. Эта частота будет использоваться для нахождения корреляций между словами и личностными характеристиками пользователя.

Мы провели корреляционный анализ Пирсона между баллами личностных характеристик, полученных из результатов теста, и частотой слов из записей каждого пользователя. Результаты приведены в Таблице 2. Наиболее статистически значимые корреляции выделены жирным шрифтом.

Таблица 2 – Результаты корреляционного анализа Пирсона

	Депрессивность	Доверчивость	Мечтательность	Тревожность	Эмоциональная лабильность
ехать	0,027	0,092	-0,013	0,177	0,05
мечта	-0,14	-0,5	**0,382**	-0,189	**0,301**
башня	**0,232**	-0,05	0,162	0,125	-0,08
родной	-0,05	0,003	**-0,325**	0,023	**-0,213**
сквозь	0,106	0,34	0,035	**-0,257**	-0,06
просьба	0,024	0,014	0,086	-0,094	-0,124
проявлять	-0,17	-0,178	-0,01	-0,04	-0,06
интересоваться	-0,107	0,062	-0,132	0,135	-0,02
пистолет	**-0,324**	0,06	-0,01	0,05	0,023
игнорировать	**-0,374**	**-0,216**	**-0,358**	-0,195	-0,25
Пушкин	-0,01	-0,08	0,07	0,01	-0,61
благодарить	**-0,246**	-0,03	-0,135	-0,31	-0,28
крепкий	-0,136	-0,178	-0,124	0,131	**-0,312**
военный	0,229	0,065	0,065	0,078	0,154
острый	-0,194	0,05	**-0,357**	0,0002	**-0,256**
легко	-0,137	**-0,254**	0,154	0,0006	**-0,325**
сложность	**0,235**	-0,07	**-0,256**	-0125	-0,035
жертва	-0,121	-0,124	0,084	-0,158	-0,105
мечтать	**0,354**	-0,098	0,025	0,065	0,188
божественный	-0,186	0,015	-0,125	-0,85	-0,125
любовник	0,177	**-0,321**	-0,095	0,178	0,197

благодарность	-0,21	-0,005	**-0,351**	-0,14	-0,151
здоровый	**-0,382**	0,027	**-0,325**	-0,05	**-0,325**

Для предсказания личностных характеристик была построена регрессионная модель. В качестве выборки, для обучения этой модели, использовалась частота слов, с наиболее высоким коэффициентом корреляции, и результаты прохождения личностного опросника. Точность построения модели регрессии для каждой характеристике отражена в Таблице 3.Было обнаружено, что проще всего вычислить мечтательность, а сложнее всего определить тревожность.

Таблица 3 – Точность модели регрессии

Черта личности	Депрессивность	Доверчивость	Мечтательность	Тревожность	Эмоциональная лабильность
Точность	0,182	0,325	0,45	0,008	0,335

5 Заключение

Полученные на основе анализа результаты имеют достаточно низкую точность. Для повышения точности исследования, следует значительно увеличить количество тестируемых и анализируемых пользователей, а также расширить количество собираемых и анализируемых параметров пользовательских профилей таких как, например, эмоции на фотографиях, время активности пользователя и другие. Благодаря этому точность результатов возрастет и возможно будет получить новые дополнительные факторы, влияющие на определение темперамента пользователя.

6 Список используемой литературы

[1] Статистика роста пользователей социальных сетей, Электронный ресурс URL: https://www.statista.com/study/12393/social-networks-statista-dossier/

[2] L. Saulsman and A. Page. The five-factor model and personality disorder empirical literature: A meta-analytic review* 1. Clinical Psychology Review, 23(8):1055–1085, 2004

[3] M. Barrick and M. Mount. The Big Five personality dimensions and job performance: A meta-analysis. Personnel psychology, 44(1):1–26,1991.

[4] T. Judge, C. Higgins, C. Thoresen, and M. Barrick. The big five personality traits, general mental ability, and career success across the life span. Personnel psychology, 52(3):621–652, 1999.

[5] Back M, Stopfer J, Vazire S, Gaddis S, Schmukle S, et al. (2010) Facebook profiles reect actual personality, not self-idealization. Psychological Science 21: 372–374.

[6] Self-Expression on Social Media: Do Tweets Present Accurate and Positive Portraits of Impulsivity, Self-Esteem, and Attachment Style?

[7] Kramer, N. C., & Winter, S. (2008). The relationship of self-esteem, extraversion, self efficacy, and self-presentation within social networking sites. Journal of Media Psychology, 20,106–116.

[8] Ross, C., Orr, E.S., Sisic, M., Arseneault, J.M., Simmering, M.G., & Orr, R.R. (2009). Personality and motivations associated with Face book use. Computers in Human Behavior, 25, 578–586.

[9] Muscanell, N.L., & Guadagno, R.E. (2012). Make new friends or keep the old: Gender and personality differences in social networking use. Computers in Human Behavior, 28, 107– 112.

[10] Gosling, S.D., Gaddis, S., and Vazire, S. (2007). Personality impressions based on Facebook profiles. In Proceedings of the International Conference on Weblogs and Social Media(Boulder, Colorado, USA, March 26–28, 2007).

[11] O. D. John. Big five inventory, 2000.

[12] Документация API Вконтакте, Электронный ресурс URL: https://vk.com/dev/manuals

[13] F. Mairesse, M. Walker, M. Mehl, and R. Moore. Using linguistic cues for the automatic recognition of personality in conversation and text. Journal of Artificial Intelligence Research, 30(1):457–500, 2007.

[14] J. Pennebaker and L. King. Linguistic styles: Language use as an individual difference. Journal of personality and social psychology, 77(6):1296–1312, 1999.

List of references

[1] Statistics of growth of users of social networks, Electronic resource URL: https://www.statista.com/study/12393/social-networks-statista-dossier/

[2] L. Saulsman and A. Page. The five-factor model and personality disorder empirical literature: A meta-analytic review* 1. Clinical Psychology Review, 23(8):1055–1085, 2004

[3] M. Barrick and M. Mount. The Big Five personality dimensions and job performance: A meta-analysis. Personnel psychology, 44(1):1–26,1991.

[4] T. Judge, C. Higgins, C. Thoresen, and M. Barrick. The big five personality traits, general mental ability, and career success across the life span. Personnel psychology, 52(3):621–652, 1999.

[5] Back M, Stopfer J, Vazire S, Gaddis S, Schmukle S, et al. (2010) Facebook profiles reect actual personality, not self-idealization. Psychological Science 21: 372–374.

[6] Self-Expression on Social Media: Do Tweets Present Accurate and Positive Portraits of Impulsivity, Self-Esteem, and Attachment Style?

[7] Kramer, N. C., & Winter, S. (2008). The relationship of self-esteem, extraversion, self efficacy, and self-presentation within social networking sites. Journal of Media Psychology, 20,106–116.

[8] Ross, C., Orr, E.S., Sisic, M., Arseneault, J.M., Simmering, M.G., & Orr, R.R. (2009). Personality and motivations associated with Face book use. Computers in Human Behavior, 25, 578–586.

[9] Muscanell, N.L., & Guadagno, R.E. (2012). Make new friends or keep the old: Gender and personality differences in social networking use. Computers in Human Behavior, 28, 107– 112.

[10] Gosling, S.D., Gaddis, S., and Vazire, S. (2007). Personality impressions based on Facebook profiles. In Proceedings of the International Conference on Weblogs and Social Media(Boulder, Colorado, USA, March 26–28, 2007).

[11] O. D. John. Big five inventory, 2000.

[12] Documentation API Vkontakte, Electronic resource URL: https://vk.com/dev/manuals

[13] F. Mairesse, M. Walker, M. Mehl, and R. Moore. Using linguistic cues for the automatic recognition of personality in conversation and text. Journal of Artificial Intelligence Research, 30(1):457–500, 2007.

[14] J. Pennebaker and L. King. Linguistic styles: Language use as an individual difference. Journal of personality and social psychology, 77(6):1296–1312, 1999.

МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СОЦИАЛЬНОЙ СРЕДЕ КАК ОСНОВА ПРОТИВОДЕЙСТВИЯ ИДЕОЛОГИЧЕСКОМУ ЭКСТРЕМИЗМУ

Мачуева Д.А [1]
ladyd_7@mail.ru

Глебов В.В [1]
Glebov_vitia@mail.ru

Ажмухамедов Искандар Маратович [1]
д.т.н., доцент
iskander_agm@mail.ru

[1] Астраханский государственный университет, г. Астрахань, 414056, Россия

Аннотация

Различные экстремистские и террористические организации, пользуясь расширившимися возможностями современных коммуникативных технологий, осуществляют воздействие на сознание социальных групп путем организации и проведения деструктивных информационных акций. Для выработки адекватных мер противодействия влиянию экстремистов на общество необходимо правильно представлять механизмы распространения информации в социуме. С этой целью в работе представлена имитационная модель процесса информационного взаимодействия в социальных системах. Задача данного проекта – разработка алгоритмов и моделей, позволяющих исследовать закономерности информационного взаимодействия в социальных системах, проводить мониторинг «информационного фона» и прогнозировать настроения в обществе. Для моделирования информационного взаимодействия в социальной системе разработана соответствующая математическая модель, основанная на результатах теории клеточных автоматов с применением

элементов теории нечетких множеств. Данная модель нацелена на определение важных аналитических зависимостей между параметрами социальных систем и динамикой информационного обмена. Разработанная модель реализована в виде алгоритмического и программного обеспечения. Проведенные с использованием данного ПО расчеты позволили выявить основные закономерности процесса информационного взаимодействия в социальных системах, что в свою очередь позволило сформулировать некоторые рекомендации по управлению данным процессом.

Abstract

Various extremist and terrorist organizations, taking advantage of the expanded capabilities of modern communication technologies, influence the consciousness of social groups by organizing and conducting destructive information campaigns. To develop adequate measures to counteract the influence of extremists on society, it is necessary to correctly represent the mechanisms of information dissemination in society. To this end, the paper presents a simulation model of the process of information interaction in social systems. The objective of this project is the development of algorithms and models to investigate the patterns of information interaction in social systems monitor the “information background” and predict mood in society. To simulate information interaction in a social system, a corresponding mathematical model has been developed, based on the results of cellular automata theory using elements of the theory of fuzzy sets. This model aims to identify important analytical relationships between the parameters of social systems and the dynamics of information exchange. The developed model is implemented in the form of algorithmic and software. The calculations carried out with the use of this software made it possible to identify the main regularities of the process of information interaction in social systems, which in turn made it possible to formulate some recommendations for managing this process.

Ключевые слова: математическая модель, распространение информации, информационное управление, противодействие экстремизму, информационный экстремизм, процесс информационного взаимодействия, социальная система, теория нечетких множеств.

Keywords: mathematical model spread of information, information management, countering extremism, information extremism, communication process, social system, theory of fuzzy sets.

1. Введение

Все большее распространение наряду с актами открытой агрессии получают ненасильственные скрытые формы экстремизма, которые основаны на использовании современных средств коммуникации и доступа к информационным ресурсам. Так называемый информационный экстремизм становится одной из наиболее острых проблем в современном социуме. Современные информационно-коммуникационные технологии обладают огромным потенциалом для влияния на сознание социальных групп путем организации и направления процессов массовой коммуникации. Технологический прогресс, значительно повлиявший на процессы социального общения и обмена данными, образование и социализации личности, пополнил арсенал экстремистов современными средствами воздействия на личность и социум в целом. Значительно способствуют распространению идей экстремизма следующие особенности Интернет-коммуникации [4,5,7]:

- резкое ухудшение качества информации;
- увеличение объемов ненужной человеку, «фоновой» информации, что приводит к разрушению барьеров восприятия вредоносной, антисоциальной информации;
- информационные «фантомы» – возможность распространения слухов в виртуальной среде;

Для выработки мер противодействия деструктивным информационным акциям экстремистов необходимо правильно представлять механизмы распространения информации.

2. Постановка задачи

Исходя из этого, актуальной задачей является разработка алгоритмов и моделей, которые позволят исследовать закономерности информационного взаимодействия, проводить мониторинг «информационного фона» и прогнозировать настроения в обществе на разных временных этапах.

3. Разработка методики

Для моделирования процесса информационного взаимодействия (ПИВ) необходимо охарактеризовать социальную систему, в которой происходит обмен информацией. Социальная система (СС) – это сложноорганизованное упорядоченное целое, включающее отдельных индивидов и социальные общности, объединенные разнообразными связями и взаимоотношениями. Значимыми параметрами СС являются связность, коммуникабельность и восприимчивость ее элементов к внешним воздействиям [6].

Поскольку социальным системам имманентно присуща субъективная неопределенность, моделирование происходящих в них процессов превращается в слабо формализуемую проблему [2]. В качестве инструментария для анализа субъективных факторов целесообразно использовать аппарат теории нечетких множеств [1].

Так, для формализации субъективных данных предлагается определить лингвистическую переменную «Уровень фактора» и задать терм-множество ее значений из трех или пяти элементов:

{низкий; средний; высокий}

{сильно отрицательный; отрицательный; нейтральный;

положительный; сильно положительный} (1)

Процесс распространения информации проходит следующим образом. Любая информация вносится в СС в начальный момент времени t=0 некоторым конечным числом ее представителей (назовем их инициирующим множеством). Если информационное воздействие производится осознанно и целенаправленно, члены инициирующего множества, как правило, имеют или активно демонстрируют сильно выраженное положительное или отрицательное мнение относительно этой информации. Дальнейший межличностный информационный обмен обеспечивает доведение информации до сведения остальных участников коммуникации. Целью моделирования ПИВ является определение доли информированных членов СС, а также распределения мнений в терминах множества (1) на каждом шаге t=t+1.

Количество K информированных членов социальной системы на шаге t=t+1 представляет собой зависимость:

$$K_{(t+1)} = K_{(t+1)}\left(L, \bar{b}, q_t, K_{(t)}\right),$$

где L – объем инициирующего множества, $\bar{b}$ – коэффициент связности СС (усредненное количество связей между участниками взаимодействия в системе), q_t – доля участников на шаге t, которые готовы дальше распространять информацию (делать «репост»).

Значение коэффициента q_t зависит от двух факторов – от доли участников с высоким уровнем общительности и от актуальности распространяемой информации на временном шаге t. Уровень общительности является постоянным свойством членов СС, однако актуальность какой-либо информации со временем снижается. Исходя из этого, для определения q_t предложена следующая формула:

$$q_t = Com \bullet Act_t = Com \bullet Act_0 \bullet e^{-\alpha * t / \tau_{act}},$$

где Com – доля участников с высокой коммуникабельностью, Act_0 – начальное значение актуальности информации при t=0 (обычно принимается равным 1); α – коэффициент падения актуальности (согласно многочисленным исследованиям, α=2,3 [3]); τ_{act} – максимальное время сохранения актуальности информации (время ее жизненного цикла).

Исходные данные о количестве связей в системе, коммуникабельности, а также восприимчивости (или, напротив, консерватизме) ее членов для больших СС могут носить характер статистических распределений. То же относится и к имеющемуся начальному распределению мнений в системе по тематике распространяемой информации. Для получения этих данных рекомендуется метод репрезентативного социологического опроса на основе выборочной совокупности, позволяющий экстраполировать выводы на всю социальную систему.

Показатель «уровень восприимчивости» характеризует склонность человека менять свою точку зрения, ориентируясь на мнение окружающих. Значению «низкая восприимчивость» соответствует способность сохранять свое мнение под воздействием информационного фона, а значению «высокая» – значительная степень конформности.

Учитывая все сказанное, можно сформулировать некоторые правила информационного обмена и формирования мнений в СС, допускающие формализацию и автоматизацию математического расчета:

1. Информацией в СС делятся только участники:

— с высокой степенью коммуникабельности;
— с сильно выраженным собственным отношением к этой информации (положительным или отрицательным);

2. Мнение участников с низкой восприимчивостью не меняется, тогда как участники со средней и высокой восприимчивостью, получая эмоционально окрашенные отзывы, меняют свое мнение.
3. Участники со средней восприимчивостью умеренно поддаются стороннему влиянию: переходят от нейтрального мнения – к положительному или отрицательному (или наоборот) от положительного или отрицательного – к сильно выраженному позитивному или негативному отношению, получая соответствующие отзывы от других участников СС.
4. Участники с высокой восприимчивостью довольно легко поддаются давлению окружающих: их мнение «скачет» от отрицательного к положительному, от нейтрального к сильно положительному или отрицательному, в зависимости от стороннего влияния.

Введем следующие обозначения:

— $\omega^{\mathrm{H}}, \omega^{\mathrm{C}}, \omega^{\mathrm{B}}$ – доли членов СС с низкой, средней и высокой восприимчивостью;
— K_t^{++} и ν_t^{++} – соответственно количество и доля участников с сильно положительным отношением к обсуждаемой информации на момент времени *t*;
— K_t^{+} и ν_t^{+} – количество и доля участников с положительным мнением;
— K_t^{H} и ν_t^{H} – количество и доля участников с нейтральным отношением;
— K_t^{-} и ν_t^{-} – участники с отрицательным мнением;
— K_t^{--} и ν_t^{--} – участники, у которых на момент *t* сложилось сильно отрицательное мнение.

Тогда количество информированных членов СС определяется по формуле:

$$K_{t+1} = K_t + q_t \bullet \left(\frac{N - K_t}{N} \right) \bullet \left(K_t^{++} + K_t^{--} \right) \bullet \overline{b},$$

где N – общая численность СС, а коэффициент $\frac{N-K_t}{N}$ отражает долю остававшихся неинформированных участников на предыдущем шаге.

Количество участников с положительным мнением можно рассчитать по следующей формуле:

$$K_{t+1}^{+} = K_t^{+} + (K_{t+1} - K_t) \cdot [\nu_0^{+} - \nu_0^{+} \cdot (\omega^{\mathrm{C}} + \omega^{\mathrm{B}}) \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}} \right) - \nu_0^{+} \cdot (\omega^{\mathrm{C}} + \omega^{\mathrm{B}}) \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}} \right) + \nu_0^{++} \cdot \omega^{\mathrm{C}} \cdot \left(\frac{K^{--}}{K^{++} + K^{--}} \right) + \nu_0^{-} \cdot \omega^{\mathrm{B}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}} \right) + \cdot \nu_0^{\mathrm{H}} \cdot \omega^{\mathrm{C}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}} \right)]$$

Множители $\frac{K_t^{++}}{K_t^{++}+K_t^{--}}$ и $\frac{K_t^{--}}{K_t^{++}+K_t^{--}}$ отражают доли участников информационного обмена, которые делятся с остальными участниками СС сильно выраженным положительным и отрицательным мнением соответственно. По формуле можно видеть, как поддаются их влиянию и меняют мнение в ту или иную сторону (вычитаются или прибавляются) участники со средней и высокой восприимчивостью.

В свою очередь, количество членов СС с сильно позитивным отношением к распространяемой информации вычисляется по следующей формуле:

$$K_{t+1}^{++} = K_t^{++} + (K_{t+1} - K_t) \cdot [\nu_0^{++} - \nu_0^{++} \cdot (\omega^{\mathrm{C}} + \omega^{\mathrm{B}}) \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}} \right) + \nu_0^{+} \cdot (\omega^{\mathrm{C}} + \omega^{\mathrm{B}}) \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}} \right) + \nu_0^{\mathrm{H}} \cdot \omega^{\mathrm{B}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}} \right)]$$

Количество нейтрально настроенных участников:

$$K_{t+1}^{\mathrm{H}} = K_t^{\mathrm{H}} + (K_{t+1} - K_t) \cdot [\nu_0^{\mathrm{H}} - \nu_0^{\mathrm{H}} \cdot (\omega^{\mathrm{C}} + \omega^{\mathrm{B}}) + \nu_0^{-} \cdot \omega^{\mathrm{C}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}} \right) + + \nu_0^{+} \cdot \omega^{\mathrm{C}} \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}} \right) + \nu_0^{++} \cdot \omega^{\mathrm{B}} \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}} \right) + \nu_0^{--} \cdot \omega^{\mathrm{B}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}} \right)$$

Количество участников СС с отрицательным и сильно отрицательным мнением определяется аналогично.

Расчетный пример

Для выявления закономерностей ПИВ приведем пример социальной системы объемом в 10 млн. человек, характеризуемой следующими показателями:

1. Распределение количества связей у участников СС: 80% имели от 1 до 5 коммуникационных связей; у 20% количество контактов было в диапазоне от 6 до 36;
2. Коэффициент восприимчивости чужого мнения для 20% участников оценивался значением «Низкий», для 60% – «Средний» и для 20% – «Высокий»;
3. Начальное распределение мнений в СС относительно распространяемой информации I: $\nu_0^{++} = \nu_0^{--} = 0{,}05$; $\nu_0^{+} = \nu_0^{-} = 0{,}15$; $\nu_0^{\text{H}} = 0{,}6$ (преимущественно нейтральная равновесная среда);
4. Объем инициирующего множества был выбран 0,01% от генеральной совокупности – 1000 человек, имевших сильно выраженное положительное мнение относительно I;
5. Доля участников коммуникации, готовых распространять полученную информацию, на такте t=0 определялась как q0=0,4.

В результате были получены графики нарастания количества информированных агентов, а также распределения мнений участников информационного обмена на каждой итерации (рис. 1).

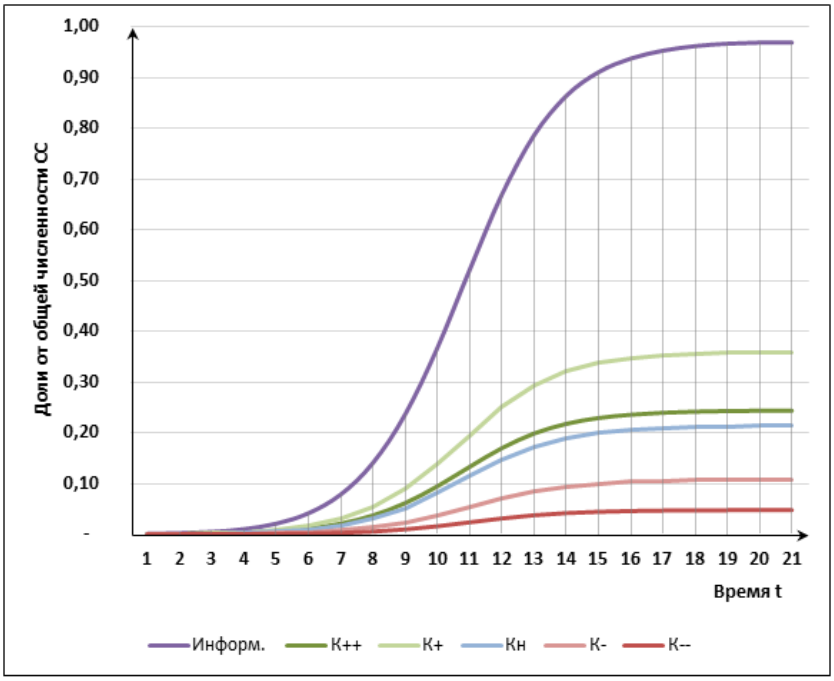

Рис. 1. Графики нарастания количества информированных участников ПИВ и распределения их мнений

Как мы видим, полученные графики имеют форму сигмоиды. Также видно, что с определенного момента наступает резкий рост количества информированных участников, который затем замедляется, и со временем дальнейшая передача информации практически прекращается («вектор информированности» остается постоянным). При этом полная информированность СС не достигается, так как теряется актуальность распространяемой информации. Однако обмен мнениями между участниками может продолжаться дольше – результаты расчетов показывают, что «вектор мнений», хоть и незначительно, но продолжает меняться. Подобное наглядное представление процесса информационного

взаимодействия на основе приведенной модели позволяет определять важные аналитические зависимости между параметрами социальных систем (связностью, восприимчивостью, коммуникабельностью) и динамикой информационного обмена.

4. Результаты

Разработанная модель реализована в виде алгоритмического и программного обеспечения. Приведенные с использованием данного ПО расчеты позволили выявить основные закономерности процесса информационного взаимодействия в социальных системах, что в свою очередь позволило сформулировать некоторые рекомендации по управлению данным процессом.

5. Заключение

Исходя из изложенного, можно предложить некоторые меры воздействия на социальную систему с целью изменения ее характеристик для противодействия распространению вредоносной информации:

1. Дискредитация источника распространяемой деструктивной информации приведет к уменьшению доверия и восприимчивости к ней;
2. Инициирование и запуск другого информационного блока отвлечет участников коммуникации от изначально деструктивной информации, снижая ее актуальность и готовность ее распространять.

Также следует помнить, что наибольший эффект первая мера будет оказывать на начальном этапе распространения информации, пока процесс не перешел в стадию резкого роста, а вторая мера - на стадии резкого роста.

6. Список используемой литературы

[1] Ажмухамедов И. М., Ажмухамедов А. И., Мачуева Д. А. Modeling of communication process in social environment // Journal of Theoretical and Applied Information Technology. 2016. Vol. 85. № 2. P. 146-154.

[2] Ажмухамедов И.М. Синтез управляющих решений в слабо структурированных плохо формализуемых социотехнических системах / И.М. Ажмухамедов // Управление большими системами. – 2013. – № 42. – С. 29-54.

[3] Деревяшко В.В. Влияние фактора старения информации на ее ценность для организации / В.В. Деревяшко // Математические и инструментальные методы экономики. Экономические науки. – 2010. – 1(62). – С. 425-427.

[4] Казарин О.В. Социально-правовые и технологические аспекты проблемы выявления деструктивных информационных воздействий в сети Интернет / О.В. Казарин, В.П. Охапкин, Е.П. Охапкина, Р.А. Шаряпов // Вестник Российского государственного гуманитарного университета. – 2017. – № 3 (9). – С. 132-147.

[5] Проявление экстремизма в молодежной среде – ДВТП // [Электронный ресурс] URL: http://www.dvtp.ru/node/3750 (дата обращения: 26.11.2018)
[6] Мачуева Д.А. Моделирование процесса информационного взаимодействия в социальных системах / Д.А. Мачуева, И.М. Ажмухамедов // Системы управления, связи и безопасности. – 2018. – № 2. – С. 18-39. URL: http://sccs.intelgr.com/archive/2018-02/02-Machueva.pdf
[7] Мозговой В.Э. Информационный экстремизм как инновационная девиация социума начала XXI века / В.Э. Мозговой // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 1. – С. 61-65.

List of references

[1] Azhmuhamedov I. M., Azhmuhamedov A. I., Machueva D. A. Modeling of communication process in social environment // Journal of Theoretical and Applied Information Technology. 2016. Vol. 85. № 2. P. 146-154.
[2] Azhmuhamedov I. M. Synthesis of control solutions in poorly structured poorly formalized socio-technical systems / I.M. Azhmuhamedov // Management of large systems. – 2013 - №42. – p.29-54
[3] Derevyashko V. V. Impact of information aging on its value to the organization / V. V. Derevyashko // Mathematical and instrumental methods economy. Economics. – 2010. – 1(62). – p.425-427
[4] Kazarin O. V. Socio-legal and technological aspects of the problem of identifying destructive information effects on the Internet // O. V. Kazarin, V. P. Ohapkin, E. P. Ohapkina, R. A. Sharyapov // Bullentin of the Russian State University for the Humanities. – 2017. – № 3 (9). – C. 132-147.
[5] The manifestation of extremism in the youth environment - DVTP // [Electronic resource] URL: http://www.dvtp.ru/node/3750 (date of the application: 26.11.2018)
[6] Machueva D. A. Modeling the process of information interaction in social systems / Machueva D. A., Azhmuhamedov I. M., // Control, communication and security systems. – 2018. – № 2. – p. 18-39. URL: http://sccs.intelgr.com/archive/2018-02/02-Machueva.pdf
[7] Mozgovoi V. E. Information extremism as an innovative deviation on the society of the beginning of the XXI century / V. E. Mozgovoi // Humanities, socio-economic and social sciences. – 2015. – № 1. – p.61 – 65.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РЕАЛИЗАЦИИ ЗАЩИЩЁННОГО УДОСТОВЕРЕНИЯ ЛИЧНОСТИ НА ОСНОВЕ СТЕГАНОГРФИЧЕСКИХ И КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Полетаев Н.С.[1]
npoletaev97@gmail.com

Гурская Т.Г.[1]
kafedra_ib_agu@mail.ru

Ажмухамедов И.М.[1]
д.т.н., доцент
iskander_agm@mail.ru

[1] Астраханский государственный университет, г. Астрахань, 414056, Россия

Аннотация

Документы, удостоверяющие личность, играют большую роль в обеспечении личной и общественной безопасности. Однако наиболее широко используемые в настоящее время бумажные документы обладают рядом существенных недостатков. Для их устранения ранее была предложена методика, предусматривающая совместное использование стеганографических и криптографических алгоритмов. В данной работе описываются подходы к реализации программного обеспечения, позволяющего на практике реализовать указанную методику. В программном обеспечении присутствует три основных модуля: модуль шифрования данных; модуль стеганографического внедрения данных в изображение; модуль записи сформированных данных на смарт карту. Использование разработанного ПО позволяет получить документ, удостоверяющий личность, с повышенным уровнем защищённости от атак на его целостность и невозможностью использования третьими лицами, т.к. без знания ключа, часть которого известна лишь владельцу, а другая часть хранится в БД, невозможно расшифровать внедрённую информацию.

Abstract

Identity documents play a big role in ensuring personal security. However, the most widely used paper documents have a number of significant drawbacks; to eliminate them, a technique has been proposed, which involves the joint use of steganographic and cryptographic algorithms. This paper describes the approaches to the implementation of software that allows in practice to implement this technique. There are three main modules in the software: data encryption module; steganographic data embedding module in the image; a module for recording generated data on a smart card. Using the developed software allows you to get an identity document with a high level of protection from attacks on its integrity and the inability to use third parties, because without knowing the key, part of which is known only to the owner and the other part is stored in the database, it is impossible to decrypt the embedded information.

Ключевые слова: электронное удостоверение личности, робастный стеганографический алгоритм, диаграмма потоков данных, криптография, стеганография

Keywords: electronic identity card, robust steganographic algorithm, data flow diagram, cryptography, steganography

1 Введение

Документы, удостоверяющие личность владельца, всегда играли большую роль в обеспечении общественной и личной безопасности [7]. Подобные документы выдаются также сотрудникам на предприятиях для организации пропускного режима. В настоящее время всё ещё широко используются бумажные варианты таких документов. Очевидно, что они обладают рядом существенных недостатков:

- Такие удостоверения более подвержены механическим воздействиям чем электронные документы (например, даже кратковременный контакт с водой может привести информацию, содержащуюся на бумаге, в непригодное для чтения состояние).
- Бумажный документ может быть подделан, передан злоумышленнику.
- Невозможно обеспечить безопасное хранение персональных данных (ПДн) владельца документа, т.к. они хранятся в открытом виде.

Развитие технологии изготовления документов, удостоверяющих личность происходит непрерывно. В настоящее время их развитие связывают с биотехнологиями [8]. Государственные структуры разных стран наблюдают за развитием биометрических системы

и документов на их основе. Результатом становится создание электронных удостоверений личности. В них, помимо фотографии владельца, размещается микропроцессор с собственной памятью, в которую можно записать дополнительную информацию, в том числе и биометрические параметры. Такие документы вводят США, Германия, Великобритания, Япония и т.д. В России также разрабатывает подобный проект [9].

2 Разработка методики

В [3] была предложена схема изготовления автономного электронного удостоверения личности (ЭУЛ) на основе стеганографических и криптографических алгоритмов, позволяющая создать качественно новую идентификационную систему с повешенным уровнем безопасности. Также был разработан алгоритм цифровой стеганографии с шифрованием данных [2], позволяющий решить основную задачу при изготовлении документа, удостоверяющего личность – обеспечение совокупной целостности идентифицирующих человека признаков и персональных данных, указываемых в документе.

Предложенный алгоритм позволяет встраивать данные в графические файл, в том числе сжатые стандартом JPEG. При встраивании данных алгоритм работает с изображениями, глубина цвета которых равна 24 битам. Встраивание выполняется в канал синего цвета, т.к. к нему система человеческого зрения наименее чувствительна.

Пусть сообщение M представляет собой последовательность бит длиной N, количество пикселов в области преобразования равно C. Пикселы, в которые выполняется встраивание, равномерно распределяются по всему изображению псевдослучайным образом на основании ключа. Изображение или его часть, ограниченная областью преобразования, разбивается на два типа блоков r1 и r2, причём r1 = r2 + 1. Количество блоков длины r1 и r2 равно n1 и n2 соответственно. При условии, что n1 + n2 = N и (r1 · n1) + (r2 · n2) = C, значения r1, r2, n1, и n2 вычисляются по следующим формулам:

$$r_2 = C/N \tag{1}$$

$$n_2 = (r_2 + 1) * N - C \tag{2}$$

$$n_2 = (r_2 + 1) \tag{3}$$

$$n_1 = N - n_2 \tag{4}$$

Блоки чередуются псевдослучайным образом на основании ключа. Каждому биту сообщения соответствует свой блок, в котором в соответствии с ключом выбирается пиксел, подвергающийся изменению.

Рассмотрим процедуру формирования ключевой последовательности. Пароль, введённый пользователем, преобразуется в 16-байтовое слово с помощью любого алгоритма хэширования. Далее формируется ещё 3 таких слова путём циклической перестановки. В результате получается массив чисел размерностью [128 бит, 4 бит], столбцы которого представляют собой псевдослучайную последовательность чисел длинной 128 бит. Получая

остаток от деления этих чисел на длину блока, вычисляем позицию изменения пикселя внутри этого блока.

При глубине цвета 24 бита каждая компонента пикселя описывается 8 битами. Изменению подлежат 4, 5 и 6 биты. Отклонение интенсивности цвета в данном случае не превышает 6.3%, а общее изменение яркости пикселя не превышает 1%.

Рассмотрим встраивание информации в изображение. В соответствии с ключом в блоке пикселей выбирается номер пиксел, в который выполняется встраивание. Номер бита определяется на основании значений других пикселей этого де блока. Например, если все четвёртые биты из данного блока равны 0 или 1, то алгоритм оставляет четвёртый бит этого пикселя без изменений и переходит к рассмотрению всех пятых битов данного блока и т.д. Если все четвёртые, пятые и шестые биты всех пикселей из данного блока равны 0 или 1, то предпочтении отдаётся 4 биту. После нахождения номера бита, подлежащему модификации, происходит встраивание секретной информации.

В качестве примера рассмотрим модификацию одного блока изображения. Пусть блок состоит из пяти пикселей.

$$
\begin{array}{l}
b_1 = 1\,1\,1\,1\,0\,1\,1\,0 \\
b_2 = 1\,1\,0\,1\,0\,1\,1\,1 \\
b_3 = 1\,0\,1\,1\,0\,0\,0\,0 \\
b_4 = 1\,0\,1\,1\,0\,0\,0\,1 \\
b_5 = 1\,0\,0\,1\,0\,1\,0\,1
\end{array}
$$

Рисунок 1. Битовое представление синего канала пикселей одного блока

Как видно из рисунка четвёртые и пятые биты не удовлетворяют условию неоднородности. Соответственно согласно алгоритму, только шестой бит может быть модифицирован

3 Постановка задачи

Изложенную выше методику предлагается реализовать в виде программного обеспечения разработанного на языке высокого уровня C# в среде разработки Microsoft Visual Studio 2017 Community.

4 Результаты

Для этого были разработаны соответствующие диаграммы и блок-схемы, отражающие общие принципы работы программы. Ниже, в качестве примера, представлена Use Case диаграмма, которая описывает возможное поведение системы при взаимодействии с администратором. Администратор может выбрать изображение, подлежащее модификации, данные, подлежащие записи. Также он выбирает алгоритм, которым будет осуществляться шифрование. Наконец администратор может записать изображение на смарт карту. Подготовленное изображение с внедрённым стего, содержащим зашифрованные личные данные пользователя, администратор записывает на смарт карту.

Рисунок 2. Use Case диаграмма программного обеспечения для создания ЭУЛ

На следующем рисунке изображена диаграмма потоков данных. В программном обеспечении задействованы три модуля: шифрование данных, стеганографическое внедрение данных в изображение и запись данных на смарт карту.

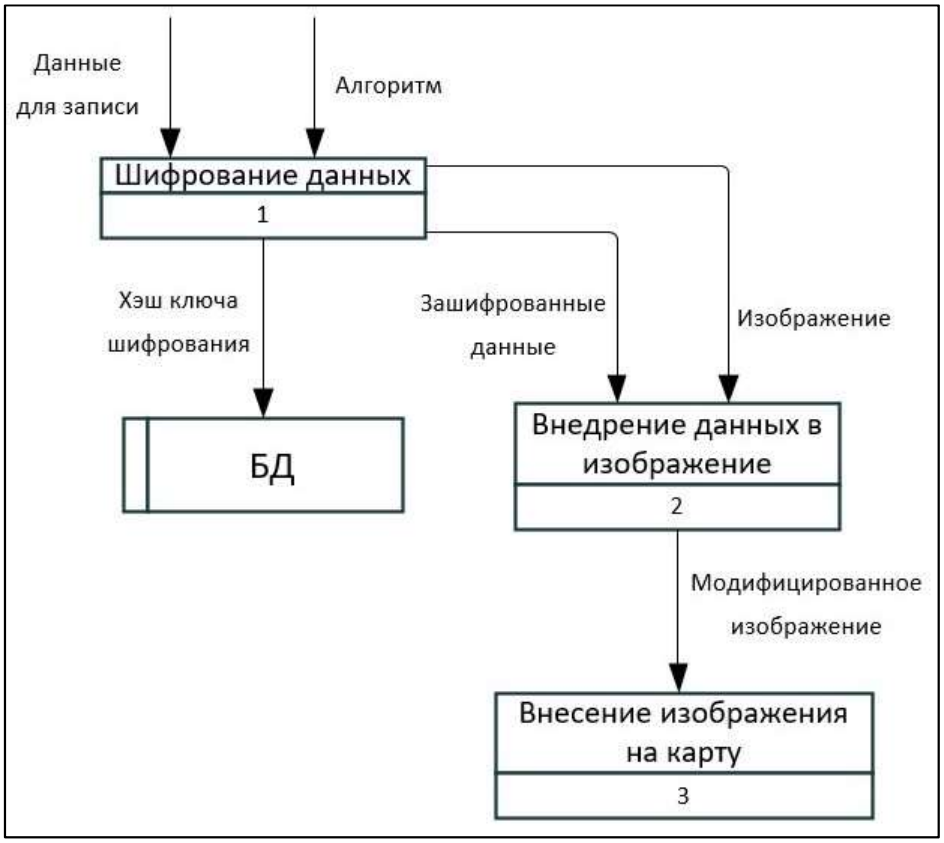

Рисунок 3. Диаграмма потоков данных в нотации Гейна-Сарсона программного обеспечения для создания ЭУЛ

Блок-схема, представленная ниже, отражает работу алгоритма по созданию ЭУЛ. В начале работы программы инициализируются переменные PlainText, Password, Image, Algorithm, в которые записываются данные для шифрования, пароль, введённый пользователем, изображение, подвергающееся модификации и информация выбранном алгоритме шифрования. Разработанное программное обеспечение реализует следующие алгоритмы шифрования: ГОСТ 28147-89 [4], ГОСТ Р 34.12-2015 [5], AES [1]. Далее вызывается функция, которая выполняет шифрование данные. Данная функция имеет три «перегрузки» для каждого алгоритма шифрования. После выполнения криптографических преобразований программа определяет область для внедрения стего. Далее программа генерирует ключевую последовательность на основе пароля, введённого пользователем. Затем выполняется встраивание зашифрованной информации в изображение на основе изложенного выше алгоритма, после чего данные записываются на смарт карту.

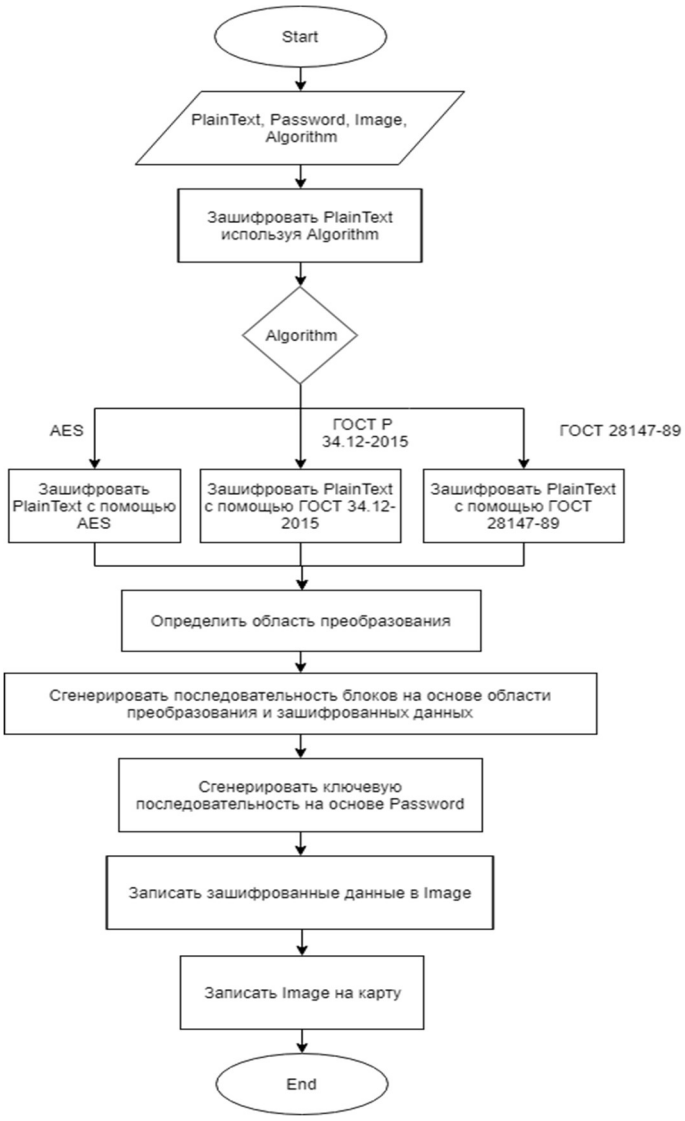

Рисунок 4. Блок-схема работы программного обеспечения для создания электронного удостоверения личности

На следующем рисунке представлен код генерации последовательности блоков.

```
public class BlockCreator
{
    public Point StartPoint { get; set; }
    public Point EndPoint { get; set; }

    public BlockCreator(Point startPoint, Point endPoint) {
        StartPoint = startPoint; //Стартовая точка области преобразования
        EndPoint = endPoint; //Конечная точка области преобразования
    }

    public List<int> GenerateBlockList(string encText) {
        int M = (EndPoint.X - StartPoint.X) * (EndPoint.Y - StartPoint.Y); // Область преобразования

        int encTextLength = encText.Length; // Длина сообщения

        int r2 = (M / encTextLength); // Длина блоков 2 типа
        int r1 = r2 + 1; // Длина блоков 1 типа

        int n2 = (r2 + 1) * encTextLength - M; // Количество блоков 2 типа
        int n1 = encTextLength - n2; // Количество блоков 1 типа

        List<int> Blocks = new List<int>();
        for (int i = 0; i < n2; i++) {
            Blocks.Add(r2);
        }
        for (int i = 0; i < n1; i++) {
            Blocks.Add(r1);
        }

        return Blocks;
    }
}
```

Рисунок 5. Листинг класса, отвечающего за генерацию последовательности блоков

Рассмотрим пример внедрения информации в изображение. Так как человеческий глаз не сможет увидеть изменение изображения, то необходимо проанализировать числовое представление синего канала строки пикселей. Была выбрана область преобразования 10x10 пикселей и строка для внедрения – 1110010000011001111010011010000101001111010010100 1. На рисунке ниже представлен результат работы программы

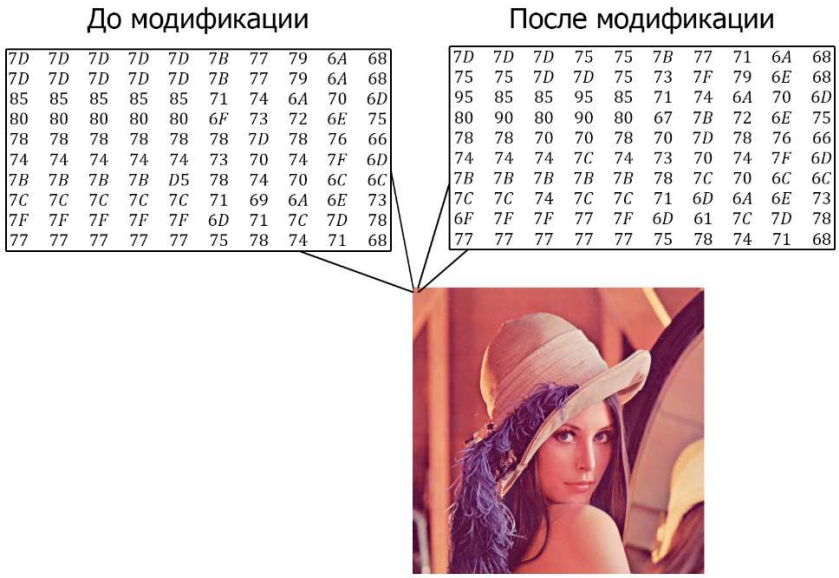

Рисунок 6. Результат работы программы

5 Заключение

Описанный подход к изготовлению электронных документов позволяет свести к минимуму описанные недостатки бумажных документов, удостоверяющих личность. Такой документ защищён от атак на его целостность, т.к. фотография и персональное данные являются единым целым. Также сведена к минимуму возможность использования документа третьими лицами, т.к. без знания ключа, часть которого известна лишь владельцу, а другая часть хранится в БД, невозможно расшифровать внедрённую информацию.

6 Список используемой литературы

[1] Federal Information Processing Standards Publication 197, AES (Advanced Encryption Standard) // https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[2] Ажбаев Т.Г., Ажмухамедов, И.М. Алгоритм цифровой стеганографии с шифрованием данных // Вестн. Астраханского гос. техн. ун-та. – 2008. - №1 (42). – С. 50-55.

[3] Ажмухамедов И.М. Электронные удостоверения личности на основе стеганографических и криптографических алгоритмов. // https://cyberleninka.ru/article/v/elektronnye-udostovereniya-lichnosti-na-osnove-steganograficheskih-i-kriptograficheskih-algoritmov

[4] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. // http://docs.cntd.ru/document/gost-28147-89

[5] ГОСТ Р 34.12-2015. Информационная технология, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ, Блочные шифры // http://wwwold.tc26.ru/standard/gost/GOST_R_3412-2015.pdf

[6] Гуриев В. Восход Европы: электронные паспорта в России // http://www.kongord.ru/Index/BigBrother07/e-pass-in-russ.html.

[7] Кириченко Ю.Н., Медведев А.В. Значение взаимодействия государственных служб Российской Федерации в предупреждении преступлений и правонарушений. Значение перехода на новое удостоверение личности. // https://cyberleninka.ru/article/v/znachenie-vzaimodeystviya-gosudarstvennyh-sluzhb-rossiyskoy-federatsii-v-preduprezhdenii-prestupleniy-i-pravonarusheniy-znachenie

[8] Клак Н.Н. Проблема идентификации человека // https://cyberleninka.ru/article/v/problema-identifikatsii-cheloveka

[9] Указ Президента Российской Федерации от 29 декабря 2012 г. № 1709 «Об основных документах, удостоверяющих личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащих электронные носители информации.»

List of references

[1] Federal Information Processing Standards Publication 197, AES (Advanced Encryption Standard) // https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[2] Azhbaev T.G., Azhmukhamedov, I.M. Digital steganography algorithm with data encryption // Vestn. Astrakhan State. tech. un-that. - 2008. - №1 (42). - p. 50-55.

[3] Azhmukhamedov I.M. Electronic identity cards based on steganographic and cryptographic algorithms. // https://cyberleninka.ru/article/v/elektronnye-udostovereniya-lichnosti-na-osnove-steganograficheskih-i-kriptograficheskih-algoritmov

[4] GOST 28147-89. Information processing systems. Cryptographic protection. Algorithm of cryptographic transformation. // http://docs.cntd.ru/document/gost-28147-89

[5] GOST R 34.12-2015. Information technology, CRYPTOGRAPHIC PROTECTION OF INFORMATION, Block ciphers // http://wwwold.tc26.ru/standard/gost/GOST_R_3412-2015.pdf

[6] Guriev V. Europe's Rise: Electronic Passports in Russia // http://www.kongord.ru/Index/BigBrother07/e-pass-in-russ.html.

[7] Kirichenko Yu.N., Medvedev A.V. The value of the interaction of public services of the Russian Federation in the prevention of crimes and offenses. The value of the transition to a new identity card. // https://cyberleninka.ru/article/v/znachenie-vzaimodeystviya-gosudarstvennyh-sluzhb-rossiyskoy-federatsii-v-preduprezhdenii-prestupleniyiy-i-pravonarusheniy-znachenie

[8] Klak N.N. The problem of human identification // https://cyberleninka.ru/article/v/problema-identifikatsii-cheloveka

[9] Decree of the President of the Russian Federation of December 29, 2012 No. 1709 “On the main documents proving the identity of a citizen of the Russian Federation outside the territory of the Russian Federation, containing electronic data carriers.”

МОНИТОРИНГ ИНФОРМАЦИОННОГО ФОНА В ВУЗЕ НА ОСНОВЕ ПРОТОКОЛА ТАЙНОГО ГОЛОСОВАНИЯ

Александрович В.П.[1]
alexandrovichvalya@gmail.com

Выборнова О.Н.[1]
кандидат технических наук
olga.vyb.90@gmail.com

[1] Астраханский государственный университет (АГУ), г. Астрахань, 414056, Россия

Аннотация

Статья посвящена задаче оценки информационного фона в вузе. Так как вести постоянный мониторинг объективной информации об отношении студентов и сотрудников к различным явлениям внутри вуза порой бывает очень непросто, зачастую в этом помогает простой метод – анкетирование. Анкетирование представляет собой анонимный опрос на определенную тематику с целью выявления недостатков функционирования рабочих процессов внутри вуза и их дальнейшего устранения. Актуальность данной работы заключается в следующем: во-первых, мониторинг информационного фона в вузе обусловлен необходимостью выявления уровня удовлетворенности студентов и преподавателей процессом обучения и качеством образования с целью дальнейшего принятия управленческих решений по совершенствованию системы менеджмента качества вуза. Во-вторых, существующие методы анкетирования в вузе не позволяют респондентам быть уверенными в том, что результаты их голосов не будут подтасованы. В статье сформулированы требования к системе оценки информационного фона в вузе на основе электронного анкетирования. Рассмотрены протоколы тайного голосования, проведен их сравнительный анализ. Для реализации системы выбран

протокол тайного голосования Фудзиока-Окамото-Охта (включая модификацию Sensus).

Abstract

The article is devoted to the problem of assessing the information background in the University. Since sometimes it is very difficult to constantly monitor objective information about the students and teaching staff's attitude towards various phenomena within the University. A simple method like survey often helps with that. The survey is an anonymous questionnaire on a specific topic in order to identify the shortcomings of the working processes within the University and their further elimination. The relevance of this work is as follows: first, monitoring of the information background in the University is due to the need to identify the level of students and teachers' satisfaction with the learning process and the quality of education with the purpose of further managerial decision-making on the improvement of the quality management system of the University; secondly, the existing methods of questioning at the University do not allow respondents to be sure that the results of their votes will not be rigged. The article formulates the requirements to the system of information background assessment in the University on the basis of electronic questionnaire. The protocols of secret ballot are considered; their comparative analysis is carried out. The Protocol of the Fujioka-Okamoto-Ohta secret ballot was chosen (including the Sensus modification) to implement the system

Ключевые слова: защищенная система мониторинга, информационный фон, протоколы тайного голосования, анкетирование, вуз, Фудзиока-Окамото-Охта, Sensus, уровень доверия респондентов.

Keywords: protected monitoring system, information background, secret ballot protocols, questionnaire sur-vey, University, Fujioka-Okamoto-Ohta, Sensus, level of respondents' trust.

Введение

Повышение требований общества к качеству образования, быстроменяющиеся организационные и экономические условия деятельности вузов, усиливающаяся конкурентная борьба на рынке образовательных услуг – всё это заставляет учебные заведения более скрупулёзно следить за своим информационным фоном. Под термином

«информационный фон» понимается соотношение негативных и позитивных высказываний о кадровом составе, инфраструктуре, качестве предоставляемых услуг вуза и других критериев, на основании которых строится репутация всего учебного заведения. Информационный фон представляет собой совокупность мнений всех учащихся данного вуза, профессорско-преподавательского состава и их непосредственных руководителей. Одним из главных факторов, которым руководствуется абитуриент при выборе того или иного вуза является репутация (как положительная, так и отрицательная) [1]. Также мнение близкого окружения абитуриента может сыграть немаловажную роль, в особенности, когда эти люди учились в данном вузе (а, следовательно, были частью информационного фона) и могут дать свою качественную оценку предоставляемых в вузе услуг.

Традиционно анкетирование проводится путём раздачи респондентам бумажных листов с различными вопросами по теме исследования. Однако бурное развитие информационных технологий и средств телекоммуникаций приводит к замене бумажного анкетирования электронным. Именно электронное анкетирование позволяет сократить как время на проведение опроса, привлечение респондентов, подсчет результатов, так и финансовые затраты на распечатку анкет.

Основные задачи статьи: проанализировать существующие методы мониторинга информационного фона в вузе и сформулировать требования для разработки защищенной системы анкетирования на основе протокола тайного голосования.

1 Анализ существующих систем мониторинга в вузе

На сегодняшний день существующие в вузе методы анкетирования можно разделить на два типа: бумажные и электронные.

Процесс анкетирования включает в себя 5 этапов: выбор темы; определение респондентов (кафедра, факультет, весь вуз и др.); проведение анкетирования; обработку анкет (подсчет и анализ распределения голосов); выработку управленческих решений на основе результатов анкетирования. При этом проведение бумажного анкетирования подразумевает распространение и сбор анкет, распечатанных на бумаге, и дальнейшую их обработку вручную. В электронном анкетировании всё намного проще: опрос создается на электронном ресурсе (например, Google Forms), после чего распространяется ссылка на данный ресурс; подсчет результатов анкетирования осуществляется автоматически.

В зависимости от вида респондентов, анкетирование может быть проведено как для студентов, так и для профессорско-преподавательского состава. Например, студентам предлагается анкетирование на темы: «Удовлетворенность студентов процессом обучения в вузе», в котором предлагается ответить на ряд вопросов, касающихся качества организации образовательного процесса, и «Преподаватель глазами студентов», итогом которого является рейтинг самых лучших, по мнению респондентов, преподавателей [2]. Для научно-педагогических работников создаются анкеты, в которых спрашивают о соответствии образования читаемым ими дисциплинам; уровне удовлетворенности материально-техническим обеспечением, библиотечными ресурсами вуза и др.

Как бумажное, так и электронное анкетирования имеют свои достоинства и недостатки. Сравнение приведено в таблице 1.

Таблица 1. Преимущества и недостатки методов анкетирования

Оценка	Анкетирование	
	Бумажное	Электронное
Плюсы	Распространение анкет в пределах одного вуза	Быстрое создание анкеты
	Развернутость	Доступность голосования 24/7
	Дополнительный контроль	Ссылки между вопросами
		Возможность ввода комментария
		Быстрый анализ
		Технический контроль
		Цена ниже бумажного анкетирования
Минусы	Респондент не может удостовериться, правильно ли был зачтен его голос	Респондент не может удостовериться, правильно ли был зачтен его голос
	Возможность подтасовки голосов (заполнение всех анкет одним или несколькими лицами, нацеленными на получение определенных результатов)	Возможность подтасовки голосов (заполнение всех анкет одним или несколькими лицами, нацеленными на получение определенных результатов);
	Возможность раскрытия анонимности анкетирования	Распространение ссылки на опрос за пределы информационного фона
	Отсутствие комментариев в опросном листе	
	Материальные затраты на распечатку анкет и выдачу заработной платы работнику, обрабатывающему результаты анкетирования	

Из Таблицы 1 следует, что электронное анкетирование имеет значительно больше плюсов и меньше минусов по сравнению с бумажным, но такие минусы как «возможность подтасовки голосов» и «респондент не может удостовериться, правильно ли был зачтен его голос» не позволяют респондентам быть уверенными в честности обработки анкет.

2 Формирование требований к процедуре оценки информационного фона

Для повышения уровня доверия респондентов к процедуре оценки информационного фона необходимо создать систему по типу электронного анкетирования, но с учетом устранения/минимизирования в ней вышеприведенных недостатков. Необходимо:

1. Ограничить доступ к анкетированию (т.е. принимать участие в анкетировании могут только зарегистрированные в системе пользователи);
2. Свести количество попыток прохождения анкетирования к одному разу;
3. Позволить респондентам просматривать как общие результаты анкетирования, так и результат обработки своей анкеты (с учетом сохранения тайны голоса).

2.1 Выбор протокола тайного голосования

Для реализации перечисленных требований необходимо рассмотреть системы электронного голосования, в основе которых лежат криптографические протоколы тайного голосования. Брюс Шнайер, один из крупнейших специалистов в области информационной безопасности, выдвинул следующие свойства, которыми должен обладать идеальный протокол электронного голосования [3]:

1. Голосовать могут только те, кто имеет право (легитимные избиратели).
2. При подсчете результатов голосования для каждого избирателя учитывается не более одного голоса.
3. Никто не может узнать, за кого проголосовал конкретный избиратель (т.е. должна обеспечиваться анонимность голосования).
4. Никто не может проголосовать за другого.
5. Никто не может тайно изменить чей-то голос.
6. При подведении итогов голосования избиратель может проверить, что его голос учтен.
7. Каждый знает, кто голосовал, а кто нет.
8. Избиратель может изменить свой голос (т.е., аннулировать свой бюллетень и проголосовать заново) в течение определенного времени.
9. Избиратель может подать протест в случае, если обнаруживает, что его голос засчитан неправильно.

Сравнительный анализ протоколов тайного голосования приведен в Таблице 2.

Таблица 2. Сравнение протоколов тайного голосования

Название протоколов	Свойство								
	1	2	3	4	5	6	7	8	9
Традиционное («бумажное») голосование	+	+	+	-	-	-	+	-	-
Упрощенный протокол голосования №1	-	-	+	-	+	-	-	-	-
Упрощенный протокол голосования №2	+	+	-	-	+	-	+	+	-
Протокол двух агентств Нурми-Саломаа-Сантин	+	+	-	+	+	+	+	+	+
Протоколы двух агентств Фудзиока-Окамото-Охта и Sensus	+	+	+	+	+	+	-	+	+
Протокол голосования с одной ЦИК на базе протокола ANDOS	+	+	+	+	+	+	-	+	+
Протокол голосования с одной ЦИК на базе «слепой» подписи	+	+	+	+	+	+	-	+	+

На данный момент протокол Фудзиока-Окамото-Охта (включая его модификацию протокол Sensus) [4] является одним из самых проверенных протоколов дистанционного электронного голосования. Несмотря на наличие у протокола голосования с одной ЦИК на базе протокола ANDOS аналогичных свойств идеального протокола тайного голосования, он не масштабируем, что неприемлемо при большом количестве избирателей. В свою очередь, протокол Фудзиока-Окамото-Охта уже был апробирован на практике при проведении электронных выборов в Эстонии в 2007 году [5]. Поэтому именно он выбран для реализации системы мониторинга информационного фона в вузе.

Предполагается, что разработанная система будет внедрена в образовательный портал вуза, тем самым решая проблемы, связанные с оповещением респондентов об анкетировании, допуском к анкетированию только субъектов информационного фона вуза, оплатой хостинга на отдельном сайте и др.

Схема голосования согласно протоколу двух агентств Фудзиока-Окамото-Охта представлена на рисунке 1.

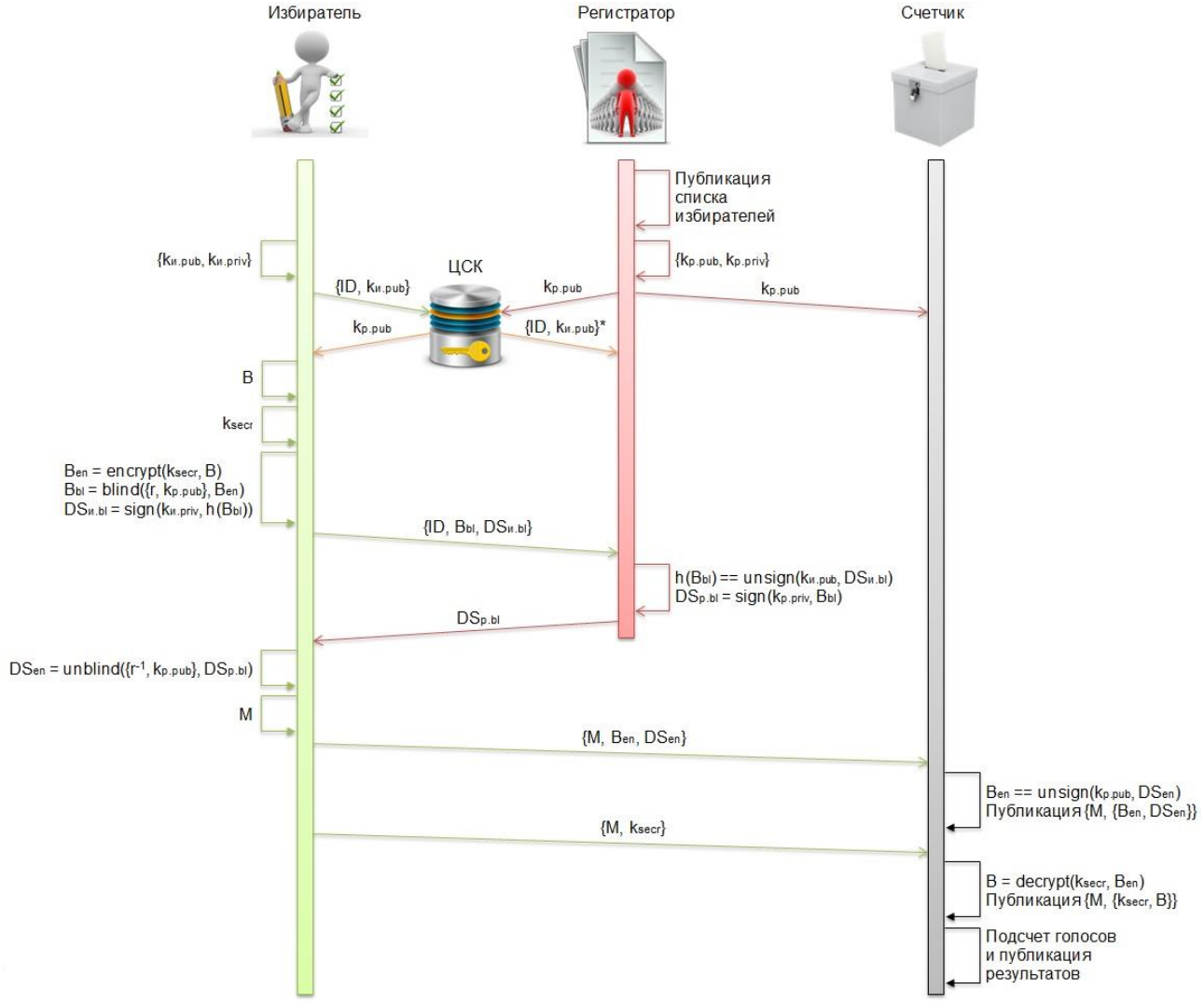

Рисунок 1. Схема протокола двух агентств Фудзиока-Окамото-Охта

2.2 Описание алгоритма работы протокола двух агентств Фудзиока-Окамото-Охта

Шаг 1. Регистратор:

- публикует список всех правомочных избирателей;
- создает пару ключей для асимметричного шифрования {kp.pub, kp.priv};
- публикует открытый ключ kp.pub в ЦСК (центр сертификации ключей). ЦСК может быть независимой организацией или подчиняться регистратору.

Шаг 2. Избиратель:

- создает пару ключей для асимметричного шифрования {ки.pub, ки.priv} и публикует открытый ключ ки.pub в ЦСК. Публикация ключа подразумевает его регистрацию на конкретного избирателя с присвоенным ему ID (у студентов под ID подразумевается номер зачетной книжки, а у преподавателей – номер личного дела);
- создает секретный ключ ksecr;
- делает свой выбор в бюллетене B;
- с помощью секретного ключа ksecr шифрует бюллетень Ben = encrypt(ksecr, B);
- с помощью «закрывающего множителя» r и открытого ключа регистратора kp.pub скрывает содержимое зашифрованного бюллетеня Bbl = blind({r, kp.pub}, Ben);
- с помощью своего закрытого ключа ки.priv стандартным образом (через хеш-образ) подписывает скрытый зашифрованный бюллетень DSи.bl = sign(ки.priv, h(Bbl));
- посылает регистратору свой идентификатор ID, скрытый зашифрованный бюллетень Bbl и ЭЦП к нему DSи.bl.

Шаг 3. Регистратор:

- стандартным образом (через хеш-образ) с помощью открытого ключа избирателя ки.pub проверяет его ЭЦП [6] к скрытому зашифрованному бюллетеню h (Bbl) == unsign (ки.pub, DSи.bl);
- с помощью своего закрытого ключа kp.priv подписывает скрытый зашифрованный бюллетень DSp.bl = sign (kp.priv, Bbl);
- посылает избирателю «слепую» ЭЦП DSp.bl к скрытому зашифрованному бюллетеню Bbl.

Шаг 4. Избиратель:

- снимает «закрывающий множитель» r со «слепой» ЭЦП регистратора DSp.bl и получает ЭЦП регистратора DSen = unblind ({r-1, kp.pub}, DSp.bl) к зашифрованному бюллетеню Ben;
- создает секретную уникальную метку M;
- анонимно посылает счетчику свою метку M, зашифрованный бюллетень Ben и ЭЦП регистратора к нему DSen.

Шаг 5. Счетчик:

- с помощью открытого ключа регистратора kp.pub, высланного напрямую регистратором или полученному из ЦСК, проверяет ЭЦП к зашифрованному бюллетеню Ben == unsign (kp.pub, DSen);
- по истечении времени, отведенного на голосование, публикует все метки M и зашифрованные бюллетени с ЭПЦ к ним {Ben, DSen} в доказательство избирателю, что его голос принят.

Шаг 6. Избиратель:

- анонимно высылает счетчику секретный ключ ksecr для метки M.

Шаг 7. Счетчик:

- с помощью секретного ключа ksecr расшифровывает бюллетень B = decrypt (ksecr, Ben);
- в дополнение к {M, {Ben, DSen}} публикует {M, {ksecr, B}} для того, чтобы избиратель убедился в правильности учета его голоса;
- подводит подсчет голосов;
- публикует результаты голосования.

Достоинства и недостатки. Поскольку никто, кроме избирателя, не может сопоставить одновременно DSen, DSи.bl и DSp.bl, а также ID и M, то исключается раскрытие выбора избирателя (обеспечивается полная анонимность).

Свойство 7 не может быть обеспечено, если только избиратель не раскроет свою личность.

Для изменения выбора избирателя в течение заданного периода времени (свойство 8):

- избирателю вначале необходимо аннулировать свой бюллетень у счетчика с раскрытием своей личности, предоставив {ID, M, ksecr};
- счетчик должен уведомить регистратора, что бюллетень избирателя с конкретным ID аннулирован;
- повторить этапы со 2 по 5.

Раскрытие личности при аннулировании бюллетеня необходимо с целью исключения повторного голосования избирателя.

В протоколе Sensus этапе 5, после проверки подписи регистратора, счетчик сразу высылает избирателю квитанцию с уведомлением, что его голос принят, а избиратель, не дожидаясь конца подачи голосов остальными избирателями, высылает счетчику секретный ключ ksecr [7].

Заключение

В результате выполнения данной статьи были проанализированы существующие методы мониторинга информационного фона в вузе, сформулированы требования для разработки защищенной системы анкетирования на основе протокола Фудзиока-Окамото-Охта и Sensus. Протокол соответствует практически всем техническим требованиям идеального протокола

тайного голосования (кроме возможности опубликования списка проголосовавших). Следовательно, при успешном внедрении протокола в систему электронного анкетирования и дальнейшей его апробации, уровень доверия респондентов к процессу оценки информационного фона в вузе заметно возрастет. Но только с учетом того, что при анкетировании не будут замечены такие махинации как продажа голосов и внесение в список голосующих так называемых «мертвых душ» [8].

Список используемой литературы

[1] Ажмухамедов И.М., Ажмухамедов А.И. Формирование рейтинговой оценки качества образования на основе нечеткой графовой модели // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2012. № 1. – С. 150-157.

[2] Анкетирование «Преподаватель глазами студентов» на факультете бизнеса и экономики АГУ [Электронный ресурс], – URL: http://asu.edu.ru/news/1161-anketirovanie-prepodavatel-glazami-studentov-na-fakultete-biznesa-i-ek.html (дата обращения: 21.11.2018)

[3] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – М.:ТРИУМФ, 2002. – 816 с.

[4] Sensus: A Security-Conscious Electronic Polling System for the Internet [Электронный ресурс]. – URL: http://lorrie.cranor.org/pubs/hicss/hicss.html (дата обращения: 20.11.18)

[5] Электронное голосование в Эстонии, [Электронный ресурс], – URL: https://ega.ee/wp-content/uploads/2016/08/eDem_infomaterjal_i-h22letamine_rus.pdf (дата обращения: 01.12.2018)

[6] Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (последняя редакция) [Электронный ресурс], – URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 18.11.2018)

[7] Протоколы голосования [Электронный ресурс], – URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema15/tema15_3 (дата обращения: 20.11.2018)

[8] Батуев К.А., Кротова Е.Л.. Исследование алгоритмов систем электронного голосования. Автоматизированные системы управления и информационные технологии. Материалы всероссийской научно-технической конференции. В двух томах. Том 2. – Пермь, ПНИПУ, 2017, С. 368-373.

List of references

[1] Azhmukhamedov I.M., Azhmukhamedov A.I. Formation of a rating mark of education quality on the basis of a fuzzy graph model. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravleniye, vychislitel'naya tekhnika i*

informatika [Bulletin of Astrakhan State Technical University. Series: Management, Computer Engineering, and Computer Science]. 2012. №1. 150-157pp. (In Russian)

[2] Questionnaire «Teacher through the eyes of students» at the Faculty of Business and Economics of ASU [Electronic resource], - URL: http://asu.edu.ru/news/1161-anketirovanie-prepodavatel-glazami-studentov-na-fakultete-biznesa-i-ek.html (appeal date: 11/21/2018)

[3] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition. – M.: TRIUMPH, 2002. - 816 p.

[4] Sensus: A Security-Conscious Electronic Polling System for the Internet [Electronic resource]. - URL: http://lorrie.cranor.org/pubs/hicss/hicss.html (appeal date: 11/20/18)

[5] Electronic voting in Estonia, [Electronic resource], - URL: https://ega.ee/wp-content/uploads/2016/08/eDem_infomaterjal_i-h22letamine_rus.pdf (access date: 01/12/2018)

[6] Federal Law «About Electronic Signature» dated April 6, 2011 № 63-FL (last revised) [Electronic resource], - URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (appeal date: 18.11. 2018). (In Russian)

[7] Voting Protocols [Electronic resource], - URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema15/tema15_3 (In Russian)

[8] Batuev K.A., Krotova E.L. Study of algorithms of electronic voting. *Avtomatizirovannyye sistemy upravleniya i informatsionnyye tekhnologii. Materialy vserossiyskoy nauchno-tekhnicheskoy konferentsii. V dvukh tomakh. Tom 2* [Automated control systems and information technology. Materials of the All-Russian Sci. and Techn. Conf. in 2 vol. Vol. 2.]. – Perm, PNRPU, 2017, 368-373pp. (In Russian)

ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ МЕТОДИКИ РАСЧЕТА ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Данилов М.М.[1]
mmdaniloff@mail.ru

Шилина А.Н.[2]
kurnevakatya@mail.ru

Московченко В.М.[2]
fvo.urgpu.npi@yandex.ru

Гайдаревский А.А.[3].
aleksey-gaidarevski@yandex.ru

[1]Академия ГПС МЧС России, г. Москва, 129366, Российская Федерация
[2]Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, г. Новочеркасск, Ростовская обл., 346428,Российская Федерация[3]Калужский филиал московского государственного технического университета имени Н.Э.Баумана, г. Калуга, Калужская область, 248000, Российская Федерация

Аннотация

В работе приведено описание последовательности решения задач управления обеспечением безопасности объектов информатизации, разработаны предложения по совершенствованию методики оценки эффективности качества управления системой обеспечения безопасности.

Abstract

The sequence description of solving the problem about the safety objects management and informatization is provided in work, suggestions for improvement effectiveness assessment of technique andsafety system management quality are developed.

Ключевые слова: информационная безопасность, объект информатизации, автоматизированные системы управления, показатели эффективности управления системой обеспечения безопасности.

Keywords: information security, informatization object, automated control systems, efficiency management factors of the safetysystem

Подобъектоминформатизации(ОИ)определяетсясовокупностьинформационныхресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а так же средств их обеспечения [1]. Значимость обеспечения защиты таких объектов определяется уязвимостью информационной сферы к различным негативным воздействиям[2] вследствие целого ряда факторов, среди которых:

- резко возросшие масштабы информационной инфраструктуры;
- наличие связей объектов информатизации с международными сетями передачи данных и хранения информации;
- политические аспекты мирового содружества и организаций;
- имеющие место компьютерные атаки на объекты критической информационной инфраструктуры [3], а так же сетях электросвязи, используемых для организации и функционирования таких объектов;
- эксплуатации зарубежных средств вычислительной техники.

Для создания современной комплексной системы обеспечения безопасности (СОБ)[4]в этих аспектах становится актуальным создание и использование автоматизированных систем управления (АСУ) для обеспечения безопасности объектов информатизации[5], а так же о проведении оценки их эффективности.

Автоматизированные системы управления в производственных и технологических процессах (АСУ ТП) — это комплекс программных и технических средств, предназначенных для создания систем автоматизации управления технологическим оборудованием и производственными процессами на предприятиях (автоматизация производства) [6]. Основными целями создания и внедрения АСУ являются: повышение качества (эффективности) управления путем упорядочения и ускорения информационных процессов; оптимизация и ускорение оперативно-технических расчетов; научное обоснование принимаемых решений; освобождение должностных лиц от нетворческой (рутинной) работы.

Несмотря на многообразие задач решаемых объектами информатизации различного назначения, звена управления, структурной топологии систем автоматизации, используемых аппаратно-программных средств, методическая основа оценки эффективности СОБ должна быть унифицированной и основываться на существующих методах, применяемых в настоящее время для исследования и оценки характеристик сложных систем [7, 8]. Данную методику следует рассматривать с позиции верифицированности оценки эффективности решения конечных задач стоящих перед системой обеспечения безопасности в целом.

Совокупность свойств СОБ [9] определяется выбранным и обоснованным множеством $\boldsymbol{Z}$показателей качества n_q, определяющих успешность решения стоящих перед СОБ задач:

$$\sum_q^1 n_q \in \boldsymbol{Z},$$

где $q = 1, 2, \dots, \boldsymbol{Z}$.

При этом, значения всех показателей качества СОБ «закрепляются» в ее созданном варианте

$$n_q = n_q(\boldsymbol{X}),\ q = 1, 2, \dots, \boldsymbol{Z},$$

где $\boldsymbol{X}$ – множество реализованных характеристик защищаемого объекта и его СОБ (топология, инженерно-технические средства, алгоритмы работы, численность и квалификация персонала и т.п.).

Отличие показателя эффективности обеспечения безопасности ОИот остальных показателей качества будет заключаться в следующем:

- содержание (вид) показателя эффективности ОИ зависит от конкретной решаемой системой $з_{ij}$-й задачи по обеспечению защиты *i-го*объекта ОИ *от j-го*негативного воздействия, а его величина определяется степенью достижения цели решения этой задачи;
- численное значение показателя эффективности АСУ ОИ$W^{ОИ}$ зависит отчисленного значения функционала показателей её качества, т.е.

$$W^{ОИ} = \sum_q^1 n_{\boldsymbol{Z}}^{ОИ} = W^{ОИ}\left(з_{ij}, n_q^{ОИ} \in \boldsymbol{Z}^{ОИ}, q = 1, 2, \dots, \boldsymbol{Z}^{ОИ} - 1\right). \quad (1)$$

Из выражения(1) следует, что показатели эффективности должны формироваться применительно к конкретной задаче, решаемой СОБ, и определяться степенью достижения цели функционированияОИ.

Величина $W_{ij}^{ОИ}$ показателя эффективности ОИ применительно к конкретной задаче $з_{ij}$, решаемой СОБ, вместе с остальными значениями показателей качества ОИ соответствует определенной величине $W_{ij}^{СОБ}$ показателя эффективности этой системы в целом:

$$W_{ij}^{СОБ} \leftrightarrow W^{ОИ}(з_{ij}, n_q^{ОИ} \in \boldsymbol{Z}^{ОИ}, q = 1, 2, \dots, \boldsymbol{Z}^{ОИ} - 1)$$

В описании показателя эффективности ОИ обозначим через $\boldsymbol{P}$ - множество задач $з_{ij}$, решаемых органов управления СОБ с применением ОИ.

Предположим, что для каждой задачи $з_{ij} \in \boldsymbol{P}$ управления по противодействию $в_j$ (j= 1, 2, …, J) негативному воздействию на i-й (i = 1, 2,…, I)объект безопасности (ОБ) в СОБ определено смысловое и формальное содержание показателя $W_{ij}^{СОБ}$эффективности ее решения. В качестве показателя $W_{ij}^{СОБ}$ могут выступать:

- абсолютная величина снижения вероятности угрозы $в_j$ негативного воздействия на i-й ОБ (с использованием, например, информационной системы анализа и оценки окружающей обстановки);
- степень защищенности i-й ОБ от j-го негативного воздействия (с использованием, например, ОИ управления силами и средствами СОБ);

— степень защищенности i-го ОБот получения недопустимого ущерба l-го вида при реализации j-го негативного воздействия (с использованием, например, системы подготовки принятия решений и оперативного реагирования на чрезвычайные ситуации);
— времяt_i, затраченное на сбор, анализ, обработку и доведение информации до соответствующих должностных лиц или населения (с использованием, например, системы сигнализации и оповещения).

Обозначим через W_{ij}^{+} и W_{ij}^{-} соответственно значения показателя $W_{ij}^{\text{СОБ}}$ при использовании в СОБ исследуемой (предлагаемой к разработке) и существующей ОИ(или при ее отсутствии). Тогда применительно к решению $з_{ij}$-й задачи показатель эффективности $W_{ij}^{\text{ОИ}}$ исследуемой (предлагаемой к разработке) ОИ может быть охарактеризован величинами:

— абсолютное приращение показателя эффективности СОБ:

$$W_{ij}^{\text{ОИ}} = W_{ij}^{+} - W_{ij}^{-}, \tag{2}$$

— относительного приращения этого показателя:

$$W_{ij}^{\text{ОИ}} (W_{ij}^{+} - W_{ij}^{-})/W_{ij}^{-}. \tag{3}$$

Положительное или отрицательное значение показателей $W_{ij}^{\text{ОИ}}$ и $w_{ij}^{\text{ОИ}}$в зависимости от содержания определяет, является ли указанное приращение следствием увеличения или уменьшения эффективности решения $з_{ij}$-й задачи при использовании ОИ.

Выбори обоснование конкретного состава имитационной системы моделирования[10]требует глубокого анализа задач управления, выделения их основных сторон и связей и представляет собой сложную задачу, трудность которой зависит от степени изученности исследуемого процесса управления, полноты и достоверности информации о нем[11].

Символическое описание процесса решения управляющим органом (УО) задач противодействия негативного воздействия представлено на рис. 1.

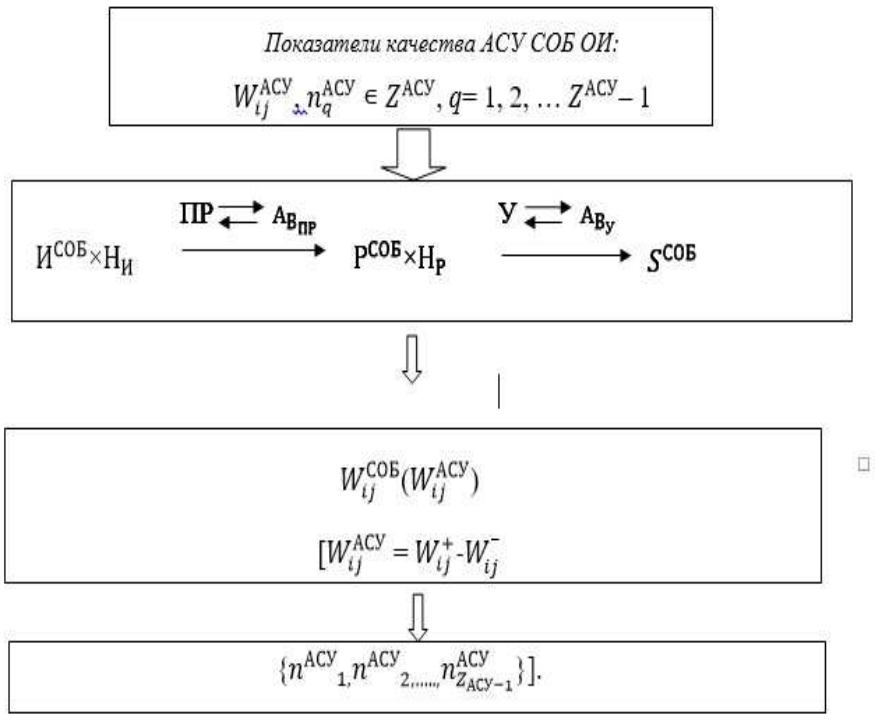

Рис.1 Символическое описание процесса решения задач управления обеспечением безопасности ОИ.

Рассмотрим более подробно структуру предлагаемого процесса решения управляющим органом (УО) задач противодействия негативным воздействиям.

Принятие решения задач управления обеспечением безопасности будет зависеть от $И^{СОБ}$– множестваинформации, поступающей в УО в результате оценки обстановки на каждом этапе управления, при множестве неопределенностей $Н_И$на каждом этапе управления; $Р^{СОБ}$ – множества решений, принимаемых и реализуемых персоналом УО в результате оценки обстановки (анализа информации $И^{СОБ}$), при множестве неопределенностей, сопровождающих рассматриваемый процесс управления $Н_Р$; а так же от $S^{СОБ}$– множества состояний СОБ в результате доведения решений $Р^{СОБ}$ до исполнителей и реализации управляющих воздействий.

Основанием для принятия решения станут механизмы (рабочие алгоритмы) УО процесса подготовки, обоснования и принятия решений $Р^{СОБ}$ – ПР и процессы реализации управляющих воздействий, являющиеся элементами общего алгоритма СОБ противодействия негативному воздействия – У.

Определим под негативным воздействием преднамеренное или непреднамеренное, организованное или случайное действие людей, событие или явление различной природы и характера, являющееся причиной негативных последствий для объекта безопасности в виде ущерба определенного вида и масштаба [9].

Негативные воздействия на процессы принятия решения $В_{ПР}$иуправления$В_У$ будут учтены алгоритмамиОИ$А_{В_{ПР}}$ и$А_{В_У}$соответственно.

Практическая реализация моделив рамках рассмотренной имитационной системы моделирования и использование зависимостей (2), (3) позволяют ответить на вопросы:

- какой является величина показателя эффективности ОИ$W_{ij}^{ОИ}$ при решении $з_{ij}$-й задачи управления при принятых в управляющем органе механизмах (рабочих алгоритмах) ее решения и алгоритмах негативных воздействий$A_{Впр}$ и $A_{Ву}$ на этот орган;
- какой вектор $\{n_1^{ОИ},n_2^{ОИ},\ldots,n_{QОИ-1}^{ОИ}\}$ количественных значений показателей качества ОИ соответствует оцененному значению $W_{ij}^{ОИ}$ показателя эффективности ОИ и показателю $W_{ij}^{СОБ}$ эффективности СОБ в целом.

Представленная в работе модель позволяетсформировать исходные данные и произвести оценкуэффективности функционированияОИпри решении управляющим органомзадачобеспечения безопасности в условиях прогнозируемых негативных воздействий.

Список используемой литературы

[1] ГОСТ Р51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

[2] Доктрина информационной безопасности Российской Федерации (утвержденная 9 сентября 2000 г. Президентом Российской Федерации).

[3] Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а так же объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природы».

[4] Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009.

[5] В.В.Бондарев. Введение в информационную безопасность автоматизированных систем: учебное пособие. – МГТУ им. Н.Э.Баумана, 2016.– 116-123 с.

[6] Федеральный закон от 26 июлю 2017 г. № 187-ФЗ «О безопасности информационной инфраструктуры Российской Федерации».

[7] Чуев Ю.В., Михайлов Ю.Б., Кузьмин В.И. Прогнозирование количественных характеристик процессов. М.: Сов. Радио, 1971.

[8] Михайлов Ю.Б. Математические основы повышения точности прогнозирования количественных характеристик процессов. М.:Научтехлитиздат, 2000.

[9] Теория подобия и моделирования. М.: Известия, 1951.

[10] В.В.Волковицкий, В.В.Волхонский. Системы контроля и управления доступом. СПб.: Экополис и культура, 2003.

[11] Научно-методические основы обеспечения безопасности защищаемых объектов. – М-: Горячая линия – Телеком, 2016. – 322 с.

List of references

[1] State standardspecification P51275-2006. Information security. Informatization object. The factors influencing information. general provision.

[2] The information security doctrine of the Russian Federation (approved on September 9, 2000 by the President of the Russian Federation).

[3] Federal Service for Technical and Export Control order March 14, 2014 No. 31 "About the approval of Requirements to ensuring information security in automated control production systems and technological processes on crucial objects, potentially dangerous objects, and also the objects posing the increased hazard to life and human health and for the environment».

[4] Gatchin Y.A., Klimov E.V.Information security bases: manual. – SPb: St.Petersburg State University of ITMO,

[5] 2009. V.V. Bondarev. Information security of the automated systems introduction: manual. – BMSTU, 2016. – 116-123 pages.

[6] Federal law July 26, 2017 No. 187-FZ "About safety of information infrastructure in the Russian Federation"

[7] Chuyev Y.V., Mikhaylov Y.B., Kuzmin V.I. Prediction of theprocesses quantitative characteristics M.: Sov. Radio, 1971.

[8] Mikhaylov Y.B. The increasing prediction accuracy mathematical bases of the processes quantitative characteristics. M.: Nauchtekhlitizdat, 2000.

[9] Similarity theory and model operations. M.: News, 1951.

[10] V.V. Volkovitsky, V.V. Volkhonsky. Control and access systems management. SPb.: Ecopolice and culture, 2003.

[11] Scientific and methodical bases of protected objects safety.– M-: The hotline - the Telecom, 2016. – 322 pages.

АНАЛИЗ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX

Иниватов Д. П. [1]
daniilini@mail.ru

Данилова О. Т. [1]
к.ф.-м.н., доцент
olga.danlot@yandex.ru

[1] Омский государственный технический университет, г. Омск, 644050, Россия

Аннотация

В настоящей работе представлены результаты по извлечению содержимого криминалистически значимых данных, оставленных вследствие работы пользователя ОС Linux, приводится описание обнаруженной информации, приведены программы, с помощью которых производилось исследование.

Abstract

This article presents the results of extracting the contents of forensically significant data left as a result of the work of the user of the Linux operating system, a description of the detected information, and the programs with which the research was performed.

Ключевые слова: ОС Linux, следообразование, цифровые следы, файл, реестр, удалённый доступ, пользователь, экспертиза.

Keywords: Linux OS, traceability, digital footprint, file, registry, remote access, user, expertise.

В связи с распоряжением Правительства РФ №2299-р от 17 декабря 2010 года−, утверждающим план перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения, а именно переход на операционную систему, основанную на базе ядра Linux, возникает острая необходимость в изучении, модификации и дальнейшем усовершенствовании данного дистрибутива. При этом следует обратить внимание на проблему практического определения тех или иных следов, связанных с несанкционированными действиями пользователя в Unix-подобных операционных системах на базе ядра Linux.

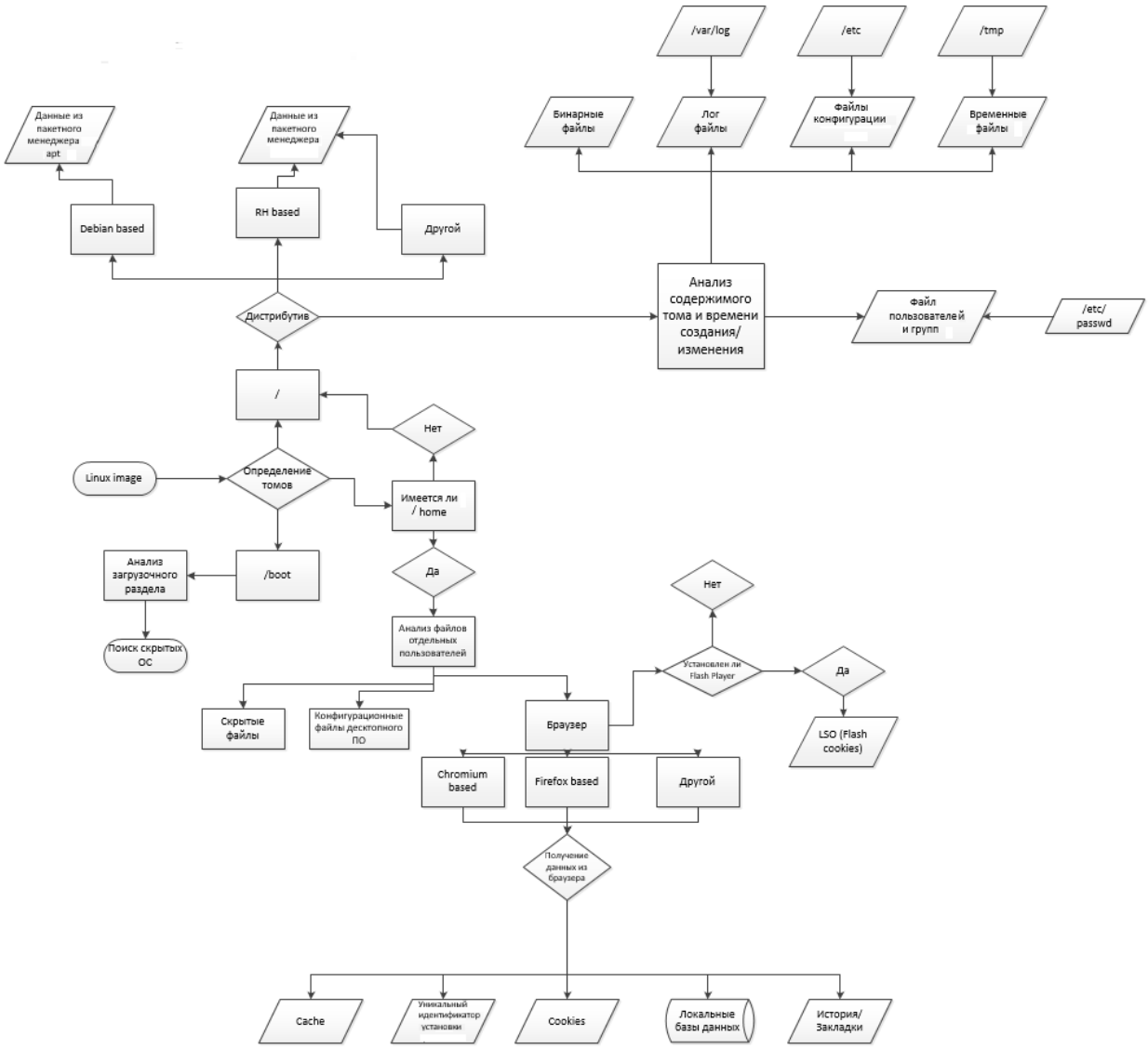

Рисунок 1 – Схема алгоритма исследования цифровых следов в ОС Linux.

При исследовании следует иметь в виду, что одной из отличительных особенностей ОС Linux от Windows является отсутствие реестра, т.е. большинство настроек приложения хранятся в директории /etc − неким аналогом HKLM в ОС Windows, а особый интерес о деятельности пользователя ПК и работы системы представляют файлы журналов, для которых отведена специальная директория /var/log. На рисунке 1 представлена схема алгоритма исследования цифровых следов, связанных с действиями пользователя в ОС Linux.

В настоящей работе анализ проводился с помощью встроенного файлового менеджера в ОС Ubuntu и путём введения команд в терминал. Учтено, что не все файлы являются общедоступными, а значит для открытия таких файлов через терминал необходимо перейти в root-режим. Сделать это можно с помощью команды «sudo -i».

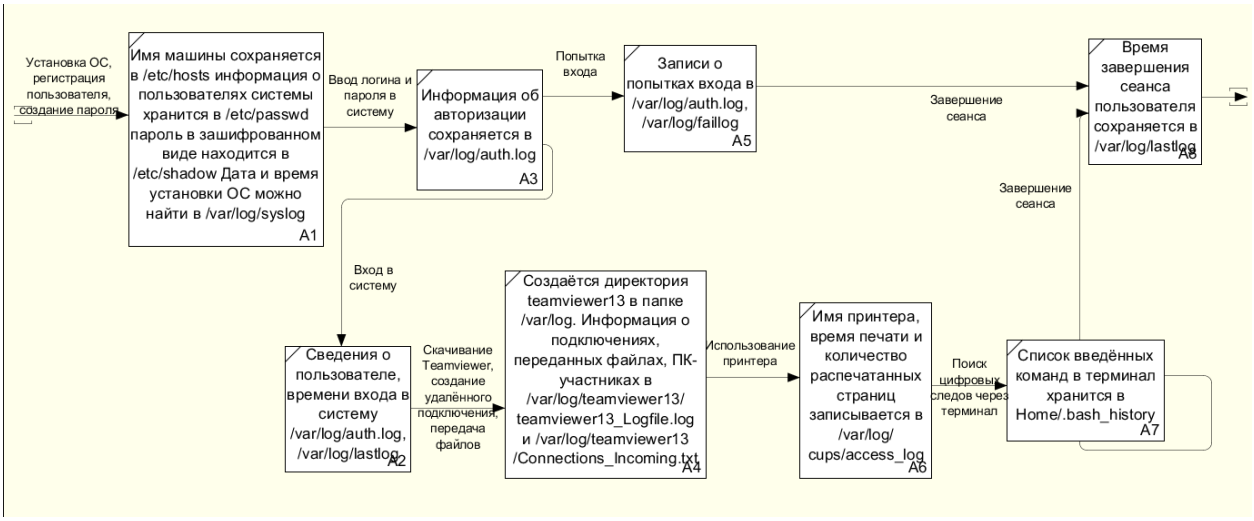

Рисунок 2. Иллюстрация процесса оставления следов пользователем ОС Linux.

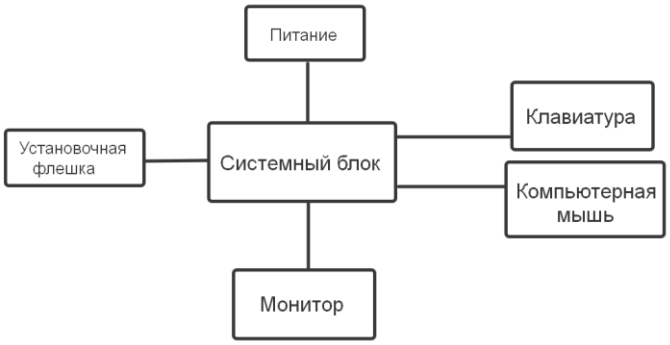

Рисунок 3. Схема учебно-исследовательского стенда

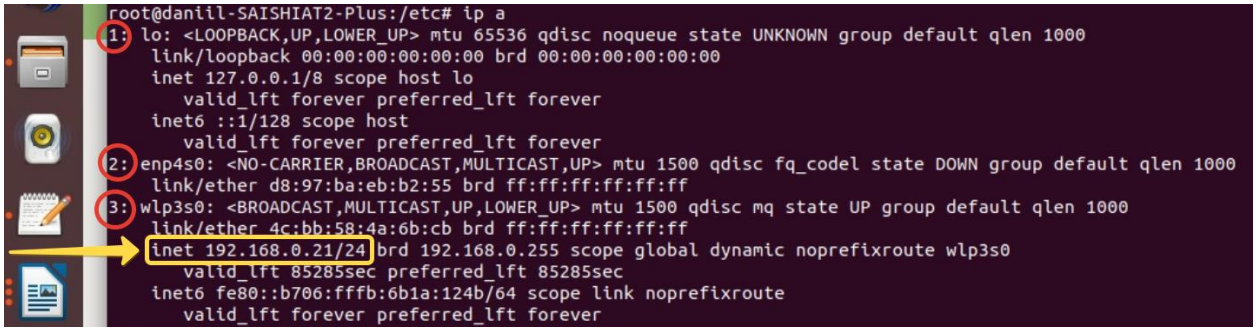

Рисунок 4. Иллюстрация работы в терминале

На рис. 4 показан результат обработки команды «ip a» в терминале ОС Linux. Красным цветом выделены сетевые подключения, жёлтым – IP-адрес компьютера. mtu – это максимальный размер блока данных, обрабатываемых интерфейсом. Файл с настройками интерфейсов хранится в /etc/init.d/network. Имя машины, IP-адрес, имя компьютера хранится в /etc/hostname, IP-адреса хранятся в /etc/hosts.

Рисунок 5. Иллюстрация обработки команды «hostname –I» в терминале.

На рис. 5 представлен IP-адрес машины. Настройки получения ip адреса хранятся отдельно для каждого сетевого интерфейса в файлах /etc/sysconfig/network-scripts/ifcfg-имя_интерфейса, например, eth0. Также данную информацию можно получить в более полном виде, используя команду «ip a». Рис. 3.

```
daniil@daniil-VirtualBox:~$ history
    1  env "PYTHONIOENCODING=UTF-8" "PYTHONUNBUFFERED=1" "PYTHONPATH=/home/danii
l/.vscode/extensions/ms-python.python-2018.6.0/pythonFiles/experimental/ptvsd" p
ython -m ptvsd --host localhost --port 46583
    2  cat /var/log/auth.log
    3  w
    4  jockey-kde
    5  ubuntu-drivers-common
    6  sudo apt-get install jockey-kde
    7  sudo apt-get install ubuntu-drivers-common
    8  jockey-kde
    9  ubuntu-drivers-common
   10  jockey
   11  jockey gtk
   12  jockey-gtk
   13  /home/daniil/Загрузки/uld
   14  /home/daniil/Загрузки/uld/install.sh
   15  sudo
   16  sudo -i
   17  hostname
   18  uname -r
   19  uname -a
   20  ip a
   21  w
```

Рисунок 6. Реализация команды «history» в терминале ОС Ubuntu.

На рисунке выше показана история введённых команд с терминала. Каждая строчка этого файла содержит информацию об одной команде. Данные хранятся в хронологическом порядке. Может находиться не более 500 последних команд. История хранится в ~/.bash_history.

```
localhost - - [26/Sep/2018:14:10:07 +0600] "POST /printers/Samsung_M2020_Series_SEC30CDA7368A3D_ HTTP/1.1" 200 305 Create-
Job successful-ok
localhost - - [26/Sep/2018:14:10:07 +0600] "POST /printers/Samsung_M2020_Series_SEC30CDA7368A3D_ HTTP/1.1" 200 14275 Send-
Document successful-ok
```

Рисунок 7. Иллюстрация содержимого файла var/log/cups/access_log.

На рис. 7 показан файл, хранящий в себе записи о работе пользователя с принтером, названии принтера, времени печати. Первая строка сообщает об успешном создании файла, отправляемого для принтера, вторая – об успешной доставке на принтер.

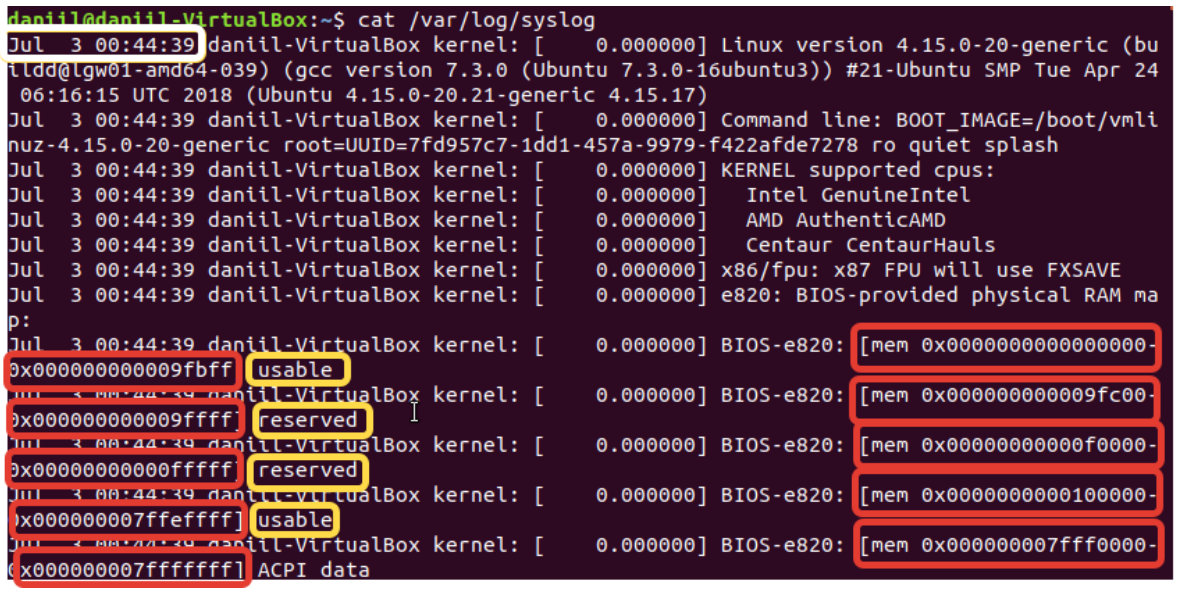

Рисунок 8. Изображение содержимого глобального системного журнала.

На рисунке сверху представлен глобальный системный журнал, содержащий сообщения с момента запуска системы от ядра, различных служб, обнаруженных устройств, сетевых интерфейсов и т.д. Содержит информацию о событии, источник сообщения и описания сообщения. Поможет определить дату и время установки системы (белая рамка), использование (жёлтая рамка) или резервирование областей памяти (красная рамка), хранится в /var/log/syslog. Открытие данного файла было произведено в терминале командой «cat», которая открывает файл для чтения и выгружает в терминал.

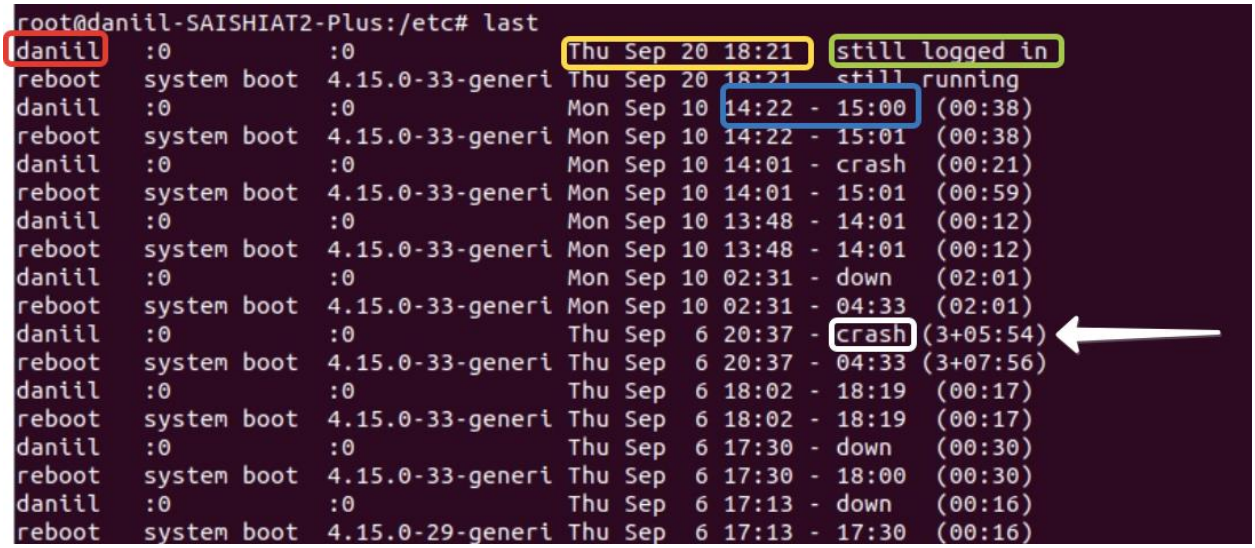

Рисунок 9. Содержание журнала сессий пользователей ОС.

Вышеприведённый журнал ранится в /var/log/lastlog. Получить информацию о его содержимом помимо прямого обращения к нему командой «cat /var/log/lastlog» можно командой last. В данном файле хранится информация о последних сессиях пользователей системы. С помощью этого файла можно определить пользователя системы (красная рамка), дату начала сессии (жёлтая), текущее состояние (зелёная), длительность сессии (синяя) и причину завершения сессии (белая стрелка и рамка), в конкретном примере было отключение питания от сети.

Рисунок 10. Изображение содержимого файла /etc/passwd.

Информация в текстовом формате о пользовательских учётных записях. На рисунке 10 открыта через интегрированное приложение WordPad. На рисунке красным цветом выделен пример информации о пользователе «daniil». Каждая строчка содержит сведения о конкретном пользователе и содержит 7 полей, отделённых друг от друга знаком «:» (выделен жёлтыми рамками), выделим наиболее значимые поля: первое поле – имя пользователя, 3 и 4 поля – user id и group id, UNIX использует user id для определения принадлежности файлов в системе; 6 поле – домашний каталог пользователя для хранения его личных данных, 7 поле – местонахождение программной оболочки, использующейся по умолчанию в терминале для этого пользователя. В данном случае используется bash. Вышеописанная информация хранится в /etc/passwd.

Рисунок 11. Иллюстрация содержимого файла /etc/shadow, открытого через терминал.

daniil:**6YlTGSMah$wLBbbpx0NmtrlAwyPrISgVn3fF0NDxR65lpvWzv1tABGs7zuF2G5gWcUnWtz/YPcOgQLfj.G0HFmBCs9tv14.1**:17780:0:99999:7:::

Текстовое представление, проиллюстрированной на рисунке 11 информации.

Данный файл содержит значения паролей в хешированном по алгоритму MD5 виде во втором поле (выделено жирным шрифтом, на рисунке – красной рамкой). Аналогично предыдущему лог-файлу содержит информацию о пользователях, данные разбиты на поля, отделённые символом «:». Символ «*» говорит, что данная учётная запись временно отключена (вторая строка, второе поле). Третье поле даёт информацию о дате последней смены пароля. В данном примере указано число «17780». Оно говорит о количестве дней, пройденных от 1 января 1970 года.

Оставление следов при удалённом соединении на примере TeamViewer.

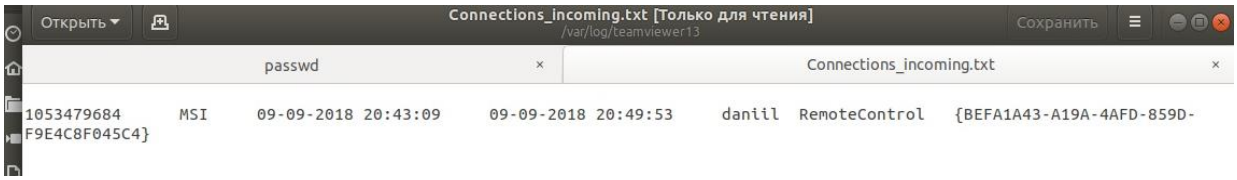

Рисунок 12. Содержимое файл /var/log/teamviewer13/Connections_Incoming.txt

Представленный на 12 рисунке файл содержит краткую информацию о наличии удалённых соединений, предоставляет данные об имени машины партнёра, дате и времени начала и конца соединения.

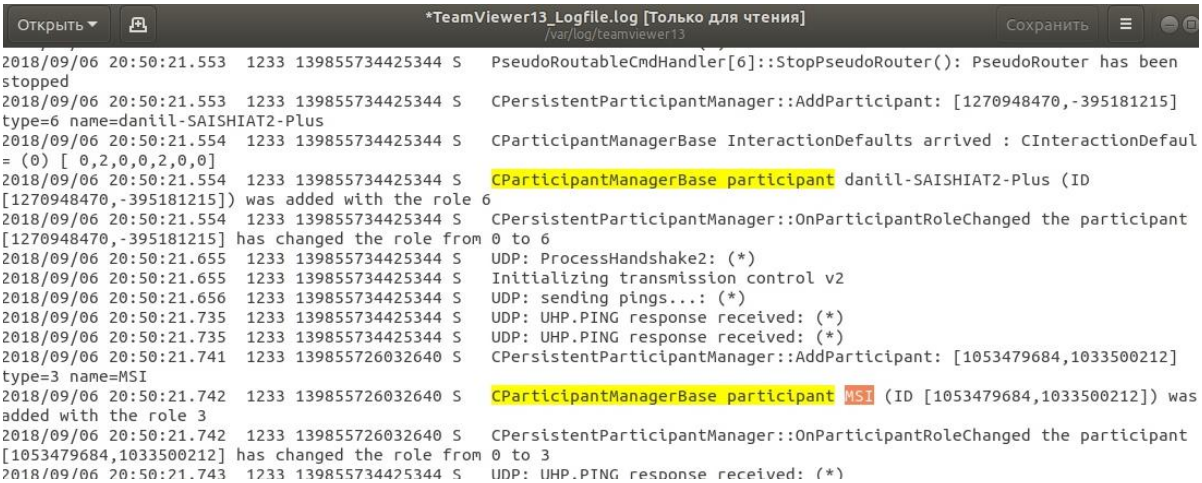

Рисунок 13. Иллюстрация содержимого файла /var/log/teamviewer13/ teamviewer13_Logfile.log.

Проиллюстрированный на рис. 13 файл содержит более подробную информацию об удалённых подключениях, чем файл на рис. 12. Поскольку файл довольно объёмный, будет рациональным решением пользоваться поиском по файлу для выявления наиболее важных мест. Таким образом, можно определить имена компьютеров-участников удалённого соединения, для этого нужно вбить в поиск «CParticipantManagerBase participant», следующее слово-словосочетание будет являться именем ПК-партнёра соединения. Также данный файл содержит информацию о протоколах, через которые были переданы те или иные данные. На вышепроиллюстрированном примере хорошо видно использование протокола UDP.

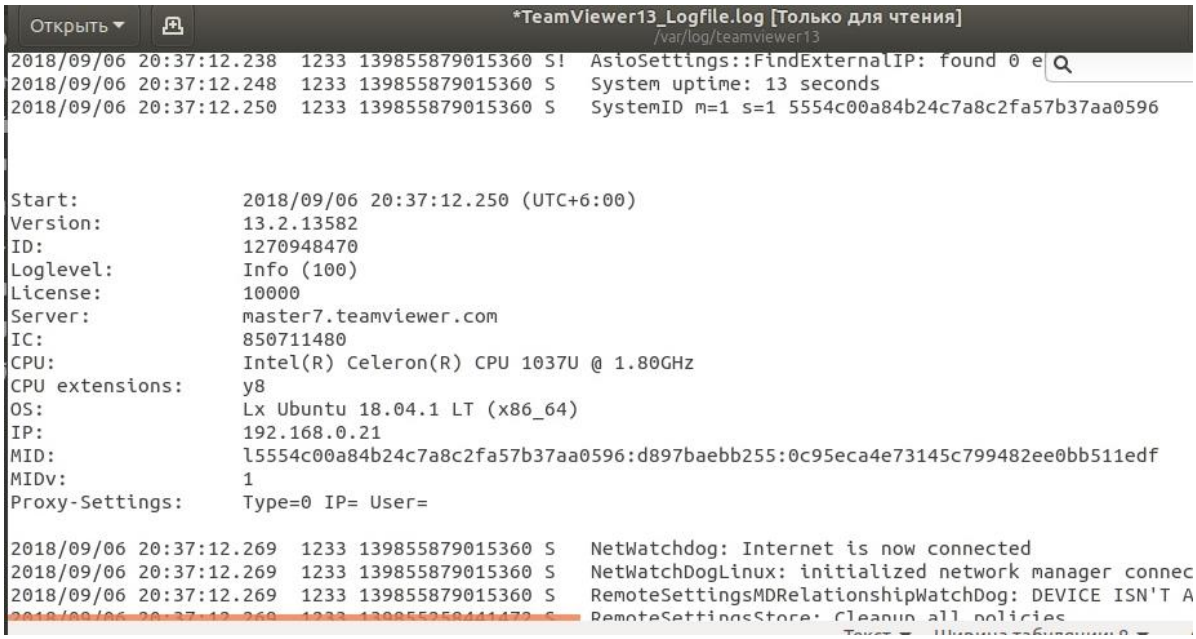

Рисунок 14. Содержимое файла /var/log/teamviewer13/teamviewer13Logfile.log.

Вдобавок к вышеприведённому описанию, данный файл содержит информацию о сервере, через которое было произведено соединение, центральном процессоре ПК, версию ОС, IP-адрес машины, версию программы, время начала соединения, ID соединения.

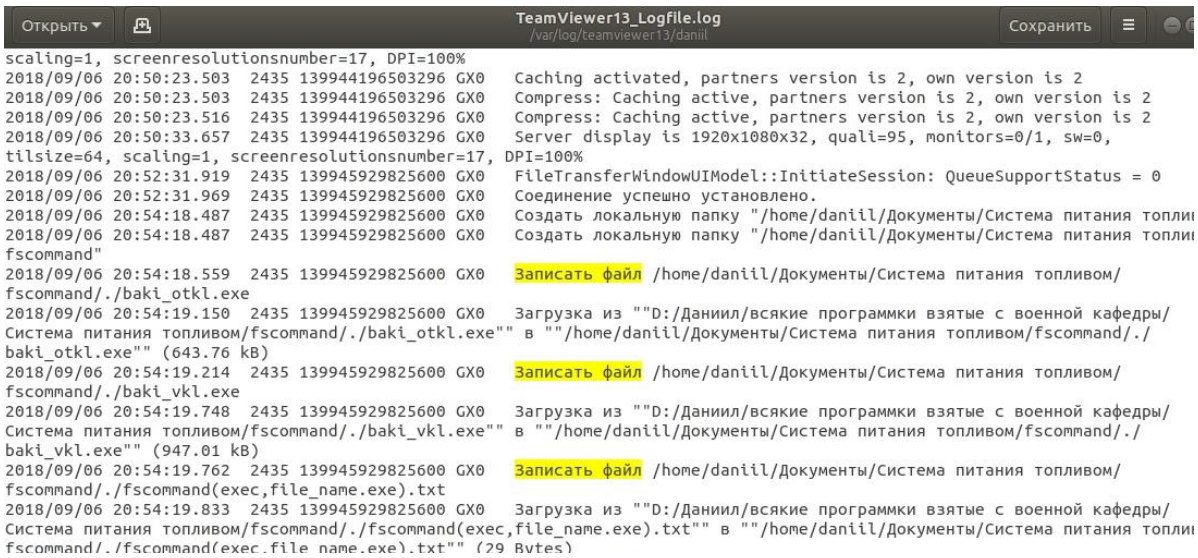

Рисунок 15. Иллюстрация содержимого файла /var/log/teamviewer13/teamviewer13Logfile.log.

Информация о переданных файлах при удалённом соединении. В русскоязычной версии программы teamviewer след о передаче файлов остаётся следующим образом: производится запись «Записать файл» после чего указывается имя директории для записи, следующая строка даёт информацию о том, с какой директории происходит копирование файла у ПК-партнёра соединения. Присутствует информация о дате и времени передачи.

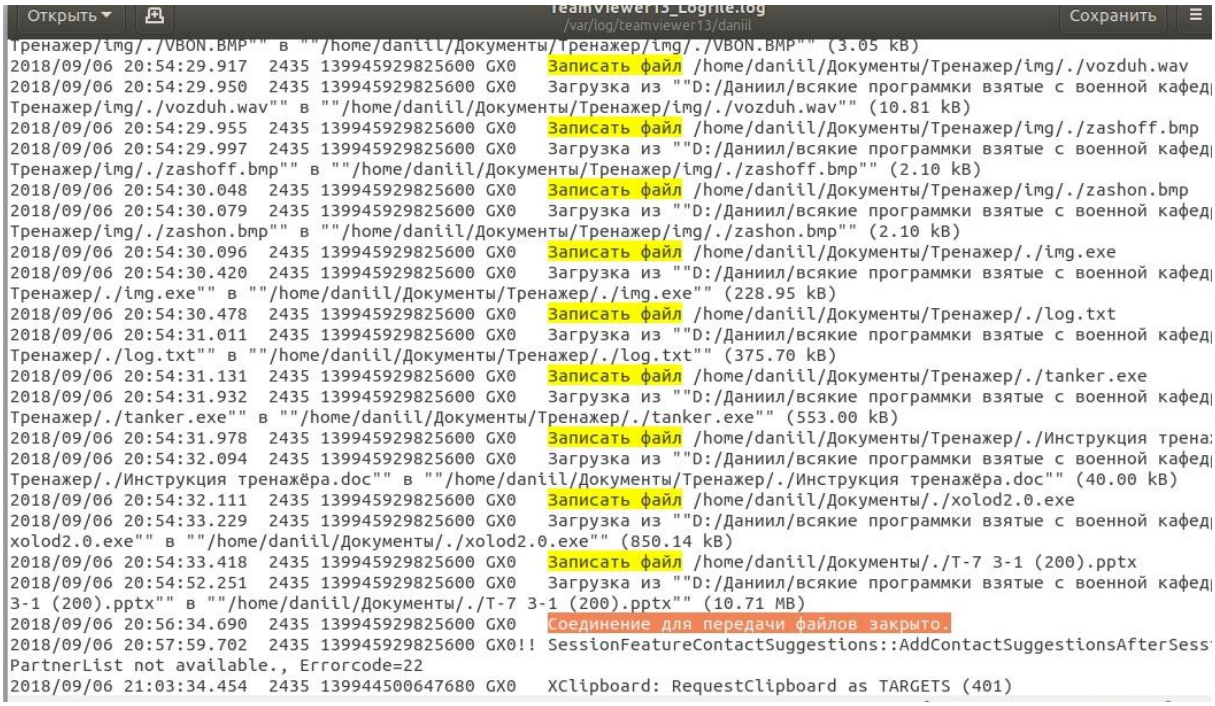

Рисунок 16. Иллюстрация содержимого файла /var/log/teamviewer13/teamviewer13Logfile.log.

На рис. 16 показано сообщение в лог-файле о прекращении удалённого соединения. Окончание передачи файлов определяется записью «Соединение для передачи файлов закрыто».

Вывод: В ходе работы с цифровым носителем информации была создана учётная запись пользователя ОС, совершены различные действия внутри системы, были собраны и

проанализированы оставленные цифровые следы. Итогом работы является определение перечня действий пользователя, которые оставляют свой след в системе:

- Создание учётной записи

- Информация о пароле (наличие его в зашифрованном виде, дата последней смены пароля)

- IP-адрес машины

- Информация о подключениях

- Использование съёмных носителей

- Попытки входа в систему

- Время активности пользователя (сеанс работы)

- Сведения об удалённых подключениях, передаче файлов

- Сведения о пользовании принтером, распечатке документов

- История введённых команд с терминала

Список используемой литературы

[1] Федотов Н.Н. Форензика – компьютерная криминалистика. – М.: Юридический мир, 2007. – 360 с.

[2] Данилова О.Т., Киреев А.П. Разработка модуля выборки файлов, удовлетворяющих входным параметрам: расширению, времени создания, модификации//Хроники объединенного фонда электронных ресурсов «Наука и образование». – 2018. – № 6. – С. 37.

[3] Нехорошев А.Б., Шухнин М.Н. Практические основы компьютерно-технической экспертизы: учебно-методическое пособие. – Саратов: Научная книга, 2007. – 266 с.

List of references

[1] Fedotov N. N. Forensic – computer forensics. – M.: Yuridicheskiy mir, 2007.- 360 p. (In Russian)

[2] Danilova O.T., Kireev A.P. Development of a module for selecting files that satisfy the input parameters: expansion, creation time, modification // Chronicles of the joint fund of electronic resources "Science and Education". - 2018. - № 6. - p. 37. (In Russian)

[3] Nekhoroshev AB, Shukhnin M.N. Practical basics of computer technical expertise: a teaching aid. - Saratov: Scientific book, 2007. - 266 p. (In Russian)

ПОДДЕРЖКА АКТУАЛЬНОГО СОСТОЯНИЯ ПРОГРАММНОГО ОБЕСПЕЧНЕИ КАК СРЕДСТВО ЗАЩИТЫ ДАННЫХ

Калашникова В.А.[1]
Lera_27_07@mail.ru

Жолобов П. А.[1]
Tip4ik26@gmail.com

Филатов А. Д.[1]
alexdmfilatov@mail.ru

Песков М.В.[1]
mvpeskov@hotmail.com

[1]Северо-Кавказский федеральный университет, г. Ставрополь, 355009, Россия

Аннотация

В современном мире пользователи и организации не всегда считают нужным поддерживать актуальность используемого программного обеспечения, тем самым подвергая угрозе не только свои личные данные, но и информацию с ограниченным доступом, которая может стать доступна, как внутренним, так и внешним пользователям.

Самая актуальная причина обновлять программы – это устранение критических уязвимостей в программах, позволяющих злоумышленникам получить доступ к компьютеру, обрабатываемым данным или нанести какой-либо другой вред.

Известны уязвимости в сертифицированных СЗИ от НСД Secret Net 7 и Dallas Lock 8.0, которые широко применяются для защиты информации с ограниченным доступом, включая сведения, составляющие государственную тайну. Таким образом, злоумышленник может попытаться использовать известные уязвимости указанных СЗИ для получения несанкционированного доступа к защищаемой информации.

Было продемонстрировано проведение успешной атаки на компьютер, защищенный СЗИ от НСД Secret Net версии 7.2, и систему, защищенную СЗИ от НСД Dallas Lock 8.0-K.

Таким образом, только поддержка актуального состояния программного обеспечения позволяет защитить данные от несанкционированного доступа, так как можно неограниченно пытаться расширять защиту за счет установки дополнительных «слоев» защиты, однако, все они могут иметь свои уязвимости, пользуясь которыми, злоумышленник может получить доступ к защищаемой информации.

Abstract

In the modern world, users and organizations do not always consider it necessary to maintain the relevance of the software used, thereby putting at risk not only their personal data, but also the information with limited access that can be made available to both internal and external users.
The most actual reason for updating software is to eliminate critical vulnerabilities in programs that allow attackers to gain access to a computer, data, or cause any other harm.
There are known vulnerabilities in certified ISS from NSD Secret Net 7 and Dallas Lock 8.0, which are widely used to protect information with limited access, including information constituting state secrets. Thus, an attacker can attempt to exploit the known vulnerabilities of the specified ISS to gain unauthorized access to the protected information.
A successful attack on a computer protected from the unauthorized access control by Secret Net Version 7.2, and a system protected from the unauthorized access control by Dallas Lock 8.0-K was demonstrated.
Therefore, only the maintenance of the current state of the software allows to protect data from unauthorized access, as you can unlimitedly try to extend protection by installing additional "layers" of protection, however, they all can have their vulnerabilities, using which an attacker can gain access to the protected information.

Ключевые слова: актуальность, программное обеспечение, средства защиты информации, уязвимости, доступ, контроль, Dallas Lock, Secret Net, несанкционированный доступ.

Keywords: software relevance, software, information security tools, vulnerabilities, access, control, Dallas Lock, Secret Net, unauthorized access.

В современном мире пользователи и организации не всегда считают нужным поддерживать актуальность используемого программного обеспечения, тем самым подвергая угрозе не только свои личные данные, но и информацию с ограниченным доступом, которая может стать доступна, как внутренним, так и внешним пользователям.

Хорошо известно, что процесс разработки и сопровождения ПО заключается в постоянном совершенствовании кода своих продуктов. Причин для обновления ПО может быть несколько.

Некоторые обновления приносят с собой новые функции или улучшают уже существующие. Другие обеспечивают совместимость программ друг с другом, с разными протоколами, новыми версиями ОС и т.д. Лучшая совместимость обеспечивает меньшее количество ошибок и сбоев в работе ПО и аппаратных компонентов. Важное место

занимают обновления безопасности: они закрывают уязвимости и исправляют критические ошибки в прикладном и системном ПО (ППО и СПО соответственно).

Когда программная среда работает стабильно, а набор функций устраивает пользователя, у него не возникает желание обновить ПО. Кроме того, большая часть обновлений заключается в приобретении новых версий коммерческих продуктов.

Самая актуальная причина обновлять программы – это устранение критических уязвимостей в программах, позволяющих злоумышленникам получить доступ к компьютеру, обрабатываемым данным или нанести какой-либо другой вред. Особенно уязвимы наиболее популярные и широко распространенные ОС и программы, непосредственно взаимодействующие с сетью Интернет. Поэтому пока существуют пользователи той или иной программы, будут так же существовать злоумышленники, действия которых будут направлены на эксплуатацию известных и поиск новых уязвимостей СПО и ППО, в том числе с использованием вредоносного ПО.

Для существенного повышения защищенности информационных систем применяются специализированные средства защиты информации (далее – СЗИ). Однако не стоит забывать, что реализованные в виде программных или аппаратно-программных комплексов СЗИ так же могут содержать уязвимости.

Таким образом, актуальной задачей является необходимость своевременного обновления не только СПО и ППО, но в особенности СЗИ, так как они являются первым рубежом защиты от несанкционированного доступа к защищаемой информации.

Рассмотрим возможности злоумышленника при использовании в информационных системах неактуальных версий СЗИ.

Известны [1,2] уязвимости в сертифицированных СЗИ от НСД Secret Net 7 и Dallas Lock 8.0, которые широко применяются для защиты информации с ограниченным доступом, включая сведения, составляющие государственную тайну. Таким образом, злоумышленник может попытаться использовать известные уязвимости указанных СЗИ для получения несанкционированного доступа к защищаемой информации.

Продемонстрируем проведение успешной атаки на компьютер, защищенный СЗИ от НСД Secret Net версии 7.2, содержащей уязвимость [1]. Авторизуемся в ОС с ограниченными в соответствии с настроенной политикой безопасности правами пользователя Гость (Рис. 1-2).

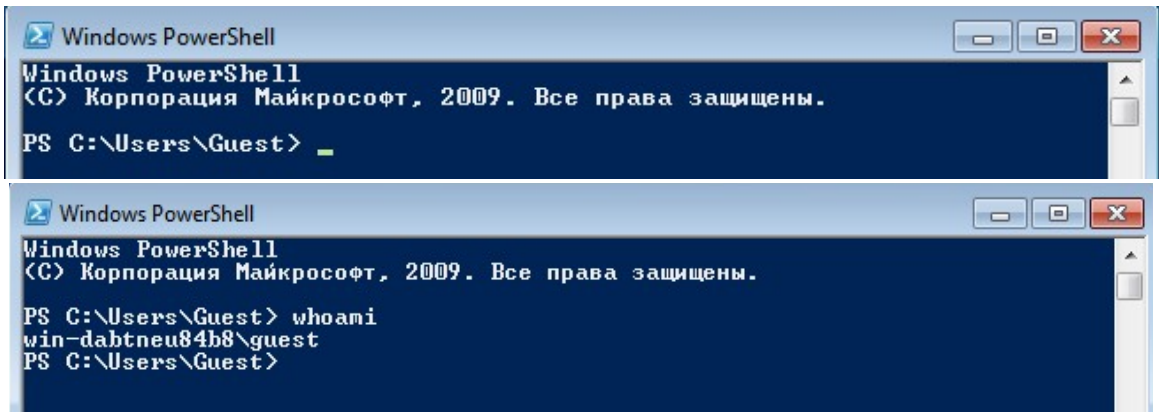

Рисунок 1. Авторизация в ОС с ограниченными правами пользователя

При попытке получения доступа к файлу, которому установлен уровень конфиденциальности, превышающий уровень конфиденциальности пользователя Гость, система защиты Secret Net 7.2 выводит на экран сообщение об отказе в доступе (Рис.2).

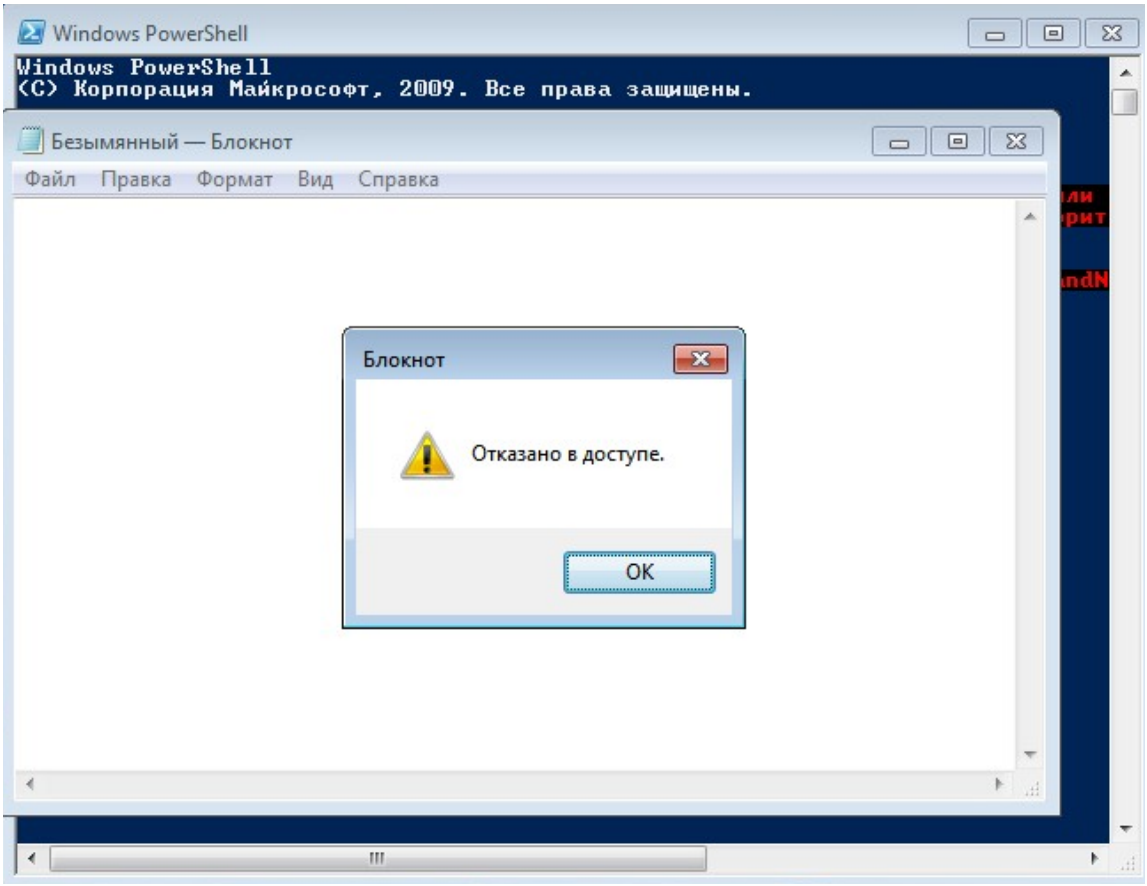

Рисунок 2. Попытка открыть файл пользователем не имеющем права на чтение

Далее воспользуемся приложением-эксплойтом [3], предназначенным для повышения прав доступа пользователя в обход системы защиты (Рис.3).

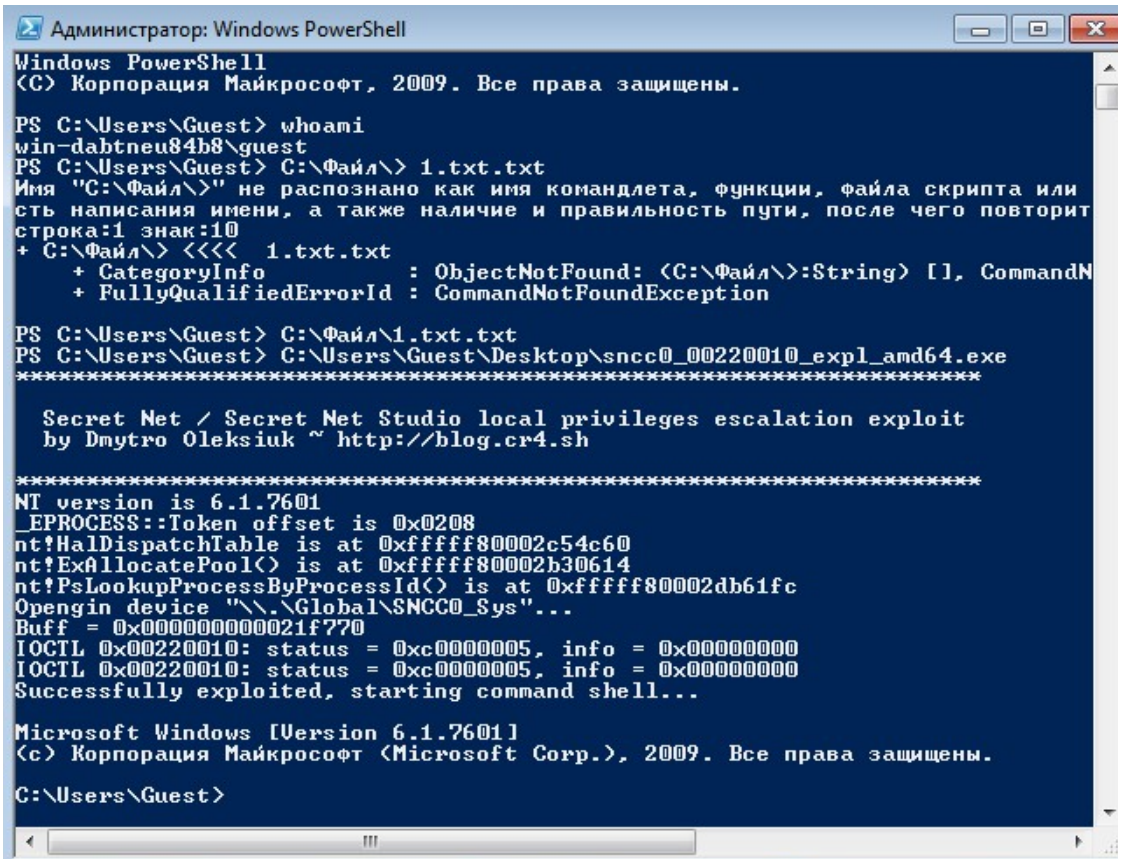

Рисунок 3. Эксплуатируем уязвимость Secret Net 7.2.

В результате атаки права пользователя Гость повышены до уровня прав локальной системы (Рис.4) и получен доступ (Рис.5) к защищаемой информации несмотря на запрет доступа настроенный в политике безопасности Secret Net 7.2.

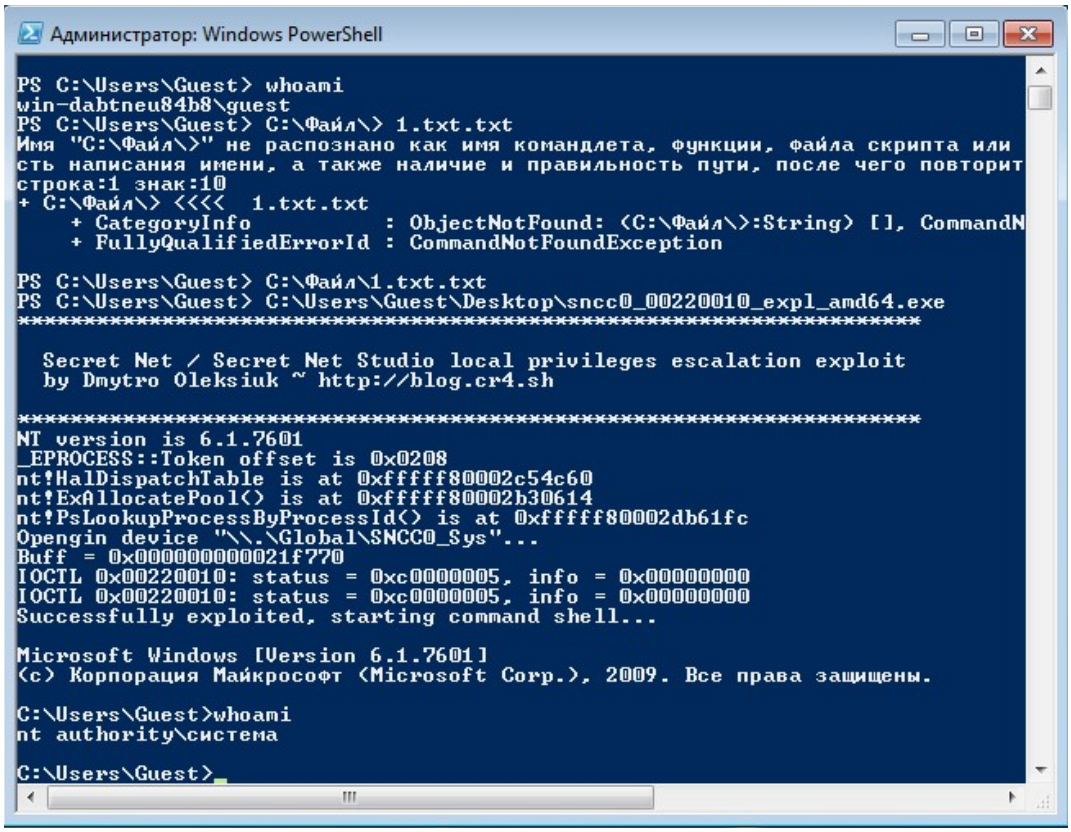

Рисунок 4. Повышаем права пользователя Гость до прав локальной системы

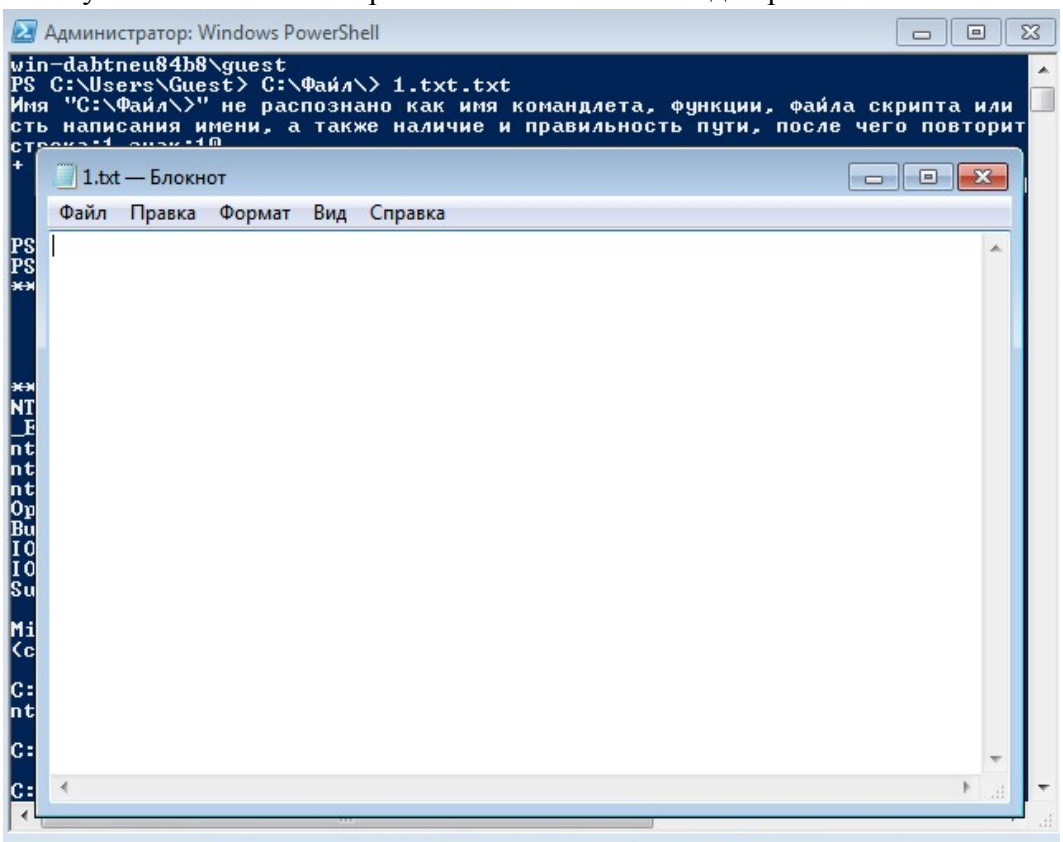

Рисунок 5. Получен доступ к защищаемому файлу

Одним из возможных путей устранения описанной уязвимости [2] может являться настройка замкнутой программной среды (ЗПС). Однако можно показать, что настройка ЗПС не гарантирует устранение других уязвимостей.

Во втором примере, продемонстрируем проведение успешной атаки на систему, защищенную СЗИ от НСД Dallas Lock 8.0-K (сборка 223). Предварительно настроим в системе механизм ЗПС, ограничивающий запуск неизвестного ПО.

Авторизуемся в ОС с ограниченными в соответствии с настроенной политикой безопасности правами пользователя Гость.

Откроем от его имени защищаемый файл с использованием разрешённого механизмом ЗПС приложения NotePad.exe с дополнительным атрибутом потока данных :: $DATA [2, 4].

Результат получения доступа к защищаемой информации в обход СЗИ от НСД Dallas Lock 8.0-K (сборка 223) с использованием уязвимости [2] приведет на Рис. 6.

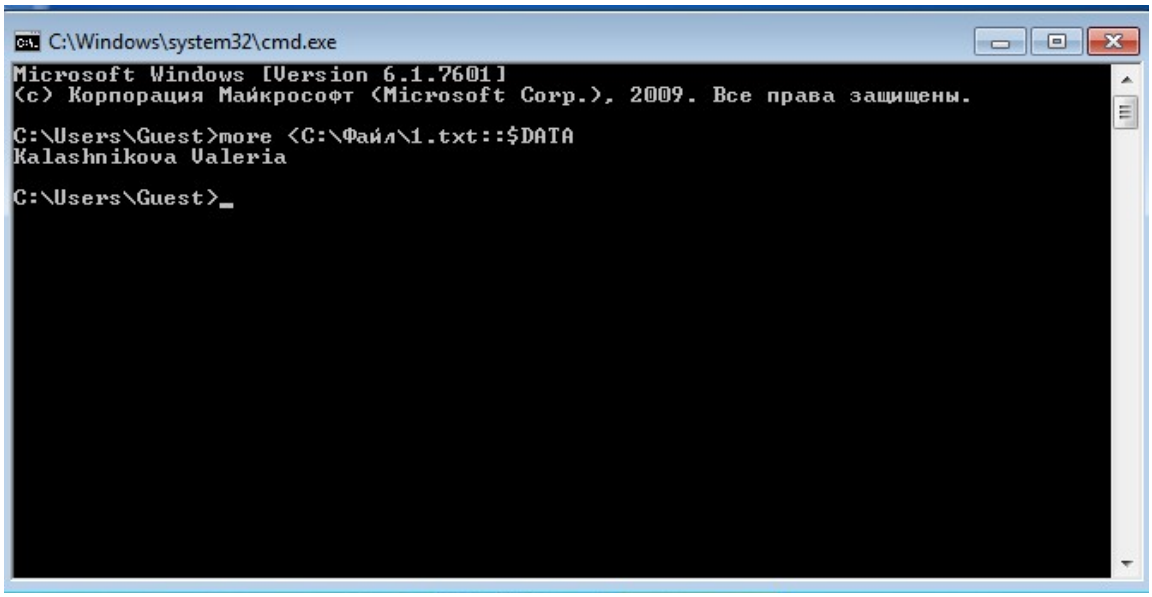

Рисунок 6. Эксплуатация уязвимости Dallas Lock 8.0-K (сборка 223)

При попытке открытия файла с помощью стандартного механизма СЗИ от НСД Dallas Lock 8.0-K выводит сообщение о запрете доступа к защищаемому файлу (Рисунок 7).

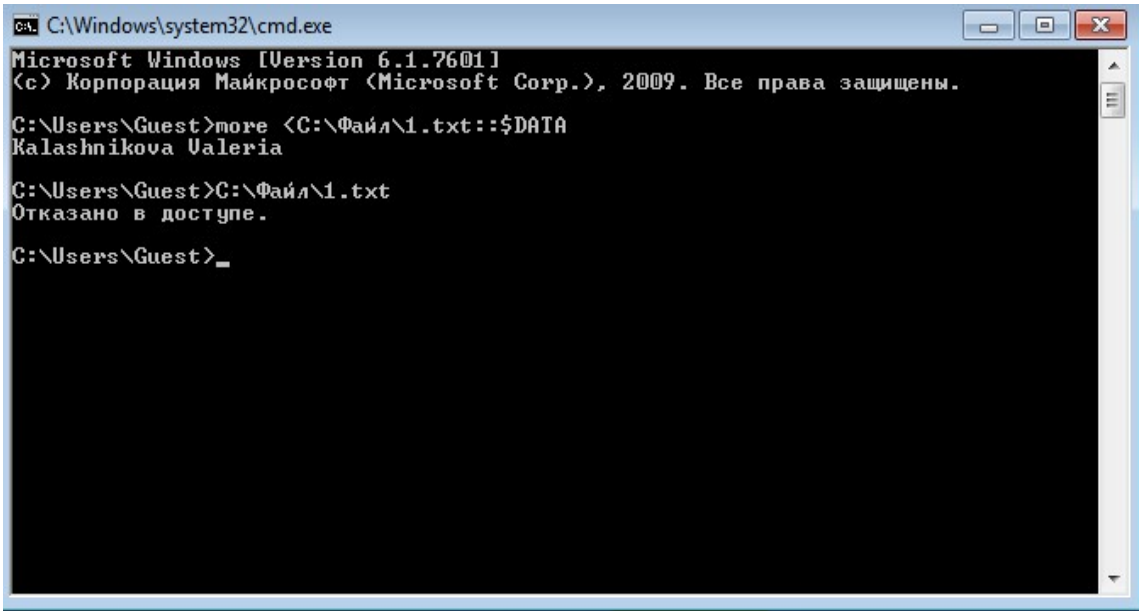

Рисунок 7. Попытка открыть файл в основном потоке вывода

Единственным путем устранить обе уязвимости является обновление в соответствии с [5, 6] уязвимых версий СЗИ от НСД Secret Net 7.2 и Dallas Lock 8.0-K (сборка 223) до актуальных: Secret Net 7.6 и Dallas Lock 8.0-K (сборка 347.4).

Таким образом, только поддержка актуального состояния программного обеспечения позволяет защитить данные от несанкционированного доступа, так как можно неограниченно пытаться расширять защиту за счет установки дополнительных «слоев» защиты, однако, все они могут иметь свои уязвимости, пользуясь которыми, злоумышленник может получить доступ к защищаемой информации.

Список используемой литературы

[1] БДУ – Уязвимости [Электронный ресурс]. URL: http://bdu.fstec.ru/ubi/vul/view/id/17248 (дата обращения: 22.04.2017)

[2] БДУ – Уязвимости [Электронный ресурс]. URL: http://bdu.fstec.ru/ubi/vul/view/id/18489 (дата обращения: 22.04.2017)

[3] URL: https://github.com/cr4sh/secretnet_expl

[4] URL: https://habr.com/post/357122/

[5] URL: https://www.dallaslock.ru/about/news/OBNOVLENIE-SIGNATUR-SOV-DALLAS-LOCK/

[6] Обход правил разграничения доступа в средствах защиты от НСД URL: https:// geektimes.ru/post/276796/ (дата обращения: 22.04.2017)

[7] URL: https://www.dialognauka.ru/press-center/article/16761/

[8] Федеральный закон от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

[9] Информационное сообщение ФСТЭК России от 12.04.2016 г. №240/24/1649 «Об уязвимостях в сертифицированных средствах защиты информации Secret Net и мерах по их нейтрализации».

[10] Информационное сообщение ФСТЭК России от 19.07.2016 г. №240/24/3246 «Об уязвимостях в сертифицированных средствах защиты информации Dallas Lock 8.0».

List of references

[1] Information security threat data bank – vulnerability [Electronic resource]. URL: http://bdu.fstec.ru/ubi/vul/view/id/17248 (date of the application: 22.10.2018)

[2] Information security threat data bank – vulnerability [Electronic resource]. URL: http://bdu.fstec.ru/ubi/vul/view/id/18489 (date of the application: 22.10.2018)

[3] URL: https://github.com/cr4sh/secretnet_expl

[4] URL: https://habr.com/post/357122/

[5] URL: https://www.dallaslock.ru/about/news/OBNOVLENIE-SIGNATUR-SOV-DALLAS-LOCK/

[6] Bypassing the rules of access control in the means of protection from unauthorized access URL: https://geektimes.ru/post/276796/ (date of the application: 22.10.2018)
[7] URL: https://www.dialognauka.ru/press-center/article/16761/
[8] Federal Law of July 26, 2017 No. 187-ФЗ “On the Security of the Critical Information Infrastructure of the Russian Federation”.
[9] Information message FSTEC of Russia from 12.04.2016 №240/24/1649 « On vulnerabilities in certified secret Net information security tools and measures to neutralize them».
[10] Information message FSTEC of Russia from 19.07.2016 №240/24/3246 « On Vulnerabilities in Certified Dallas Lock 8.0 Information Security».

РАЗРАБОТКА ПРОТОКОЛА АУТЕНТИФИКАЦИИ КОСМИЧЕСКОГО АППАРАТА ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ СКРЫТНОСТИ СИСТЕМЫ СПУТНИКОВОЙ СВЯЗИ

Калмыков М.И.[1]
kia762@yandex.ru

Чистоусов Н.К.[1]
kia762@yandex.ru

Степанова Е.П.[1]
kia762@yandex.ru

Калмыков И.А.
д.т.н., профессор
kia762@yandex.ru

[1] Северо-Кавказский федеральный университет, г. Ставрополь, 355028, Российская Федерация

Аннотация

Для организации эффективного контроля и управления необслуживаемыми объектами добычи углеводородов, расположенных в районах Крайнего Севера используются систем спутниковой связи, которые входят в состав автоматизированных системах дистанционного контроля и управления. Так как объекты находятся за Полярным Кругом, то для организации связи необходимо использовать низкоорбитальную группировку космических аппаратов. Чтобы обеспечить достоверный обмен данными между объектами и центром управления в состав группировки входит от 48 до 60 спутников. Проведенные исследования показали, что низкоорбитальная система спутниковой связи обладает целым рядом уязвимостей, что может негативно сказаться на работе. При резком увеличении количества группировок космических аппаратов спутник-нарушитель может воспользоваться следующей уязвимостью. В процессе работы такой спутник сможет перехватить

команду управления, задержать, а затем навязать ее абонентскому терминалу, расположенному на объекте управления. В результате навязанной ретрансляционной помехи работа такого необслуживаемого объекта будет нарушена. Чтобы устранить данную уязвимости предлагается повысить информационную скрытность системы спутниковой связи за счет опознавания спутника. Очевидно, что эффективность работы системы опознавания спутника во многом определяется протоколом аутентификации. Поэтому разработка протокола аутентификации, построенного на основе доказательства с нулевым разглашением знаний, способного опознавать спутник при минимальных затратах является актуальной задачей.

Abstract

For the organization of effective control and management of maintenance-free hydrocarbon production facilities located in the Far North, satellite communication systems are used, which are part of the automated remote control and management systems. Since the objects are located beyond the Arctic Circle, it is necessary to use a low-orbit grouping of spacecraft to organize communication. To ensure reliable data exchange between the objects and the control center, the group includes from 48 to 60 satellites. Studies have shown that the low-orbit satellite communication system has a number of vulnerabilities that can adversely affect the work. With a sharp increase in the number of spacecraft groupings, the offending satellite could take advantage of the following vulnerability. In the process of operation, such a satellite will be able to intercept the control command, delay, and then impose it on the subscriber terminal located on the control object. As a result of the imposed relay interference, the operation of such an unattended object will be disrupted. In order to eliminate this vulnerability, it is proposed to increase the information secrecy of the satellite communication system by identifying the satellite. It is obvious that the effectiveness of the satellite identification system is largely determined by the authentication Protocol. Therefore, the development of authentication protocols, built on the basis of the proof with zero disclosure of knowledge, able to identify the satellite at minimum cost is an urgent task

Ключевые слова: систем опознавания спутника, криптографические протоколы аутентификации типа «запрос-ответ», протоколы аутентификации с нулевым разглашением знаний.

Keywords: identification systems of the satellite, cryptographic authentication protocols of the type "request-response" authentication protocols with zero disclosure of knowledge

Введение

В современных условиях развития технологий добычи и транспортировки углеводородов наблюдается тенденция к более интенсивному использованию природных богатств Крайнего Севера. Так как объекты добычи и транспортировки углеводородов располагаются в малонаселенных районах, то качество контроля и управления такими объектами будет определяться эффективностью работы автоматизированных систем дистанционного контроля и управления. Учитывая то, что объекты управления находятся за Полярным Кругом, для организации обмена данными необходимо использовать низкоорбитальные системы спутниковой связи (НССС). Так период вращения таких спутников невелик, то группировка НССС содержит до 60 космических аппаратов (КА). По мере увеличения числа компаний и стран, приступивших к основанию богатств шельфа Северного Ледовитого океана, будет возрастать число группировок КА. С целью повышения помехозащищенности НССС предлагается усилить ее информационную скрытность путем применения запросно-ответной системы определения статуса КА. Поэтому разработка протокола аутентификации космического аппарата для повышения информационной скрытности системы спутниковой связи является актуальной задачей.

Постановка задачи

Очевидно, имитостойкость системы «свой-чужой», используемой для определения статуса КА, во многом зависит от протокола аутентификации. В настоящее время существует множество таких протоколов типа «запрос-ответ». Наиболее криптоскойкими являются протоколы аутентификации, построенные на доказательстве с нулевым разглашением знаний. Однако, данные протоколы для обеспечения требуемого уровня стойкости к подбору ответов на вопрос требуют многократного обмена данными между претендентом и проверяющей стороной. Поэтому целью работы является разработка протокола аутентификации космического аппарата, построенного на основе доказательства с нулевым разглашением знаний и обладающего минимальным временем необходимым для опознавания КА.

Разработка методики

Проведенные исследования работ [1-3] показали, что наибольшей криптографической стойкостью обладают протоколы аутентификации, построенные на основе доказательства с нулевым разглашением знаний. При этом проведенные исследования показали, что в основе таких протоколов происходит многократный обмен данными между претендентом P и проверяющим V. Рассмотрим протокол аутентификации Фиата-Шамира [4], который содержит два алгоритма, первый из которых используется для получения секретного и открытого ключей:

1. Выбираются два больших простых числа Q и G, которые держатся в секрете. Затем вычисляется произведение $M = Q \cdot G$.Это частью открытого ключа.

2. Претендент P реализует следующие действия:

- осуществляет выбор случайного числа A, для которого выполняется

$$НОД(M, A) = 1, \quad (1)$$

где A – секретное число; $A \in \{1, 2, .., M-1\}$.

- производится выбор числа H, для которого выполняется условие

$$H = A^2 \bmod M. \quad (2)$$

где H – квадратичный вычет по модулю M.

Кроме того, выбранное число H должно иметь мультипликативную инверсию согласно

$$H \cdot H^{-1} \equiv 1 \bmod M. \quad (3)$$

Для данного протокола: секретный ключ A, открытый ключ (M, H).

Для выполнения аутентификации претендента P используется второй алгоритм:

1. Претендент P выбирает случайное число K, где $1 < K < M-1$. Данное число называют обязательством. Используя обязательство, производится вычисление

$$E \equiv K^2 \bmod M. \quad (4)$$

Затем претендент P пересылает число E проверяющей стороне V.

2. Проверяющая сторона V осуществляет выбор случайного числа B, из условия $B \in \{0, 1\}$, которое передается претенденту P.

3. Получив число B, претендент P вычисляет выражение

$$У = K \cdot A^c \bmod M. \quad (5)$$

Если B = 0, то проверяющему передается $У = K$, а если B = 1, то $У = K \cdot A \bmod M$.

4. После получения ответа «У» проверяющая сторона V проверяет правильность ответа:

- если проверочный вопрос B = 0, то вычисляются равенство

$$L = Y^2 \bmod M; \quad (6)$$

- если проверочный вопрос B = 1, то вычисляются равенство

$$L = (Y^2 H) \bmod M. \quad (7)$$

Претендент P аутентифицируется как «свой» при выполнении условия

$$L \equiv E \bmod M. \quad (8)$$

В противном случае – претенденту P присваивается статус «чужой».

Основным недостатком рассмотренных протоколов является низкая скорость аутентификация, которая связана с необходимостью выполнения t = 20-40 циклов проверки для обеспечения требуемого уровня стойкости к навязыванию ложного образа.

Для устранения указанных недостатков был разработан протокол аутентификации типа «запрос-ответ», построенный на доказательстве с нулевым разглашением секрета, который состоит из следующих этапов. На предварительном этапе:

1. Для обеспечения высокой криптостойкости необходимо выбрать большое простое число q. Затем вычисляется число g, с помощью которого можно получить все ненулевые

вычеты по модулю q. Для выполнения аутентификации используются: секретный ключ U, случайные числа S и T, где $1<\{U, S, T\}<q-1$. Последних два числа предназначены для формирования секретного сеансового ключа S(j) и чисел T(j), которые позволяют определять повторное применение сеансового ключа S(j). Для получения сеансовых ключей S(j) и чисел T(j) предлагается использовать разработанную псевдослучайную функцию [5]. Тогда имеем

$$S(j)=g^{\frac{1}{S(j-1)+j+1}} \bmod q,\ T(j)=g^{\frac{1}{T(j-1)+j+1}} \bmod q \qquad (9)$$

где j – номер проводимого сеанса; $S(j=0)=S; T(j=0)=T$.

На этапе работы низкоорбитальной системы спутниковой связи:

1. Для аутентификации КА ответчик, который располагается на борту спутника, вычисляет истинный статус космического аппарата на j-ом сеансе связи, где $U(j)=U$,

$$C(j)=g^{U(j)}g^{S(j)}g^{T(j)} \bmod q, \qquad (10)$$

2. Ответчик реализует процесс «зашумления» секретных данных U, S(j) и T(j), согласно

$$U^*(j)=U+\Delta U(j) \bmod q, \qquad (11)$$

$$S^*(j)=S(j)+\Delta S(j) \bmod q, \qquad (12)$$

$$T^*(j)=T(j)+\Delta T(j) \bmod q, \qquad (13)$$

где $\Delta U(j), \Delta S(j), \Delta T(j)$ – параметры зашумления на j-ом сеансе.

3. Затем ответчик определяет зашумленный статус спутника, согласно

$$C^*(j)=g^{U^*(j)}g^{S^*(j)}g^{T^*(j)} \bmod q. \qquad (14)$$

На этапе аутентификации космического аппарата:

1. При появлении КА в зоне видимости станции спутниковой связи, запросчик, который входит в состав абонентского терминала необслуживаемого объекта, выбирает случайное число d(j), которое удовлетворяет $1<d(j)<q-1$. Это число пересылается спутнику.

2. Ответчик вычисляет ответы на поставленный вопрос d(j), используя выражения

$$r_1(j)=U^*(j)-d(j)U(j) \bmod \varphi(q). \qquad (15)$$

$$r_2(j)=S(j)^*-d(j)S(j) \bmod \varphi(q), \qquad (16)$$

$$r_3(j)=T(j)^*-d(j)T(j) \bmod \varphi(q). \qquad (17)$$

Ответчик передает запросчику сигнал $(C(j), C^*(j), r_1(j), r_2(j), r_3(j))$.

3. Запросчик, получив сигнал $(C(j), C^*(j), r_1(j), r_2(j), r_3(j))$, проводит проверку ответов

$$Y(j)=C^{d(j)}(j)g^{r_1(j)}g^{r_2(j)}g^{r_3(j)} \bmod q. \qquad (18)$$

Проверка будет пройдена, если $Y(j)=C^*(j)$. Тогда запросчик аутентифицирует КА как «свой». В противном случае запросчик присваивает КА статус «чужой».

Для оценки информационной скрытности низкоорбитальной системы спутниковой связи воспользуемся вероятностью пропуска спутника-нарушителя для системы опознавания КА, которая определяется

$$P_{ПС}=\frac{N(i)}{N(max)}P_{ПО}, \qquad (19)$$

где N(i) – количество этапов опознавания спутника при использовании i-го протокола аутентификации; N(max) – максимальное количество этапов в протоколе аутентификации, построенном на основе доказательства с нулевым разглашением знаний; $P_{ПО}$ – вероятность подбора ответа на вопрос запросчика.

При этом вероятность подбора ответа на вопрос запросчика определяется как

$$P_{ПО} = \frac{1}{2^L}, \tag{20}$$

где L – разрядность ответа на поставленный вопрос.

Результаты

Рассмотрим пример реализации данного протокола аутентификации Фиата-Шамира. Пусть выбраны два простых числа p = 5, q = 7. Тогда их произведение будет равно n = 35. Определим квадратичные вычеты по модулю n = 35 из условия

$$u^2 = v \bmod n, \tag{10}$$

где $1 \le u \le n$.

В ходе исследований были найдены следующие значения квадратичных вычетов

$$u = \{1, 4, 6, 9, 11, 14, 15, 16, 21, 25, 29, 30, 34\}.$$

Если значение числа v=16. Тогда обратное мультипликативное значение числа равно его v^{-1}=11, так как $(16 \cdot 11) \bmod 35 = 176 \bmod 35 = 1$.

Вычислим значение секретного ключа. Тогда получаем s = 9, так как $\left|9^2\right|_{35}^{+} \bmod 35 = 11$. Таким образом, получили открытые ключи (n, v) = (35, 11).

Рассмотрим алгоритм аутентификации для данного протокола. Данный порядок операций, выполненный один раз называется аккредитацией.

1. Пусть претендент P выбирает случайное числа r из условия $r \in \{1, 2, .., n-1\}$. Выберем число r = 8. Затем претендент вычисляет значение $x = r^2 \bmod n = 8^2 \bmod 35 = 29$.

Данное значение x=29 передается проверяющему B как свидетельство.

2. Проверяющий абонент V выбирает число c = 0, которое передается претенденту P.

3. Претендент P производит вычисление, используя равенство (6). Так как значение проверочного бита B = 0, то проверяющему абоненту V будет передано число y = r = 8.

4. Проверяющий V, получив ответ, производит проверку согласно условия (7). Тогда

$$z = y^2 \bmod n = 8^2 \bmod 35 = 29.$$

Так как полученное значение делает истинным выражение (8), т.е. $z = x = 29 \bmod 35$, то проверяющий абонент V делает вывод, что - претендент P имеет статус «свой».

Рассмотрим ситуацию, когда проверяющий V пересылает претенденту P значение проверочного бита B = 1. Тогда получаем.

3. Претендент P производит вычисление ответа, при условии B = 1, Тогда имеем

$$y = (rs) \bmod n = (8 \cdot 9) \bmod 35 = 2.$$

4. Проверяющий V, получив ответ, производит проверку согласно условия (7). Тогда

$$z = (y^2 v) \bmod n = (2^2 \cdot 16) \bmod 35 = 29.$$

Так как полученное значение делает истинным выражение (8), т.е. $z = x = 29 \bmod 35$, то проверяющий абонент V делает вывод - претендент P имеет статус «свой».

Рассмотрим выполнение разработанного протокола аутентификации. Пусть задано простое число q = 29, для которого имеется g = 2. Секретным ключом выбираем U = 24., в качестве сеансового ключа S(j) = 16, а параметр T(j) = 25. Воспользуемся выражением (10) и получим истинный статус космического аппарата

$$C = g^U g^S g^T \bmod q = \left|2^{24} \cdot 2^{16} \cdot 2^{25}\right|_{29}^{+} = \left|2^9\right|_{29}^{+} = 19.$$

Истинный статус в коде C = 19 записывается в память КА.

Выбираем «зашумление» равное $\Delta U = 7, \Delta S = 8, \Delta T = 7$. Тогда получаем следующие зашумленные значения U^* = 3, $S^*(j)$ = 24 и $T^*(j)$ = 4. Тогда зашумленный статус равен

$$C^* = g^{U^*} g^{S^*} g^{T^*} \bmod q = \left(2^3 \cdot 2^{24} \cdot 2^4\right) \bmod 29 = 2^3 \bmod 29 = 8.$$

Рассмотрим процесс аутентификации спутника. Запросчик, увидев в космический аппарат, передает случайное число d (j) = 8. Найдем ответы на вопрос. Получаем

$$r_1(j) = \left(U^* - d(j)U\right) \bmod \varphi(29) = \left(3 - 8 \cdot 24\right) \bmod 28 = 7;$$
$$r_2(j) = \left(S^*(j) - d(j)S(j)\right) \bmod \varphi(29) = \left(25 - 8 \cdot 16\right) \bmod 28 = 8;$$
$$r_3(j) = \left(T^*(j) - d(j)T(j)\right) \bmod \varphi(29) = \left(4 - 8 \cdot 25\right) \bmod 28 = 0.$$

Истинный и зашумленный статусы, а также ответы на случайное число d пересылаются запросчик. Запросчик проводит проверку статуса космического аппарата

$$A(j) = C(j)^{d(j)} g^{r_1(j)} g^{r_2(j)} g^{r_3(j)} \bmod q = 2^3 \bmod 29 = 8.$$

Используя равенство $A(j) = C^*(j) \bmod q = 8$, запросчик определяет, что КА является «своим», и между КА и объектом управления проводится обмен данными.

Обсуждение

Проведем сравнительный анализ протоколов аутентификации, построенных на доказательстве с нулевым разглашением знаний. Пусть N(max) = 40. Пусть разрядность всего ответа на вопрос d(j) будет составлять L = 80 разрядов. Тогда разработанный протокол аутентификации и протокол аутентификации Фиата-Шамира будут иметь равные вероятности подбора ответа на вопрос $P_{ПО}(1) = P_{ПО}(2) = 1/2^{80} = 8{,}272 \cdot 10^{-25}$.

Для вычисления вероятности пропуска спутника-нарушителя для системы опознавания КА, использующей протокол аутентификации Фиата-Шамира. воспользуемся (19). Пусть N(1) = 25. Тогда получаем.

Пусть система опознавания КА использует разработанный протокол аутентификации, базирующийся на доказательстве с нулевым разглашением знаний. Для данного протокола количество этапов аутентификации равно N(2) = 2. Тогда значение вероятности пропуска спутника-нарушителя для системы опознавания КА, использующей разработанный протокол аутентификации, будет равно $P_{ПС}(2) = 2P_{ПО}/40 = 4{,}136 \cdot 10^{-26}$. Полученные результаты свидетельствуют о том, что применение разработанного протокола позволяет повысить

информационную скрытность НССС в 12,5 раза по сравнению протоколом аутентификации Фиата-Шамира

Заключение

В статье представлен разработанный протокол аутентификации, базирующийся на доказательстве с нулевым разглашением знаний. Данный протокол позволяет определить статус КА с меньшими временными затратами по сравнению с протоколом аутентификации Фиата-Шамира. Проведенные результаты показали, уменьшение этапов необходимых на определения статуса спутника позволяет повысить информационную скрытность низкоорбитальной системы спутниковой связи. Так при разрядности ответов, равной L = 80 разрядов, использование протокола аутентификации Фиата-Шамира позволяет обеспечить вероятность пропуска спутника-нарушителя для системы опознавания $P_{ПС}(1) = 5{,}1698 \cdot 10^{-25}$. Использование разработанного способствует повышению информационной скрытности НССС, обеспечив вероятность пропуска спутника-нарушителя для системы опознавания $P_{ПС}(2) = 4{,}136 \cdot 10^{-26}$. Полученные результаты свидетельствуют о том, что применение разработанного протокола позволяет повысить информационную скрытность НССС в 12,5 раза по сравнению протоколом аутентификации Фиата-Шамира/

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18 – 07 - 01020

Список используемой литературы

[1] Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.

[2] Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. - М.: Академия, 2009. - 272 с.

[3] Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2007. – 320 с.

[4] Зубов А.П., Алферов А.П., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.

[5] Калмыков И.А., Дагаева О.И. Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции// Известия ЮФУ. Технические науки, Таганрог: ТРТУ, 2012. №12, - С. 123-134

List of references

[1] Pashintsev, [1] Schneier B. Applied cryptography. Protocols, algorithms, source texts in C language. – M.: Publishing house TRIUMPH, 2003. - 816 p.

[2] Cheremushkin, A.V. Cryptographic protocols. The main characteristics and vulnerabilities. - Moscow: Academy, 2009. - 272 p.

[3] S. V. Tabachnikov Cryptographic protocols and their application in financial and commercial activity: textbook for universities. – M.: Hot line-Telecom, 2007. - 320 p.

[4] Zubov, Alferov, A. P., Kuzmin, A. S., Cheremushkin, A.V. fundamentals of cryptography. - Moscow: Helios ARV, 2002. - 480 p V. P., Kalmykov, M. I., Lyakhov A. V. Application of error-correcting authentication Protocol spacecraft for low-orbit satellite communication systems// information and communication technology. 2015. - № 2. − S. 183-190

[5] Kalmykov I. A. Dagaeva O. I. New data protection technology in e-Commerce systems based on the use of pseudo-random functions// Izvestiya yufu. Engineering Sciences, Taganrog: TSURE, 2012. No. 12, - P. 123-134

ФОРМИРОВАНИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ У УЧАЩИХСЯ

Наумова А.В.
Ставропольский государственный педагогический институт,

г. Ставрополь, 355000, Российская Федерация
nastya.naumova.1999@list.ru

Кузина Н.Н.
Ставропольский государственный педагогический институт,

г. Ставрополь, 355000, Российская Федерация,
Старший преподаватель кафедры математики и информатики
r.natasha2010@mail.ru

Аннотация

В данной статье говорится об актуальной на сегодняшний день проблеме систематизации условий формирования культуры информационной безопасности у учащихся. При этом доказывается актуальность формирования обозначенной культуры у отечественных педагогов, которая обусловлена современным информационным развитием человеческой цивилизации и общества. В статье рассматриваются сущностные, структурные и содержательные характеристики явления информационной безопасности личности учащихся, связанные с необходимостью введения общеобразовательными учреждениями в содержание общего среднего образования таких компонентов, которые непосредственно были бы связаны с формированием информационно личностной безопасности учащихся. Так как только образовательные учреждения в ряду других социальных институтов, в соответствии с существующим законодательством в образовательной сфере, способны оказывать ежедневное влияние на каждого учащегося, обеспечивая систематическую работу по его информационной подготовке.

Abstract

In this article it is spoken about the relevant for today problem of systematization of terms of forming of culture of information security among students. At the same time, the urgency of the formation of the designated culture among domestic teachers, which is due to the modern information development of human civilization and society, is proved. The article deals with the essential, structural and substantive characteristics of the phenomenon of information security of students ' personality, associated with the need to introduce educational institutions in the content of General secondary education such components that would be directly related to the formation of information personal security of students. Since only educational institutions in a number of other social institutions, in accordance with the existing legislation in the field of education, are able to have a daily impact on each student, ensuring systematic work on his information training.

Ключевые слова: информационная безопасность, формирование культуры, информационная культура, культура информационной безопасности, информационная безопасность учащихся, информационные ресурсы, защита информации, обеспечение технической защиты, учащиеся, образовательные учреждения.

Keywords: information security, culture formation, information culture, culture of information security, information security of students, information resources, information protection, technical protection, students, educational institutions.

В настоящее время человеческая цивилизация вступила в новую эпоху своего развития – эпоху информационного общества. За последние десятилетия информационное влияние на людей и их сознание значительно выросло. В связи с этим, о специфической информационной социализации современного подрастающего поколения можно говорить, как о свершившимся факте [1].

С огромной скоростью сегодня развиваются средства массовой информации и коммуникации. Эти интенсивно развивающиеся информационные системы, вне всякого сомнения, воздействуют на психическую сферу личности современных подростков, так как формирование интеллектуальных и морально-нравственных качеств у школьников на этапе взросления не является завершенными. В связи с переходом к информационному обществу и внедрением совершенно новых инновационных и коммуникационных технологий в образовательный процесс, направленный на развитие творческой и исследовательской деятельности учащихся, следует обратить особое внимание на культуру информационной безопасности, которая, в первую очередь, обеспечивает информационно-психологическую безопасность человека и определяет готовность к осуществлению деятельности по

обеспечению информационной безопасности своей личности и личности окружающих. Не следует забывать и то, что информационная культура, как продукт реализации творческого потенциала личности индивида выражается в применении компьютерных информационных технологий, составляющей которых являются многочисленные классы программных продуктов обеспечения, а также в умении извлекать информацию из различного рода источников и во владении основами аналитической переработки информации.

Обратимся теперь к самому понятию «информационная безопасность». Данный термин, впервые появился в нормативных правовых актах, научных и иных публикациях на рубеже 80-90-х годов XX века, когда было окончательно осознано реальное значение информации в жизни общества и человека. Первоначально понятие «информационная безопасность» трактовалось, как безопасность информации, состояние которой обеспечивается изначально самой защитой информационных данных от утраты, модификации, блокировки и копирования информационных потоков, а также от преднамеренных или случайных деструктивных воздействий внутреннего или внешнего свойства информационных ресурсов. Следует отметить то, что информационная безопасность имеет важную функцию защиты информации от всевозможных противоправных воздействий, носящих как случайные, так и специфические ошибки пользователей информационных систем.

В целом информационная безопасность в современном мире – безусловно важное условие обеспечения интересов гражданина и общества. В настоящее время информационная безопасность имеет важный аспект - разработку информационной защиты учащихся. Поставив в центр внимания учеников - наиболее незащищенных потребителей опасной информации, следует понимать, что информационная безопасность выступает в качестве защиты их личности от воздействия опасностей со стороны деструктивных информационных потоков. Важно иметь в виду, что негативная сторона доступности к глобальной информации, связана с существенным повышением деструктивности информационного воздействия на личность учащихся, у которых еще окончательно не сформированы целостное мировоззрение и устойчивые взгляды и убеждения [10]. .

Сегодня ставятся важнейшие задачи, обусловленные потребностями общества в формировании научных, методических и организационных механизмов, которые должны в режиме постоянного времени обеспечивать информационную безопасность учащихся. Главная задача заключается в том, что нужно, как можно лучше классифицировать теоретические основы в области безопасности подростков. В связи с этим, важно принимать во внимание необходимость формирования культуры информационной безопасности школьников в условиях общеобразовательных школ. В образовательных учреждениях следует организовать обучение безопасного использования информационных ресурсов. Ведь изначально школы созданы для того, чтобы научить учеников использовать информацию так, чтобы она открывала им мир. В зависимости от того, насколько важна получаемая школьниками информация, возникает огромное количество вопросов. И помочь найти ответы на эти вопросы, объяснить учащимся что-то непонятое и незнакомое в мире информации можно только в школах, несмотря на то, что сориентироваться в этом поистине колоссальном обрушивающемся потоке информации очень сложно, так как обработка информации занимает огромное количество времени, а сам поток поступающей информации постоянно возрастает.

Ученикам следует знать, что любая сфера деятельности связана с обменом информации, и она нуждается в безопасности. В настоящий момент отсутствует единая научная теория информационной безопасности, что в свою очередь обостряет проблему

воспитания учащихся, которые непрерывно используют ресурсы глобальной сети. Образовательные учреждения обязаны обучить незащищенных от получаемой в большом количестве информации учащихся рациональным приемам и способам работы с той информацией, которая скрывает в себе негативный и чрезмерно-агрессивный характер, влияющий на психические, социальные и нравственные качества подростков. Школам, первоначально, необходимо уберечь учеников от цензуры и пропаганды распространения насилия и жестокости со стороны СМИ (в первую очередь, со стороны сети Интернет), обостряющих проблему информационной безопасности учащихся [3].

Наиболее актуально сегодня формирование информационной культуры безопасности учащегося, перед которым открыты разнообразные перспективы более совершенного применения информационных ресурсов. Огромная проблема состоит в отсутствии единого процесса формирования информационной культуры подрастающего поколения, а также в подготовке учащихся к жизни в информационно-опасном обществе, которое имеет такие опасности, как:

1). Проблема отбора надёжной, качественной и достоверной информации в большом ее объёме;

2).Очевидная возможность разрушения современными информационными технологиями частной конфиденциальной жизни людей;

3).Сложность приспособления в большинстве случаев людей к среде информационного общества и др.

При решении данной проблемы особое место, безусловно, необходимо занять общеобразовательным учреждениям, но, в первую очередь, важнее педагогам этих учебных заведений проявить свою непоколебимость по отношению к учащимся. Следует проводить классные мероприятия по информационной безопасности, которые должны формироваться учителями, понимающими всю суть важности данной проблемы. Для этого нужно детально продумывать содержание занятий по информационной безопасности учеников, чтобы основательно донести до них всю значимость данных занятий. Перед педагогом стоит важная задача: необходимо поддержать ребёнка в его саморазвитии, принять его выбор и желание укрепить свою позицию в социуме, а также постараться открыть путь к социализации и адаптации, что является одним из главных условий успешного обучения информационной безопасности [5].

В большинстве случаев, принципиально-важное значение имеет само осознание педагогом теории информационной безопасности, так как, зачастую, учителя не всегда сами владеют той областью знаний, которые непосредственно связаны с формированием информационной культуры учащихся. В первую очередь, необходимо разработать комплексную программу, способствующую приучению учеников к культуре безопасного поведения в информационной среде. Данная программа поможет обучить детей правилам безопасного времяпровождения в нынешнем информационном обществе. Необходимо помнить, что обучение правильному безопасному поведению работы со средствами массовой информации будет эффективным при использовании технологий критического анализа информации. В ходе освоения данного материала, учащиеся должны идентифицировать негативное влияние нежелательной информации на их психику. Им необходимо узнать о способах и методах защиты, в первую очередь, от той информации, которая содействует разрушению их внутреннего мира. Углубляясь в изучение данного курса, расширяющего знания учащегося в плане обеспечения личной безопасности, подрастающему поколению следует научиться отбирать для себя ту информацию, которая поспособствует ускоренному

процессу формирования культуры безопасности в современном информационном пространстве.

Подводя итог, можно сказать, что информационная безопасность учащихся в общеобразовательном учебном заведении может быть достигнута при успешной реализации процесса, влияющего на развитие личности и представляющего собой совокупность внешних факторов, а также благодаря осуществлению воспитательной функции образования и практической направленности отбора содержания образовательных ресурсов, наряду с использованием технологий фильтрации поступающей информации. Исходя из вышесказанного, следует отметить, что педагогам необходимо уметь успешно использовать общую совокупность знаний, средств, методов и процедур для обеспечения технической защиты информации. Учителя должны эффективно защищать от негативных информационных воздействий со стороны деструктивной информационной среды общества психологическую безопасность личности своих воспитанников и обеспечивать информационно-психологическую безопасность их личности от негативных воздействий информационной среды общества.

Список используемой литературы

[1] Кузина Н.Н. Культура информационной безопасности личности педагога: структура, содержание основных компонентов и общее определение //Всероссийская научно-практическая конференция « Преемственность дошкольного и начального образования: проблемы и направления». - Киров: Изд-во МЦИТО, 2018. - https://mcito.ru/publishing/epub/collections (№36).

[2] Кузина Н.Н. Структура и содержание модели формирования культуры информационной безопасности личности у студентов педагогического вуза. Всероссийская научно-практическая конференция «Защита детства: проблемы, поиски, решения», Филиал СГПИ г.Железноводск, 2018.

[3] Кузина Н.Н. Культура информационной безопасности личности педагога: общая понятийная и структурная характеристика //Материалы XII Международной научно-практической конференции – Ставрополь: РИО ИДНК, 2017 – С. 690-694.

[4] Кузина Н.Н. Культурологический подход и его методологическое значение в формировании культуры информационной безопасности у студентов педагогического вуза //Педагогические науки. – Вып. 2 (23). – Ставрополь: Изд-во Ставролит, 2017. – С. 38-4.

[5] Кузина Н.Н. Методологические основы формирования культуры информационной безопасности у студентов педагогического вуз //Проблемы современного педагогического образования Педагогика и психология. – Вып. 53 (10). – Ялта: Изд-во РИО ГПА, 2016. – С. 80-8.

[6] Коробкина А.А. Информационная безопасность и информационная культура школьников в интернет – пространстве http://human.snauka.ru/2017/04/23366.
[7] Серебряник Е.Э. Формирование информационно-личностной безопасности учащихся основной школы http://www.dissercat.com/content/formirovanie-informatsionno-lichnostnoi-bezopasnosti-uchashchikhsya-osnovnoi-shkoly.
[8] Осипова Е.А. Формирование информационной культуры у учащихся https://nsportal.ru/nachalnaya-shkola/materialy-dlya-roditelei/2017/12/26/formirovanie-informatsionnoy-kultury-u.
[9] Бочаров С.Н. Формирование у учащихся культуры безопасного поведения в современном информационном пространстве https://scienceforum.ru/2015/article/2015017194.
[10] Белякова Е.Г., Березенцева А.И., Загвязинская Э.В. Информационная культура и информационная безопасность школьников https://cyberleninka.ru/article/n/informatsionnaya-kultura-i-informatsionnaya-bezopasnost-shkolnikov.

List of references

[1] Cousina N. N. Culture of information security of the teacher's personality: structure, content of the main components and General definition //all-Russian scientific and practical conference "Continuity of preschool and primary education: problems and directions". - Kirov: ICITO Publishing house, 2018. - https://mcito.ru/publishing/epub/collections (No. 36).
[2] Cousina N. N. The structure and content of the model of formation of culture of information security of the individual students of pedagogical University. All-Russian scientific-practical conference "Protection of childhood: problems, searches, solutions", Branch of Saratov state pedagogical University Zheleznovodsk, 2018.
[3] Cousina N. N. Culture of information security of the teacher's personality: General conceptual and structural characteristics / / Proceedings of the XII International scientific and practical conference-Stavropol: RIO IDNK, 2017-P. 690-694.
[4] Cousina N. N. Culturological approach and its methodological importance in the formation of information security culture among students of pedagogical high school //Pedagogical Sciences. – Vol. 2 (23). – Stavropol: publishing house of Stavrolit, 2017. - P. 38-4.
[5] Cousina N. N. Methodological bases of formation of culture of information security in students of pedagogical high school / / Problems of modern pedagogical education Pedagogy and psychology. – Vol. 53 (10). – Yalta: Izd-vo RIO HPA, 2016. – S. 80-8

[6] Information security and information culture of schoolchildren in the Internet space http://human.snauka.ru/2017/04/23366.
[7] The silversmith E. E. Formation of information and personal security courses. http://www.dissercat.com/content/formirovanie-informatsionno-lichnostnoi-bezopasnosti-uchashchikhsya-osnovnoi-shkoly.
[8] Osipova E. A. Formation of information culture of students https://nsportal.ru/nachalnaya-shkola/materialy-dlya-roditelei/2017/12/26/formirovanie-informatsionnoy-kultury-u;
[9] Bocharov S. N. Formation of students ' culture of safe behavior in the modern information space https://scienceforum.ru/2015/article/2015017194.
[10] Belyakova E. G., Berezantseva A. I. Zagvyazinsky E. V. Informational culture and informational security of the students https://cyberleninka.ru/article/n/informatsionnaya-kultura-i-informatsionnaya-bezopasnost-shkolnikov.

THE PROCESS MODEL REQUIREMENTS FOR THE "SMART CITY" SYSTEM USING THE BLOCKCHAIN DISTRIBUTED TRANSACTION NETWORK

Затолокин М.Ю.
ferrasil@yandex.ru

Курчеева Г.И
к.э.н, доцент
kurcheeva@yandex.ru

Новосибирский Государственный Технический Университет,
630073, г. Новосибирск, Россия

Аннотация

В период активного развития цифровых технологий и также перехода нашей экономики к статусу "цифровой", активно по всему миру интегрируются различные компоненты систем умного города, позволяя улучшать жизнь граждан и упрощать их способ взаимодействия с обширной инфраструктурой города, начиная от умных датчиков, считывающих показатели света и воды до организации интерактивных общественных зон, наделенных большим спектром сенсоров для контроля состояния городских объектов, слежения за порядком и предотвращения инцидентов. Для организации взаимодействия всего этого широкого спектра устройств необходима устойчивая, прозрачная и оперативная модель обработки данных для получения должного, близкого к эталонному результата внедрения этих самых технологий. В данной статье предложено рассмотреть процессных подход внедрения технологии блокчейн применимо к разным компонентам систем умного города, учитывая особенности каждого из них, а также в последствии соотнести определенные варианты с некоторыми выделенными показателями уровня жизни населения, позволяя оценить качество и

оправданность внедрения этих нововведений. Производится обоснование актуальности использования технологии блокчейн в системах умного города, базируясь на основных принципах функционирования децентрализованных сетей. По итогу рассмотрения ряда базовых принципов технологии блокчейн, поставлен план на апробацию этих принципов конкретно на одной из сфер умного города.

Abstract

During the period of active development of digital technologies and also the transition of our economy to the status of "digital", various components of smart city systems are being actively integrated around the world, allowing us to improve the lives of citizens and simplify their way of interacting with the city's extensive infrastructure, ranging from smart sensors that read light indicators and water until the organization of interactive public areas, endowed with a large range of sensors to monitor the state of urban objects, monitor order and prevent incidents. To organize the interaction of all this wide range of devices, a stable, transparent and operational data processing model is necessary to obtain a proper, close to the reference result of the implementation of these technologies. This article proposes to consider the process approach of implementing the blockchain technology applicable to different components of the smart city systems, taking into account the characteristics of each of them, as well as subsequently correlating certain options with some selected indicators of the standard of living of the population, making it possible to assess the quality and justification of these innovations. A justification is made of the relevance of the use of blockchain technology in smart city systems, based on the basic principles of functioning decentralized networks. Following the review of a number of basic principles of the blockchain technology, a plan was put to test these principles specifically in one of the areas of the smart city.

Ключевые слова: Блокчейн, децентрализованная сеть, умный город, устранение посредников, интернет вещей, транзакции.

Keywords: Blockchain, decentralized network, smart city, intermediary's elimination, internet of things, transactions.

Introduction

Currently, cities face difficult challenges to improve the quality of citizens life. According to the report “Prospects for World Urbanization in 2014” (United Nations , 2014), more than half of the world’s population currently lives in urban areas, and another 2.5 billion people are expected to move to cities by 2050. Due to the high population density of residents in large cities of the world, some urban phenomena affect the conditions and quality of people’s life: an increase in traffic jams, carbon dioxide, greenhouse gas emissions and waste [1].

The concept of "smart city" is the answer to these problems. This concept has gained popularity over the past few years. Many cities define themselves as “smart”, based on a number of characteristics and components inherent in these cities (such as high-speed network, the society informatization, the superiority of intellectual work, and so on). A common underlying fact is that these smart cities benefit from the use of innovative types of information and communication technologies (ICT) to support the joint and interoperable infrastructure use[2].

For the city development, more and more new ideas and models are needed, which in turn require conditions for the creation and implementation of the urban environment and which directly or indirectly affect the quality of citizens life.

It is necessary to state that the individual technologies of the smart city, which increase the quality of life, are implemented in most large Russian cities. These include smart lighting, smart road traffic, systems for monitoring criminal situations in inaccessible areas of the city through surveillance cameras with various improvements and others.

Method development

Preparations for the development of a comprehensive project that combines all areas of “smart city” development include also an information model “smart city” development, which Novosibirsk seeks based on a process approach, according to the authors, allows to highlight the most significant components and relate them to indicators quality of population life. Thus, it is possible to assess the uniformity in the development of technologies of the “smart city”, to identify problems in providing citizens with a quality urban environment.

To solve this task, an attempt has been made to systematize approaches to identifying the significant components of a “smart city” and to correlate them with indicators of the quality of urban life[3].

Currently, a large number of “smart city” technologies have been implemented. A smart city can be defined as the “City of Knowledge”, “Digital City”, “Cybercity ” or “ Eco City ” - depending on the goals of urban planning. Smart cities in economic and social aspects are directed to the future. They conduct ongoing critical infrastructure monitoring— roads, bridges, tunnels, railroads, subways, airports, seaports, communication systems, water, energy, and even the most important buildings — in order to optimally allocate resources and ensure security. They constantly increase the number of services provided to the population, providing a sustainable environment that contributes to the well-being and preservation of the health of citizens. The basis of these services is ICT infrastructure [4].

In order to ensure the exchange of information within this sharing structure, an appropriate hardware base is necessary to collect information from all possible components of the city. In the prevailing number of cases, this hardware base refers to the Internet of Things (IoT) — that is

“Things” (or IoT devices) that have remote reading and interaction capabilities and can communicate with other connected devices and applications (directly or indirectly).

IoT devices can collect data and process it locally or send it to centralized servers or cloud applications for further processing. Speaking about the processing of data collected from various sensors and sensors of the "smart city" together, it is impossible not to mention the issue of working with big data, since the increase in the volume of processed big data and the Internet of Things (IoT) development played an important role in the intelligent urban initiative’s feasibility.

Useful properties of the blockchain technology for smart city systems Technology

Blockchain is known as the base of Bitcoin. In addition to using the Bitcoin network, many researchers and practitioners expect that they tend to revolutionize the way we interact and transact over the Internet, resulting in a new economy. There is a huge potential for its application, for example, the impact on the work of the government, public notarial services or contracts in the online environment.

Despite the fact that there are several startups that already offer blockchain solutions for their clients, not a single application has yet reached widespread recognition, since they are faced with the competition of existing and well-proven systems. Therefore, additional and ubiquitous options for its use are needed to facilitate the introduction of the blockchain technology and to be able to reveal the real advantages for its users.

Although the blockchain technology can be considered as a new technology, and therefore it still has room for improvement in terms of efficiency and technical aspects, basic characteristics can already be identified in scientific papers.

The research of the subject shows that the blockchain technology has various characteristics, which are further analyzed in relation to the application tasks of its implementation, obtaining a set of key characteristics. For example, it is assumed that the characteristics “general and public” as well as “low mediation” lead to an increase in transparency in the system, since information becomes publicly available between participants without the influence of a third party. A brief overview of the resulting key characteristics and their basic elements is presented in Figure 1 and further clarified below.

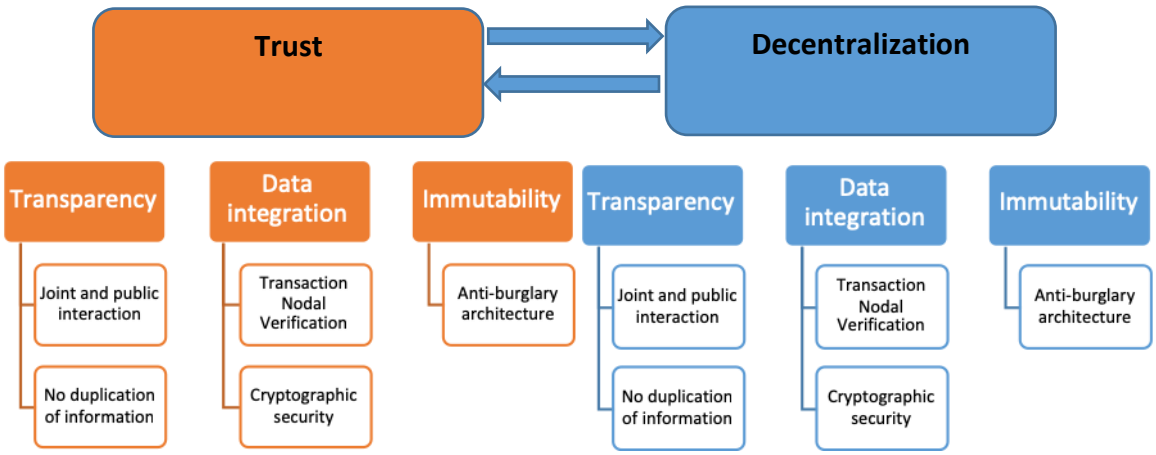

Figure 1. Basic blockchain compontents

Trust and decentralization are the two main characteristics that are basically the definition of blockchain technology. Its decentralization facilitates the creation of a private, reliable and universal environment, which is further described below.

Since the blockchain technology is based on a peer-to-peer network, which in combination with technology, is able to provide interaction between two people using public key cryptography and the fact that identifiers are covered with pseudonyms, a high degree of confidentiality for its participants is included.

Reliability in the system is established using two factors. On the one hand, transaction information is divided and stored across the entire network and therefore processed in a redundant way, and on the other hand, since the technology is based on data and codes, automated measures are facilitated, which, in turn, can reduce individual errors, since few required for manual intervention.

By providing its members with the opportunity to integrate their own programs, develop and distribute their own code, thereby forming their own environment, the blockchain technology facilitates the creation of an open and universal system. A popular example for this feature is the so-called "smart" contract, which is part of the code that serves as programmed contractual agreement between the two parties.

The use of blockchain technology allows its members to establish common and publicly developed relationships. Since there is a common look at all past and current transactions, participants have full disclosure of information about the activities of the system. New transactions are broadcast across the entire network, and since there is no single intermediary who controls the system, users can interact directly, which will reduce the mediation.

Trust can also be facilitated by the inherent technology to ensure data integrity, which is stored in the database itself, since direct interaction is provided through public-key cryptography and the fact that due to its transparency, each user can verify the broadcast transactions based on predefined rules.

Another factor that contributes to the establishment of trust is the constant design of the database, which means that after a transaction is added to a block, which, in turn, is added to a block chain, this transaction cannot be changed. This process is facilitated by the application of the so-called consensus mechanism, which, for example, requires the calculation of evidence of work. The proof of the work can be considered as a computational puzzle, which requires great effort to solve, but the solution of which is easily verifiable by others. In case the user finds a solution, he shares with the rest of the network, who, in turn, can verify its correctness, thereby reaching a consensus on the decision. One of the important aspects of the proof of work is that the puzzle that the user solves depends on the previously accepted and agreed blocks of the block chain. As various participants try to form and add new blocks to the blockchain, changes in the blockchain will lead to different decisions, identifying misuse or manipulation. [5]

Results

Both trust and decentralization are closely related and interrelated in the case of blockchain technology. On the one hand, trust building mechanisms, such as transparency, integrity and immutability of data, are necessary to create a decentralized network in which reliable and reliable transactions can take place without a trusted third party. On the other hand, decentralization allows users to participate in the network, creating the basis for a consensus mechanism, thereby making it unnecessary to use a trusted third party.

Table 2. Provision of blockchain control

Initiatives and services	Ecosystem development	Politics
Explain the principle of operation of the blockchain and find out from enterprises what problems can be solved with the help of technology.	Hold educational seminars and conferences inviting experts and experienced practitioners	Establish working groups to develop and maintain an enabling legal environment.
Start with projects with proof of concept (proof of concept) that demonstrate the merging capabilities and help interested parties understand the benefits of technology.	Developing grassroots innovations through hackathons, national competitions, bootcamps and accelerators	Promote standards and interoperability for the use of network protocols, and minimize duplication
Build smaller functional components with testing and integration steps, following a longer-term roadmap for integrating existing services.	Build relationships with IT leaders, create a favorable environment for start-ups and investments, and increase regional technical knowledge	Creating workflows for using blockchain-protected technology from unauthorized access to improve compliance and regulation

Discussion

Many modern articles on this subject undoubtedly confirm the need to introduce blockchain technology into the elements of a smart city due to the mandatory provision of transparency, immutability and possible anonymity of transaction data in the smart device data exchange network. Supporters of these statements can be traced in the works of next researchers: Lingjun Fan and G. Brian Burke described the prototype, that provides a private Blockchain infrastructure of distributed IoT devices, which basically can replicate the device data and also validate the transactions among devices through smart contracts [6].

Saber Talari and Miadreza Shafie-khah reviewed also that some of the developments in the actual implementation of smart cities with the blockchain across the world were presented already, which can be considered as samples or pilot projects for future comprehensive smart cities. [7]

Conclusion

Further research is aimed at the process models development of the communication system and the smart city parts by the exchange economy perspective and the structural features of the blockchain technology.

The economic system based on the blockchain technology works without people, which makes the transaction free in principle from such a thing as “trust”. Historically, trust has been based on business, often involving a reliable third party, which is a huge amount of capital in the realities of the present world. Blockchain technology provides a viable alternative to eliminate intermediaries, thereby reducing operating costs and increasing the efficiency of the shared access service. With this technology, you can rethink the most fundamental commercial interactions in the world; the door is open for creating new styles of digital interactions in free traffic exchange services.

Список используемой литературы

[1] Agyeman J, McLaren D (2014) ‘Smart Cities’ Should Mean ‘Sharing Cities’. In: Times

[2] Умный город: Эффективное управление развитием [электр. ресурс] URL: https://geektimes.ru/company/gsgroup/blog/265366/ ISO 37120:2014 Sustainable development of communities -- Indicators for city services and quality of life [электр. ресурс] URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=62436

[3] Курчеева Г.И. Процессный подход к оценке уровня технологического уклада) / Теория устойчивого развития экономики и промышленности: коллективная монография // Под ред. проф. А.В. Бабкина. – Санкт-Петербург, 2016. – 439 с.

[4] Курчеева Г.И., Алетдинова А.А. К разработке методики оценки возможности перехода к шестому и седьмому технологическим укладам / А. А. Алетдинова, Г. И. Курчеева // В книге: Новая экономическая реальность, кластерные инициативы и развитие промышленности (INПРОМ-2016) Труды научно-практической конференции с зарубежным участием под ред. А. В. Бабкина, 2016. – С. 63-67.

[5] Garman, C., Green, M., Miers, I.: Decentralized anonymous credentials. In: Network and Distributed System Security (NDSS) Symposium 2014, страницы. 23–26 (2014)

[6] Fan, Lingjun & Gil-Garcia, J. Ramon & Werthmuller, Derek & Burke, G & Hong, Xuehai. (2018). Investigating blockchain as a data management tool for IoT devices in smart city initiatives. 1-2. 10.1145/3209281.3209391.

[7] Saber Talari, Miadreza Shafie-khah, Pierluigi Siano, Vincenzo Loia, Aurelio Tommasetti and João P. S. Catalão (2017). A Review of Smart Cities Based on the Internet of Things Concept

List of references

[1] Agyeman J, McLaren D (2014) ‘Smart Cities’ Should Mean ‘Sharing Cities’. In: Times

[2] Smart city : effective development management URL: https://geektimes.ru/company/gsgroup/blog/265366/ ISO 37120:2014 Sustainable development of communities -- Indicators for city services and quality of life [электр. ресурс] URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=62436

[3] Kurcheeva G.I. Process approach to assessing the level of technological structure) / Theory of sustainable development of the economy and industry: a collective monograph // Under edit A.B. Babkin. – Saint-Petersburg, 2016. – 439 p.
[4] Kurcheeva G.I Aletdinova A.A. On the development of methods for assessing the possibility of transition to the sixth and seventh technological structures / A. A. Aletdinova, G. I. Kurcheeva // In the book: New Economic Reality, Cluster Initiatives and Industrial Development (INPROM-2016) Proceedings of a Scientific and Practical Conference with Foreign participation under the editorship of A. V. Babkina, 2016. – P. 63-67.
[5] Garman, C., Green, M., Miers, I. (2014): Decentralized anonymous credentials. In: Network and Distributed System Security (NDSS) Symposium 2014, pp. 23–26
[6] Fan, Lingjun & Gil-Garcia, J. Ramon & Werthmuller, Derek & Burke, G & Hong, Xuehai. (2018). Investigating blockchain as a data management tool for IoT devices in smart city initiatives. Pp. 10-12. 10.1145/3209281.3209391.
[7] Saber Talari, Miadreza Shafie-khah, Pierluigi Siano, Vincenzo Loia, Aurelio Tommasetti and João P. S. Catalão (2017). A Review of Smart Cities Based on the Internet of Things Concept , pp. 20-21.

ИССЛЕДОВАНИЕ АУТЕНТИФИКАЦИИ В ПРОТОКОЛЕ SSH

Анзина Антонина Викторовна[1]
tosz@bk.ru

Медведева Анастасия Дмитриевна[1]
medvedeva.nastya26@mail.ru

Лапина Мария Анатольевна[1]
Кандидат физико-математических наук, доцент
norra7@yandex.ru

[1] Северо-Кавказский Федеральный университет, город Ставрополь, 355000, Россия

Аннотация

Удаленный доступ представляет возможность подключения к компьютеру на любом расстоянии, его можно обеспечить при помощи протокола SSH. В настоящее время данный протокол является одним из наиболее безопасных протоколов, однако злоумышленники находят некоторые уязвимости, при помощи которых получают доступ к информации, находящейся на компьютере, именно из-за этого проблема выявления угроз безопасности протокола и их решение является актуальной. Таким образом, целью исследования является выявление уязвимостей аутентификации протокола SSH и составление рекомендаций, соблюдение которых позволит минимизировать угрозы безопасности. Исследуются три типа аутентификации: аутентификация по ip-адресу клиента, аутентификация по паролю и аутентификация по ключам RSA. При этом составляются схемы, показывающие процесс аутентификации, изучение которых помогает выявить уязвимости аутентификации. В результате рассмотрения трех типов аутентификации, аутентификация по ключам является наиболее безопасной, однако имеет некоторые уязвимости, такие как дублирование ключей, их редкое изменение и хранение большого количества ключей в неупорядоченном виде. Соблюдение рекомендаций, которые

были составлены после изучение трех типов аутентификации позволяют снизить риски возможного возникновения несанкционированного доступа к компьютеру.

Abstract

Remote access represents the ability to connect to a computer at any distance, it can be provided using the SSH protocol. Currently, this protocol is one of the most secure protocols, but attackers find some vulnerabilities with which they can gain access to information stored on a computer, precisely because of this, the problem of detecting protocol security threats and their solution is relevant. Thus, the purpose of the study is to identify security vulnerabilities in the SSH protocol and make recommendations that, if followed, will minimize security threats. Three types of authentication are investigated: authentication by the client's ip-address, password authentication and RSA key authentication. At the same time, diagrams are made showing the authentication process, the study of which helps to identify authentication vulnerabilities. As a result of examining three types of authentication, key authentication is the most secure, but it has some vulnerabilities, such as duplicate keys, their rare modification and storing many keys in an unordered manner. Compliance with the recommendations that were made after studying the three types of authentication can reduce the risks of possible unauthorized access to a computer.

Ключевые слова: удаленный доступ, протокол SSH, аутентификация по ip-адресу, аутентификация по паролю, аутентификация по ключам RSA, создание ключей RSA, угроза безопасности, уязвимость.

Keywords: remote access, SSH protocol, ip address authentication, password authentication, RSA key authentication, RSA key creation, security risk, vulnerability.

1 Введение

Основной задачей при администрировании сети является удаленный доступ, который позволяет подключаться к компьютерам на любом расстоянии, если это необходимо [1]. Для осуществления удаленного доступа существует множество бесплатных и платных платформ.

При проведении исследования рассматривается пример удаленного доступа при помощи протокола прикладного уровня SSH в операционной системе семейства Linux [2,3].

Протокол SSH расшифровывается как Secure Shell, что означает «безопасная оболочка». В работе протокола SSH участвуют две стороны: клиент (ssh) и сервер (sshd). При установлении защищенного соединения клиент проходит аутентификацию у сервера, который предоставляет командную оболочку для работы с удаленной системой. Протокол занимается шифрованием трафика, это позволяет организовать защищенное соединение между хостами сети. Существует две версии этого протокола, однако в настоящее время используется только вторая версия, она реализует более мощные алгоритмы шифрования и поддерживает возможность обнаружения умышленного искажения данных.

При неправильном использовании протокола SSH, у злоумышленника появляется возможность воспользоваться уязвимостями протокола, в результате чего все данные, находящиеся на компьютере, могут оказаться в распоряжении правонарушителя. Именно поэтому проблема выявления нарушений безопасности является актуальной [4].

2 Постановка задачи

Главной целью исследования является выявление уязвимостей аутентификации и составление рекомендаций, соблюдение которых поможет свести к минимуму существующие угрозы безопасности.

Исследуются три способа аутентификации и выявляются возможные угрозы безопасности при использовании каждого из них.

3 Разработка методик

Удаленный сеанс работы начинается после прохождения процедуры аутентификации. Утилита sshd поддерживает различные способы аутентификации: аутентификация по ip-адресу, аутентификация по паролю и аутентификация по ключу [5]. Для аутентификации клиент отправляет запрос на сервер, чтобы узнать какие способы аутентификации сервер поддерживает, если опции аутентификации (PreferredAuthentications в sshd.conf) не были изменены, то клиент пытается аутентифицироваться сначала с помощью адреса, затем при помощи публичного ключа, и в случае, если данные методы не позволили аутентифицироваться, то сервер передает зашифрованный пароль. После успешного прохождения аутентификации создается ключ симметричного шифрования из пар ключей, находящихся у клиента и сервера, с помощью которого шифруется весь последующий передаваемый через ssh трафик.

Аутентификация по ip-адресу клиента, заключается в том, что у клиента и сервера находятся ключи хоста, где секретные ключи - Ck и Cc, публичные - Pk и Pc соответственно. Важным условием при аутентификации по ip-адресу является правильный адрес клиента, которому соответствует публичный ключ на сервере. Клиент и сервер используют ключи с временной диаграммой, изображенной на рисунке 1.

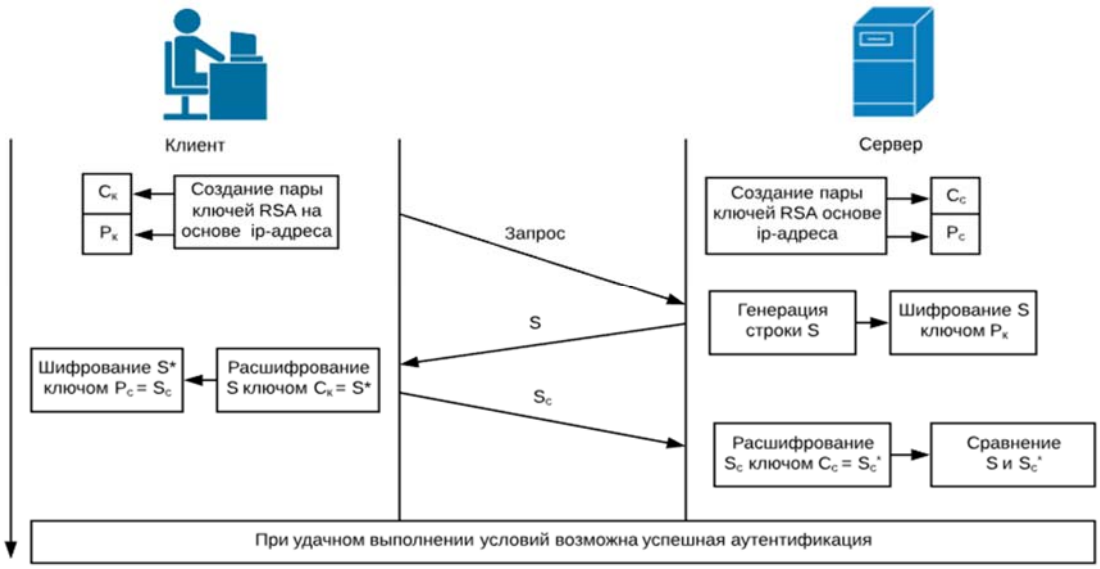

Рисунок 1. Временная диаграмма алгоритма аутентификации по ip-адресу.

В данном случае необходимо убедиться, что именно доверенный источник предоставил публичные ключи, иначе возможна подмена адреса. Таким образом, аутентификация по ip-адресу клиента является небезопасной, поэтому следует использовать другие способы аутентификации.

Следующий способ - аутентификация по паролю. Данный метод аутентификации простой. Пользователю необходимо знать логин и пароль. Аутентификация по паролю упрощает конфигурацию и подключение новых пользователей. В этом случае перед началом передачи хешированного пароля, происходит обмен асимметричными ключами между клиентом и сервером. Несмотря на то, что пароль передается по сети в зашифрованном виде, существует вероятность подбора пароля. Данный способ аутентификации является небезопасным и его не рекомендуется использовать, так как пользователи часто создают простые и короткие пароли. Аутентификация по паролю приведена на рисунке 2.

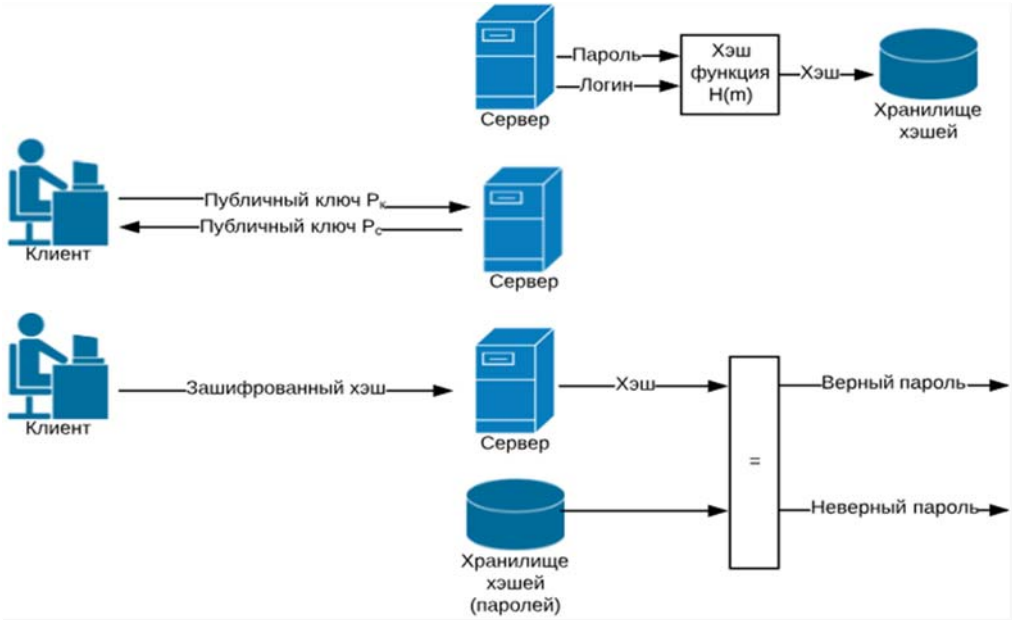

Рисунок 2. Схема аутентификации по паролю.

Аутентификация по ключам является наиболее защищенным способом авторизации. При использовании этого метода пользователь генерирует пару ключей: публичный ключ и секретный. Публичный служит для проверки идентичности пользователя. С помощью него можно зашифровывать сообщения, которые расшифровываются только соответствующим секретным ключом. В свою очередь секретные ключи хранятся в зашифрованном виде, так как являются конфиденциальной информацией. В результате запроса закрытого ключа, необходимо ввести пароль для расшифровки этого ключа. Если вдруг злоумышленник получит секретный ключ, он сможет войти в систему без дополнительной аутентификации.

Процесс настройки ключей SSH состоит из трех шагов: создание пары ключей RSA, копирование публичного ключа на сервер, аутентификация на сервере. Рассмотрим каждый шаг более подробно. Создание пары ключей происходит на устройстве клиента SSH, по умолчанию создается 2048-битная пара ключей RSA, она является достаточно безопасной, однако в случае необходимости возможно получить 4096-битный ключ. После генерации секретного и публичного ключа их можно сохранить в необходимую директорию.

Существует возможность задания ключевой фразы, она добавляет дополнительный уровень безопасности для предотвращения входа на сервер неавторизованных пользователей. В случае указания кодовой фразы, необходимо предоставлять ее каждый раз при использовании ключей или использовать программу ssh-agent.

Более подробно процесс создания пары ключей RSA представлен на блок-схеме, изображенной на рисунке 3.

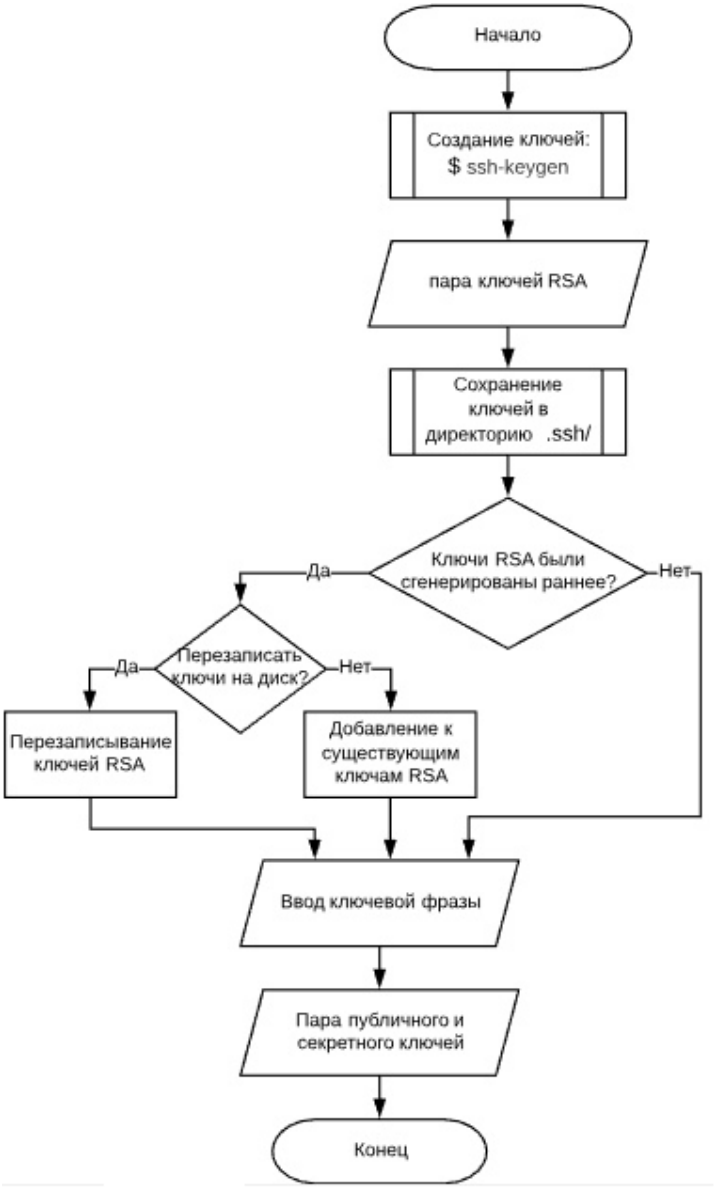

Рисунок 3. Блок-схема процесса создания пары ключей RSA.

После успешного получения публичного и секретного ключей, использующихся для аутентификации, необходимо поместить публичный ключ на сервер.

Копирование публичного ключа можно произвести несколькими способами, самый простой из них использование утилиты ssh-copy-id, если данный метод оказался недоступным по какой-либо причине, то возможно использование других альтернативных методов: копирование вручную с использованием пароля и без пароля [6,7].

Для осуществления первого метода копирования ключа необходимо иметь доступ к серверу по SSH с использованием пароля. При использовании утилиты указывается адрес удалённого хоста, а также имя пользователя, имеющего доступ к хосту по SSH. Именно для аккаунта этого пользователя будет скопирован публичный ключ SSH.

Если данная утилита не может использоваться, однако есть пароль для входа по SSH, то можно загрузить ключ вручную. Для этого необходимо использовать команду, которая получит доступ к содержимому файла с публичным ключом на локальной машине, а затем отправит его по SSH на удаленный сервер. В случае, когда нет доступа к удаленной машине по SSH с использованием пароля возможно скопировать публичный ключ на локальной машине и добавить его в конец файла на удаленном сервере. При успешном копировании публичного ключа на сервер возможен вход на удаленный хост без использования пароля. В случае, если при этом можно зайти на сервер при помощи пароля необходимо отключить эту возможность, устранив при этом возможные атаки с перебором пароля.

Алгоритм аутентификации по ключам в целом идентичен алгоритму аутентификации по ip-адресу, отличие состоит в том, что осуществляется проверка не адреса клиента, а ключ клиента и имя пользователя. Алгоритм аутентификации по ключам представлен на рисунке 4.

Рисунок 4. Функциональная диаграмма аутентификации по ключам.

Таким образом, при подключении к серверу SSH аутентификация на основе RSA-ключей использует криптосистему с открытым ключом. Одной из важных особенностей применения данного способа аутентификации является то, что пользователь может быть авторизован на сервере без регулярной необходимости отправлять пароль через сеть. Так как пароль фактически не передается, у злоумышленника нет возможности взломать его.

Аутентификация с помощью ключей обеспечивает дополнительную безопасность. Однако, правонарушителям удается выявить некоторые уязвимости, приведенные ниже [8].

В крупных предприятиях накапливается большое количество ключей SSH, в результате чего значительно усложняется поиск и управление каждым ключом. Если вдруг серверы будут перенесены в производственные среды, причем учетные данные не будут стерты, становится легко их потерять. Такой случай может предоставить злоумышленникам долгосрочный доступ к необходимым ресурсам. Для того чтобы сократить риск возникновения данной угрозы безопасности необходимо следить за количеством ключей и их упорядоченным хранением. И в процессе перенесения серверов в производственные среды, в целях безопасности необходимо удалять учетные данные.

Следующая уязвимость заключается в дублировании SSH-ключей, которая возникает при их совместном использовании общей группой сотрудников. Это снижает уровень

безопасности, поскольку сложно отменить один ключ, не нарушая связанность других ключей SSH. Избежать повторения ключей можно путем создания уникального ключа каждому сотруднику. Несмотря на временные затраты, это позволит повысить уровень безопасности.

Злоумышленники могут получить доступ к ресурсам путем использования статических ключей. Такие ключи появляются из-за редкого изменения и перераспределения. Чтобы минимизировать риск угрозы безопасности необходимо регулярно изменять ключи аутентификации.

Таким образом, SSH-ключи могут предоставить огромную возможность для злоумышленников в получении доступа к необходимым ресурсам и выполнении любой деятельности по отношению к организации, а также они могут выдавать себя за обычных пользователей.

4 Результаты и заключение

В результате были исследованы три способа аутентификации, при этом обнаружены угрозы безопасности, возникающие при аутентификации, а также даны некоторые рекомендации, позволяющие минимизировать данные угрозы.

Аутентификация по ip-адресу считается менее безопасной, так как ip-адрес можно подменить, поэтому по возможности следует использовать другие способы аутентификации. Если использовать аутентификацию по паролю, то следует тщательно выбирать его, так как злоумышленник может подобрать пароль. Наиболее безопасным методом является аутентификация по ключам. Несмотря на то, что данный способ аутентификации является самым защищенным из вышеперечисленных, существуют некоторые уязвимости, снижающие уровень безопасности, такие как дублирование ключей, их редкое изменение и большое количество, приводящее к сложному управлению ключами. Их регулярное изменение и упорядоченное хранение позволяет сократить данные уязвимости. Соблюдая рекомендации можно повысить уровень безопасности удаленного доступа при использовании протокола SSH.

5 Список используемой литературы

[1] Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.

[2] Таненбаум Э., Босх Х. Современные операционные системы // 4-е изд. – СПб.: Питер, 2015. – 1120 с.

[3] Буренин П. В., Девянин П. Н., Лебеденко Е. В., Проскурин В. Г., Цибуля А. Н. Безопасность операционной системы специального назначения AstraLinuxSpecialEdition // Учебное пособие для вузов – 2-е издание, стереотипное. – М.: Горячая линия – Телеком, 2017. – 312 с.

[4] Плут А.А., Лапина М.А. Модель анализа угроз и уязвимостей информационных систем // Студенческая наука для развития информационного общества: сборник материалов I всероссийской научно-технической конференции, 2015. – 212-214 с.

[5] Даценко А.Ю., Анзин И.В. Идентификация в информационных системах // сборник материалов V Всероссийской научно-технической конференции: в 2 частях, 2016 – 405-408.

[6] Калашникова В.А., Львова А.П., Анзин И.В. Обеспечение безопасности пользователеиос Ubuntu // Студенческая наука для развития информационного общества: Сборник материалов V Всероссийской научно-технической конференции: в 2 частях, 2016. – 233-235.

[7] Львова А.П., Калашникова В.А., Анзин И.В. Исследование эффективности стандартных механизмов безопасности операционной системы Ubuntu // Студенческая наука для развития информационного общества: сборник материалов V Всероссийской научно-технической конференции: в 2 частях, 2016. – 288-291.

[8] Ивакина Д.А. Анализ уязвимостей протокола SSH // Материалы II Всероссийской научно-технической конференции. 2015. – 109-111.

ИССЛЕДОВАНИЕ ПРИНЦИПОВ РАБОТЫ, ТЕХНИЧЕСКИХ И ЭКСПЛУАТАЦИОННЫХ АСПЕКТОВ СРЕДСТВ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Маршанский Н.А. [1]
mansdata@mail.ru

Ходакова В.А. [1]
khodakova.v@mail.ru

Лапина М.А[1].
Кандидат физико-математических наук, доцент
norra7@yandex.ru

[1] Северо-Кавказский федеральный университет
Ставрополь, 355009
Российская Федерация

Аннотация

Жизнь в современном мире как одного человека по отдельности, так и крупнейших организаций, неразрывно связана с информационными системами. С помощью компьютеров производится обмен огромного количества информации каждую секунду, и зачастую такие данные являются конфиденциальными или не предназначенные для сторонних лиц. Несмотря на стремительный рост производительности, удобства и функциональных возможностей информационных технологий, новости об утечках персональных данных даже в крупных компаниях не перестают появляться. Такое явление связано с несанкционированным доступом сторонних лиц к защищаемой информации, вызванное, в частности, неправильной настройкой систем доступа. Зачастую механизмы аутентификации замедляют работу сотрудников при входе в систему, что вызывает неосознанное сопротивление большинства обычных пользователей. В результате, если аутентификация будет чрезвычайно сложная и безопасная, сотрудники будут пытаться облегчить

процесс входа в систему, тем самым нивелируя уровень защиты. В данной статье будут рассмотрены основные системы и методы идентификации и аутентификации. Анализ технологий будет проведен с технической и пользовательской сторон, также будут рассмотрены технические трудности, возникающие при внедрении и дальнейшем использовании технологий.

Abstract

Life in the modern world, both as a single person and as a major organization, is linked with information systems. A huge amount of information is exchanged every second, and often the data is confidential or not intended for third parties. Despite the rapid growth of capacity, convenience and functionality of information technologies, news about leaks of personal data even in large companies do not cease to appear. Such a phenomenon is connected with the unauthorized access of third parties to the protected information, caused, in particular, by improper configuration of access systems. Often, authentication mechanisms slow down the work of employees when they log on to the system, which causes unconscious resistance of most ordinary users. As a result, if the authentication is extremely complex and secure, employees will try to facilitate the login process, thereby leveling the level of protection. This article will discuss the basic systems and methods of identification and authentication. Technology analysis will be carried out from the technical and user side, technical difficulties arising from the introduction and further use of technology will also be considered.

Ключевые слова: идентификация, аутентификация, безопасность, биометрические системы, парольная защита, смарт-карты, конфиденциальная информация, несанкционированный доступ.

Keywords: identification, authentication, security, biometric systems, password protection, smart cards, confidential information, unauthorized access.

1 Представления об идентификации и аутентификации

Для предоставления доступа к конфиденциальной информации строго ограниченному кругу лиц применяются системы идентификации и аутентификации, необходимые для работы с

субъектами автоматизированных систем, в роли которых могут выступать как пользователи, так и процессы.

1.1 Идентификация

Идентификация – процедура одноразовой регистрации в системе субъекта с уникальными и присущими только для него параметрами[1]. В качестве параметров могут выступать различные сочетания букв, цифр и знаков, уникальные номера, физиологические особенности человека. В настоящее время наиболее популярными идентификаторами являются пароли, информация на смарт-картах, отпечатки пальцев.

1.2 Аутентификация

Процедура аутентификации заключается в проверке предоставляемых данных, определенных при идентификации, на соответствие информации, хранящейся в системе. Наиболее распространенный пример аутентификации встречается в сети Интернета, где после регистрации на сайте необходимо вводить учетные данные для входа в личный кабинет, и вводить необходимо данные, указанные при регистрации.

1.3 Принцип работы

Классическая схема идентификации и аутентификации показан на рисунке 1.

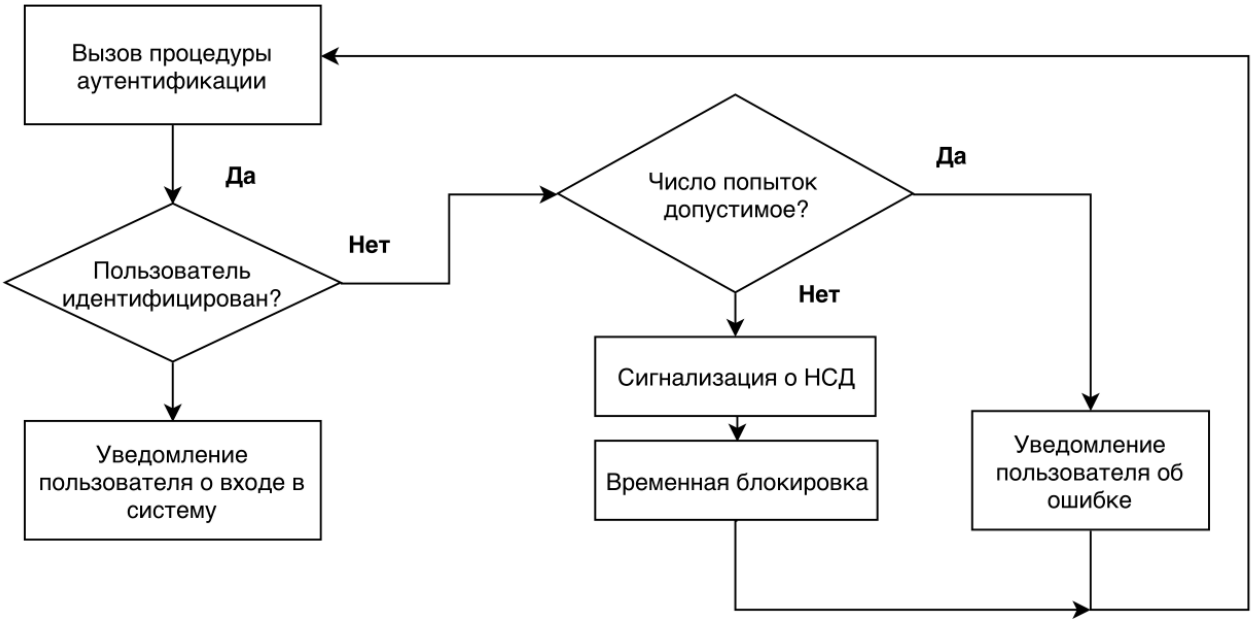

Рисунок 1. Классический пример идентификации и аутентификации.

После идентификации субъекта, полученная информация записывается в базу данных. Текущие значения будут определяться как «эталонные» для конкретного субъекта. Для успешной аутентификации субъекту необходимо передать на считывающее устройство те параметры, которые были указаны при идентификации. При совпадении значений доступ будет разрешен для текущего пользователя, а при неудачной попытке будет предложена повторная попытка аутентификации. Для большей безопасности количество попыток ограничено оптимальным значением, а если количество ошибок будет превышено, то производится сигнализация о несанкционированном доступе и блокируется возможность аутентификации.

Если речь идет о парольной идентификации, то в базе хранится информация не в открытом виде, а в виде хеш-значения для обеспечения более надежной безопасности.

2 Классификация средств идентификации и аутентификации

Современные средства идентификации и аутентификации имеют различные виды, сферы применения, степени надежности и экономические аспекты внедрения.

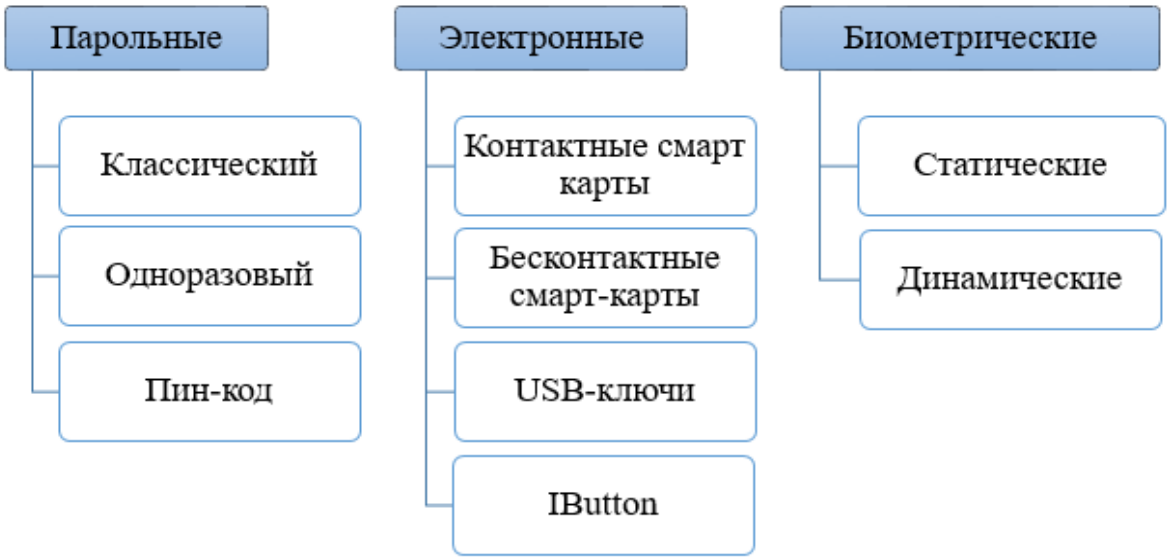

Рисунок 2. Виды средств идентификации и аутентификации.

3 Парольная защита

В большинстве информационных систем используется парольная защита. Это классическая ситуация, когда пользователи для входа в ту или иную систему вводят набор символов. Благодаря своей простоте реализации, данный метод получил огромную популярность во всем мире.

3.1 Принцип работы парольной защиты

Для регистрации субъекта в системе для начала необходимо сгенерировать уникальные параметры: набор цифр, букв разных регистров, символов. После этого полученная информация попадает в базу данных, и в последующих попытках входа в систему вводимая информация будет сравниваться со значениями, полученными при идентификации. Информация в базе данных хранится в зашифрованном виде, а именно – в виде хеш-значения. Это наиболее распространенная методика хранения и последующей проверки паролей, когда сравниваются не сами пароли в исходном виде, а их хеш-значения, полученные в результате преобразования по определенному правилу. Если база данных будет взломана, и информация попадет к нарушителю, то он не сможет узнать исходный пароль от учетных записей, т.к. процедура хеширования односторонняя, и невозможно из хеш-значения получить первоначальную информацию.

Для рационального использования парольной защиты следует определить, насколько секретна та информация, доступ к которой будет получать субъект. Если информация строго конфиденциальная, то следует использовать пароли длинной 10-12 символов с использованием букв разных регистров, цифр и символов. При этом ограничение действия пароля по времени также увеличит степень надежности пароля.

3.2 Достоинства и недостатки парольной защиты

Используя парольную защиту, возможно отказаться от внедрения дополнительных аппаратных средств защиты, процесс администрирования не приводит к большим затратам информационных и человеческих ресурсов. В дополнение к этому, для пользователей текущий метод аутентификации привычен и интуитивно понятен.

Однако существуют следующие угрозы безопасности парольных систем:

1. Разглашение параметров учетной записи через:
    a. подбор в интерактивном режиме;
    b. подсматривание;
    c. преднамеренную передачу пароля его владельцем другому лицу;
    d. захват базы данных парольной системы;
    e. перехват переданной по сети информации о пароле;
    f. хранение пароля в доступном месте.
2. Вмешательство в функционирование компонентов парольной системы через:
    a. внедрение программных закладок;
    b. обнаружение и использование ошибок, допущенных на стадии разработки;
    c. выведение из строя парольной системы.
3. Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:
    a. выбрать пароль, который легко запомнить и также легко подобрать;
    b. записать пароль, который сложно запомнить, и положить запись в доступном месте;
    c. ввести пароль так, что его смогут увидеть посторонние:
    d. передать пароль другому лицу намеренно или под влиянием заблуждения.

Также пользователь нередко становится противником любой системы безопасности, функционирование которой затрагивает его рабочие условия[*] из-за возникновения дополнительных рутинных операций. Данные явления не позволяют назвать парольную аутентификацию на основе постоянных паролей достаточным средством для обеспечения надежной защиты конфиденциальной информации.

3.3 Одноразовые пароли

Одноразовый пароль - это технология, основанная на принципе действия только для одного процесса аутентификации в течение ограниченного промежутка времени. Данный метод предотвращает угрозу разглашения параметров учетной записи и возможного перехвата информации. При перехвате одноразового пароля у нарушителя не будет возможности им воспользоваться.

В современных технологиях идентификации и аутентификации с помощью одноразовых паролей используется динамическая генерация ключей с использованием крипто-стойких алгоритмов. Такая информация доступна только для сервера аутентификации и клиента, она не передается по сети и, следовательно, недоступна для перехвата. В качестве исходных параметров используется известная обеим сторонам процесса аутентификации информация.

3.4 Уязвимости одноразовых паролей

Технология одноразовых паролей считается достаточно надежной, но у нее есть недостатки, присущие и другим системам. Наиболее серьезная проблема – возможность подмены сервера аутентификации. Пользователи будут отправлять свои данные на ложный сервер, с которого нарушитель будет получать всю информацию о субъектах. Полученную информацию злоумышленник может использовать для аутентификации на достоверном сервере, в результате чего он сможет пройти аутентификацию.

Существующий риск рассинхронизации сеансов на сервере и у клиента является серьезной проблемой синхронных систем. В этом случае информация не будет похищена, не попадет в открытые источники, но при этом пользователи не смогут пройти аутентификацию, и работа целой корпорации может прекратиться на неопределенное время. Данные ошибки случаются крайне редко, но цена ошибки при ее появлении будет высокой.

4 Электронные средства аутентификации

Электронные системы идентификации и аутентификации обеспечивают более надежную защиту, но при этом требуют внедрения дополнительных аппаратно-программных комплексов. USB-ключи представляют собой средства аутентификации, которые обеспечивают работу с цифровыми сертификатами и электронными цифровыми подписями[4]. Смарт-карты отличается от USB-ключей тем, что для использования смарт-карт необходимо наличие специального устройства чтения, подключаемого к персональному

компьютеру, а USB-ключи напрямую подключается к компьютеру через USB-порт. Выбор одной из этих технологий зависит от политики безопасности компании. При использовании автоматизированной системы пропуска, то использовать смарт-карты более целесообразно.

4.1 Смарт-карты

Бесконтактные смарт-карты широко используются в различных приложениях, важным свойством которых, выделяющим ее из ряда других смарт-карт, является отсутствие механического контакта с устройством, обрабатывающим данные с карты. Порядок проведения операций со смарт-картой и устройством чтения и записи определяется программным приложением. Пользователю необходимо поднести смарт-карту к считывателю, после чего происходит обмен данными между картой и устройством чтения, при этом карту можно хранить в бумажнике или чехле, что положительно сказывается на удобстве использования данной технологией, ведь это позволяет быстро пройти аутентификацию, но при этом возникает угроза несанкционированного произведения транзакции при попадании смарт-карты в поле антенны считывателя. Карта может начать процесс обмена информацией без ведома пользователя.

4.2 Электронные ключи iButton

Электронные ключи iButton предназначены для идентификации и последующей аутентификации пользователей, выполненные в цилиндрической форме из нержавеющей стали. Внутри содержится микросхема, хранящая в себе информацию о пользователе, которая используется в процессе аутентификации. Электронный ключ iButton, как и смарт-карту можно потерять, или его могут украсть.

Электронные технологии аутентификации не требуют от человека запоминать длинные и сложные комбинации, заботиться о секретности его пароля, что упрощает взаимодействие персонала с информационными системами, однако смарт-карта может быть утеряна или украдена, что также не позволяет назвать данный метод абсолютным и универсальным средством надежной аутентификации пользователей[1].

5 Биометрические системы аутентификации

Биометрия – совокупность методов идентификации и аутентификации пользователей на основе их физических отличительных характеристик, которые могут быть статическими и динамическими. Статические характеристики – отпечатки пальцев, сетчатки глаз, сканеры лица, рисунок вен. Динамические, или же поведенческие, – это уникальность некоторых действий пользователя, например, особенности голоса, ручной подписи или при работе с клавиатурой. Человеческий организм настолько уникален, что биометрических методов может быть больше, чем всех остальных методов аутентификации вместе взятых, а также наиболее перспективным направлением в области изучения способов защиты информации.

Процесс идентификации начинается с создания базы данных потенциальных пользователей путем снятия и последующей обработкой, заносится в базу данных полученную информацию. После этого при аутентификации пользователя повторяется процесс снятия и обработки, после чего результат сравнивается с данными в системе. В случае совпадения шаблонов пользователь получает доступ[3].

Биометрические методы аутентификации, в отличие от остальных методов, содержат множество возможных способов аутентификации, которые кардинально отличаются друг от друга. Так, метод аутентификации по сетчатке глаза является узкоспециализированным, но полученные результаты сложно фальсифицировать, а процент ошибок составляет сотые доли процента. В свою очередь, сканер отпечатка пальца стал настолько популярным, что большинство современных телефонов оснащены данным механизмом, однако, обладая необходимым оборудованием, имеется возможность обойти систему аутентификации по отпечатку пальца[4].

Табл. 1 – Сравнение биометрических методов аутентификации.

№	Метод аутентификации	Процент ошибок	Фальсификация	Скорость работы	Стоимость
1.	Отпечаток пальца	0,6%	Возможна	Высокая	Низкая
2.	Распознавание лица 2D	2,5%	Возможна	Средняя	Средняя
3.	Распознавание лица 3D	0,1%	Проблематична	Низкая	Высокая
4.	Радужная оболочка глаза	0,016%	Безуспешна	Высокая	Высокая
5.	Сетчатка глаза	0,4%	Невозможна	Низкая	Высокая
6.	Рисунок вен	0,01%	Невозможна	Высокая	Средняя

6 Заключение

Нельзя однозначно определить наилучший биометрический способ, каждый имеет свои достоинства и недостатки, но зачастую ключевым фактором становится цена вопроса реализации таких технологий. Минусов подобных технологий является их уникальность и сложность, а порой невозможность, изменения. Так, если база данных с биометрическими данными будет скомпрометирована, то данные радужной оболочки глаза нельзя будет сменить на новые, как это можно сделать с паролями[5].

Парольная защита на сегодняшний день остается одним из основных методов идентификации и аутентификации обычных пользователей ввиду простоты реализации, в то время как электронные методы повсеместно используются в коммерческих организациях из-за приемлемого соотношения цены к уровню защиты. Биометрические методы аутентификации на данный момент только набирают свою популярность, они, действительно, имеют большие перспективы на повсеместное внедрение в недалеком будущем. И все же,

какими бы ни были совершенными и безопасными системы идентификации и аутентификации, без соблюдения политик безопасности, технической защиты и других областей защиты информации вопрос о надежной защите информации от несанкционированного доступа будет оставаться открытым.

Список используемой литературы

[1] Интернет-ресурс. Идентификация и аутентификация – https://lektsii.org/10-60053.html

[2] Интернет-ресурс. Средства аутентификации – http://www.azone-it.ru/autentifikaciya-polzovateley

[3] Интернет-ресурс. SafeNet eToken 5110 http://www.cryptopro.ru/products/equipment/usbtokens/etoken

[4] Интернет-ресурс. Биометрическая идентификация http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html

[5] В.В.Платонов. Программные и аппаратные системы обеспечения безопасности – М. Издательский центр «Академия», 2013. – (Сер. Бакалавриат). с. 245.

[6] Р. Э. Смит Аутентификация: от паролей до открытых ключей. М.: «Вильямс», 2003. – с.160.

List of references

[1] Electronic resource – https://lektsii.org/10-60053.html

[2] Electronic resource – http://www.azone-it.ru/autentifikaciya-polzovateley

[3] Electronic resource – http://www.cryptopro.ru/products/equipment/usbtokens/etoken

[4] Electronic resource – http://www.techportal.ru/glossary/biom_identifikaciya.html

[5] V.V.Platonov. Software and hardware security systems - M. Publishing Center "Academy", 2013. - (Ser. Bachelor). with. 245.

[6] R. E. Smith Authentication: from passwords to public keys. M .: "Williams", 2003. - p. 160.

Анализ внутренних уязвимостей корпоративных сетей

Моторикин Д.В. [1]
popugayd8@mail.ru

Барышев Д.М. [1]
89242774511y@gmail.com

Лапина М.А. [1]
Кандидат физико-математических наук,
доцент norra7@yandex.ru

1 Северо-Кавказский федеральный университет
Ставрополь, 355009
Российская Федерация

Аннотация

Уязвимости, эксплуатация которых возможно только в пределах границ корпоративных сетей называются внутренними. Такой вид уязвимостей используется для несанкционированных действий с информацией в половине случаев. Из-за неправильных тенденций в обеспечении информационной безопасности защищённость корпоративных сетей от внешних атак находится на высоком уровне, а защищённость от внутренних уязвимостей напротив, на низком уровне. Именно поэтому важно понимать и уметь бороться с внутренними уязвимостями в корпоративной сети.

Abstract

Vulnerabilities, the exploitation of which is possible only within the boundaries of corporate networks are called internal. This type of vulnerability is used for unauthorized actions with information in half the cases. Due to incorrect trends in ensuring information security, the security of corporate networks from external attacks is at a high level, and protection from internal vulnerabilities is, on the contrary, at a low level. That is why it is important to understand and be able to deal with internal vulnerabilities in the corporate network.

Ключевые слова: уязвимость, сотрудник, злоумышленник, социальная инженерия, корпоративна сеть.

Keywords: vulnerability, employee, intruder, social engineering, corporate network.

Введение

Бурный рост технологий идет бок о бок с ростом количества уязвимостей, непосредственно связанных с данными технологиями, и неправильное понимание информационной безопасности является следствием создания уязвимостей, ведь принято считать, что вредоносные действия чаще всего исходят из-за границы периметра корпоративной сети, но на самом деле дешевле и проще эксплуатировать уязвимости изнутри сети. Из-за неправильных тенденций в обеспечении информационной безопасности часто защищённость корпоративных сетей от внешних атак находится на высоком уровне, а защищённость от внутренних уязвимостей напротив, на низком уровне. По данным InfoWatch в “Исследовании утечек конфиденциальной информации в компаниях сферы розничной торговли, гостиничного бизнеса и общественного питания“, 100% утечек в России в данной сфере связанны с внутренними уязвимостями организаций[6]. Такая статистика в социально значимой сфере полностью описывает проблемность ситуации с внутренними уязвимостями. Причиной этой проблемы является тот факт, что при наличии всех современных технологий защиты информации, они не обеспечивают защиту от неквалифицированного персонала, ошибок в администрировании корпоративных сетей, возможности внедрения злоумышленника во внутрь компании. В данной статье рассмотрим основные причины уязвимостей корпоративных сетей, рассмотрев исследование компании Positive Technologies на основе тестов на проникновение, проводившихся с 2015 по 2017 год. На рисунке № 1 представлена статистика полученная по результатам тестов на проникновения проводимых в 2016 и 2017 году.

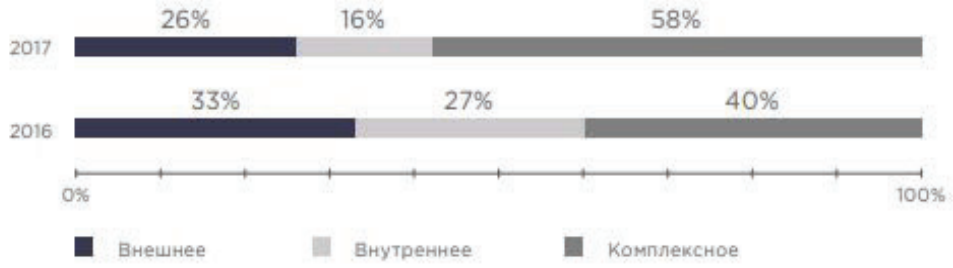

Рисунок 1.Виды тестирования на проникновения.

По результатам проведенных тестов была представлена статистика наиболее распространенных уязвимостей в корпоративных сетях за период 2017 года (Рисунок №2)

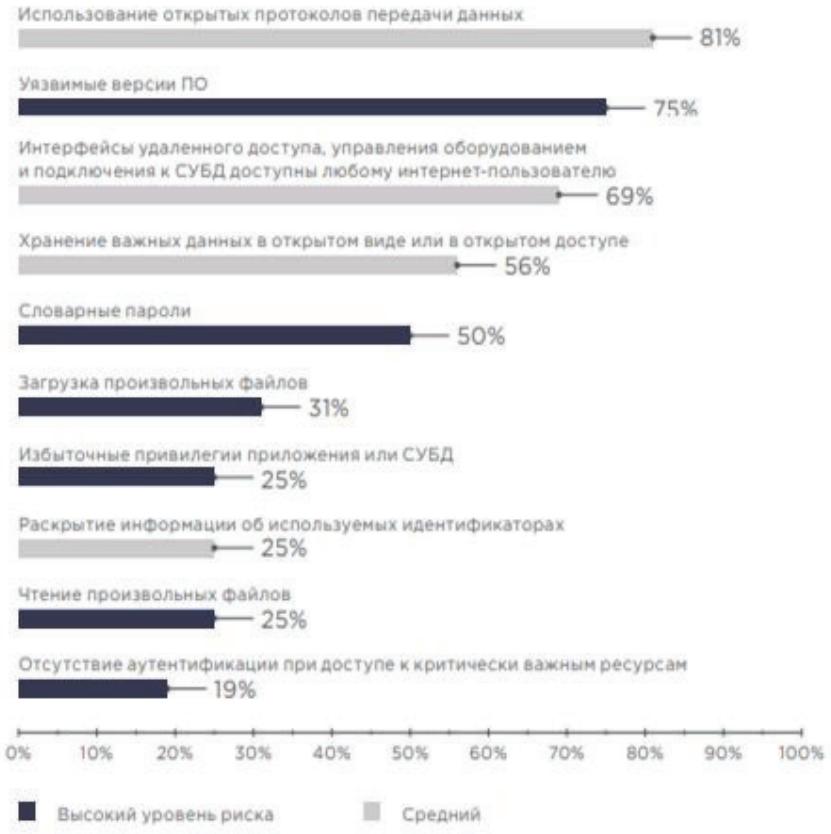

Рисунок 2.Наиболее распространенные уязвимости на сетевом периметре.[5]

Причины и решения внутренних уязвимостей

Выделим общие уровни взаимодействия корпоративной сети, для того чтобы разграничить области действий уязвимостей.

- Персонал – уровень, включающий в себя пользователей АРМ, обслуживающий персонал, и иных лиц, имеющих доступ к корпоративной сети и устройствам в ней.
- Приложения – различные приложения, установленные на хостах или серверах, взаимодействующие с сетью. (пример Браузеры)
- Операционные системы – уровень который включает в себя системы, установленные на конечных хостах в сети. (Пример Windows, Linux)
- Сети – уровень, включающий себя протоколы и стандарты взаимодействия между устройствами в сети. (Пример TCP/IP, ARP, DNS)

Данные уровни расставлены в иерархическом порядке, где на вершине будет находиться персонал, для более верного формирования понимания взаимодействия внутри корпоративных и иных сетях, так же следует выделить, что данная иерархия подойдет для рассмотрения не только внутренних угроз, но и внешних[1].
Рассмотрим типы уязвимостей и укажем, какие уровни корпоративной сети они затрагивают:

Уязвимости, связанные с ошибками в администрировании.

Данные уязвимости зависят от уровней Сети и Персонала, где непосредственно администратор своими действиями умышленно или нет, создают благоприятные условия

возможности утечки данных, компрометации сети и слабых мест, создания возможностей для использования эксплойтов.
Проблемой могут послужить, не отключенные и не используемые протоколы, службы, порты, они образуют уязвимости в системе защиты.

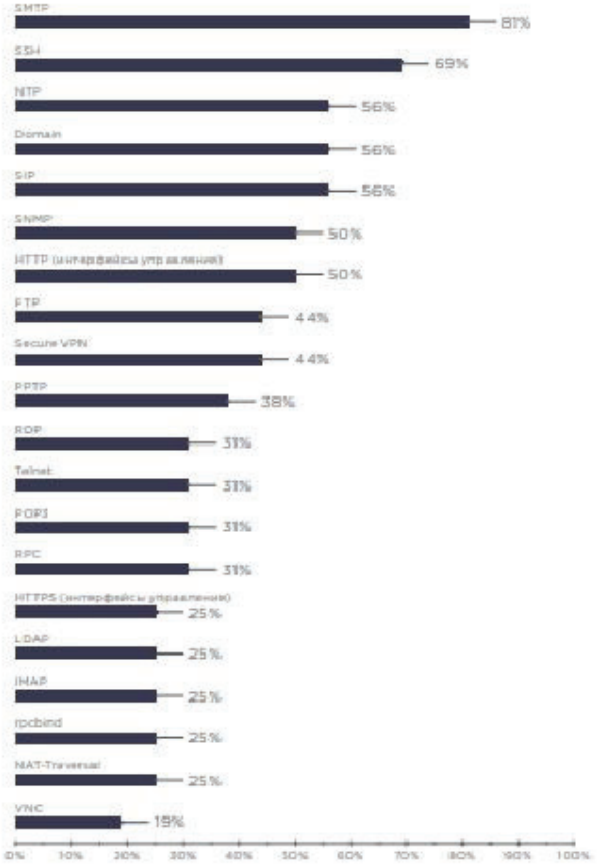

Рисунок 3. статистика использования протоколов в локальных сетях.[5]

На рисунке № 3 приведена статистика использования протоколов в локальных сетях, и стоит обратить внимание на не малую составляющую протоколов HTTP, Telnet которые не содержат в себе механизмов защиты, обеспечивающих шифрование и целостность данных. Использование таких протоколов в сети делает возможным реализацию атаки сниффинга, при которой весь перехваченный информационный поток полностью читаем, в следствии чего возможна компрометация парольно-ключевой информации[1].
Помимо использование слабо защищенных протоколов, грубейшей ошибкой отсутствие настройки механизмов безопасности. Например в телекоммуникационном оборудовании, при ненастроенных протоколах Port Security, ARP inspection, DHCP snooping, становятся возможны такие атаки как ARP-spoofing, DHCP starvation, “Человек Посередине”. Для реализации всех приведенных выше атак требует всего лишь доступ к локальной сети, что и делает эти атаки довольно популярными[3].

Использованием устаревших версий ПО.

Следующий вид уязвимостей затрагивает уровни Приложений и Операционных систем.
Любая система несовершенна по определению, и к любой из них можно найти уязвимости, которые представляют угрозу для сохранности данных. Разработчики для поддержания статуса своего продукта должны экстренно реагировать на возникшие дыры и лазейки, чтобы опередить злоумышленников, тем самым предостеречь пользователей их

продукции от утечки, уничтожения, модификации данных. Именно поэтому важно создать условия, при которых П.О. и О.С. будут регулярно обновляться[2].
Данный вид уязвимостей является острой проблемой в связи с тем, что часто обновления нагружают корпоративную сеть, вследствие чего может замедлять процесс работы, что в свою очередь является причиной для полного отказа от обновлений. Около 78 % исследуемых компаний показали наличие устаревших версий ПО при этом Средний возраст наиболее устаревших неустановленных обновлений — 73 месяца (более шести лет)[4]. На рисунке 4 приведена статистика, из которой видно, что за период с 2016 года и на период 2017 года эта проблема только прогрессировала. И вследствие чего безопасность сети в исследуемых компаниях резко падала.

Рисунок 4. Уровни риска уязвимостей связных с отсутствием обновления безопасности.

Социальная инженерия.

Следующей угрозой для корпоративной сети является социальная инженерия. Данная угроза направлена на уровень Персонала. Степень этой угрозы на прямую зависит от того на сколько персонал осведомлен в области информационной безопасности.
Социальная инженерия — один из наиболее распространенных методов целевых атак. Он сводится к эксплуатации недостатка у сотрудников опыта в вопросах безопасности. Нарушитель может выведать данные для доступа к ресурсам в телефонном разговоре или личной переписке.
Уровень осведомленности сотрудников в вопросах информационной безопасности постепенно возрастает, но пока остается на низком уровне: согласно исследованию, ни в одной из протестированных систем он не был оценен как приемлемый, хотя вдвое снизилась доля компаний, для которых уровень осведомленности сотрудников был оценен как крайне низкий. В 2015 году в среднем 24 % пользователей осуществили переход по поддельной ссылке. Не изменилась доля испытуемых, которые ввели свои учетные данные в заведомо ложную форму аутентификации или загрузили исполняемый файл: показатель остался на уровне 15 %[4].
Positive Technologies, провела исследование, с помощью социальной инженерии у сотрудника проверяемой компании были выведены учетные данные для доступа к рабочей станции сотрудника и ресурсам домена. Сотрудника выбрали в качестве мишени по результатам первичной рассылки фишинговых писем
Для рассылки Специалисты Positive Technologiest использовали письмо в котором домен, был схож по написанию с реально существующим. Внимательный сотрудник может легко обнаружить подозрительный адрес отправителя. НО практика показывает, что не все сотрудники замечают подмену. Кроме того, нарушитель может изменить адрес отправителя на реально существующий адрес одного из сотрудников, чтобы не вызвать подозрений.

Данный сотрудник не просто перешел по ссылке из письма, а еще и вступил в переписку с экспертом Positive Technologies, приняв его за администратора своей корпоративной сети. Входе переписки сотрудник с легкостью выдал не только информацию об используемом ПО, но и свой пароль , который оказался простым .
Но не все сотрудники поддаются на данный метод и при это метод можно быть обнаруженными службой безопасности . Поэтому злоумышленники часто привлекают более сложные социотехнические методы, которые требуют специальной подготовки. Примером более сложного сценария атаки может служить сценарий когда , злоумышленник регистрирует собственный домен и разработать ложную форму логина. Он создает фишинговый ресурс максимально схожим с оригинальным ресурсом , который привык видеть сотрудник. Атакующий также разрабатывает сценарии для определения версий ПО, используемого сотрудником, и последующей эксплуатации уязвимостей этого ПО[4].
Так же, пользователи сами могут создавать непреднамеренно уязвимости, используя сетевые ресурсы не по назначению, переходя на сайты с вредоносным ПО. Последствие проникновения вредоносного ПО может проявиться как в создании бэкдора, который послужит плацдармом для полного взлома корпоративной сети, так и внедрения программы-вымогателя.
В 2017 году наблюдались крупные кибератаки, в которых использовались программы-вымогатели по типу WannaCry. Нападению подверглись такие учреждение, как Национальная служба здравоохранения Великобритании или крупные компания как FedEx. Вымогатель представляет собой относительно простую форму вредоносной программы, шифрующей файлы на целевом компьютере и требующей выкуп за ключи расшифровки. Процент выплаченных выкупов достаточно высок, так как в большинстве случаев жертвы не имеют в своем распоряжении резервных копий. Все эти факторы сделали вымогатели популярным видом вредоносных программ у киберпреступников, которые часто требуют выкуп в виде криптовалюты, которую сложно отследить. Некоторым представителям программ-вымогателей (например, WannaCry) удалось скомпрометировать сотни тысяч компьютеров[6].

Внутренний саботаж

Следующий вид уязвимостей затрагивает уровни Сети, Операционные системы, Приложения и Персонал, поскольку осуществляется по средствам внутреннего саботажа.
Внутреннее саботирование может возникнуть по причине нарушение контрольной зоны неавторизованным лицом. Но данная уязвимость представляет малую угрозу поскольку большинство компаний организовывают контрольные пункты , систему видео наблюдения , и ограничения помещений с использованием технологий smart card, touch memory или подобных технологий .
Если проникновеннее в внутрь компании из вне становится достаточно сложным процессом, то подкуп рядового или уволенного сотрудника несет потенциальную угрозу.
В случае подкупа бывшего сотрудника, то злоумышленник может узнать структуру и возможные уязвимости корпоративной сети и другую полезную для него информацию , но в случае подкупа действующего сотрудника помимо разглашённой информации о структуре сети , есть угроза создание новой скрытой уязвимости. Примером такой угрозы может служить преодоление межсетевого экрана с помощью метода "Туннелирование". Суть этого метода заключается в том, что межсетевой экран может разрешать пакеты определённого протокола, тогда если за межсетевым экраном во внутренней сети, подкупленный сотрудник настроит туннель с внешним ресурсом и машиной внутри корпоративной сети, на которой будет установлен клиент туннелирования, то организуется обмен данными, который будут пропускаться межсетевым экраном. Такой канал будет, является скрытым.

Так же проблемой внутренней безопасности корпоративных сетей, затрагивающей уровень Операционных систем и Приложений, является не удовлетворяющая элементарным правилам безопасности, политика формирования паролей:

- Использование простых паролей;
- Большой период действия пароля;
- Хранение пароля на бумажном носителе или в электроном виде, на рабочем месте;
- Отсутствие ограничения попыток ввода пароля.
- А так же использование словарных паролей. Данный недостаток обнаружен в большинстве исследуемых проектах. При этом в 91 % случаев было выявлено использование слабых паролей для привилегированных учетных записей[5].

Решение внутренних уязвимостей

Для решения выше перечисленных проблем необходимо применять следующие решения:
Для решения проблем касательно неправильного администрирования, то необходимо отключить все не используемые порты и службы, и производить своевременные обновления системы.
Решить проблему с обновлениями поможет правильная настройка политики установки обновлений, в соответствии с которой П.О. и О.С. получают и устанавливаю обновления исключительно в то время, когда ресурсы компьютеров и сети не востребованы, а именно во внерабочее время.
Уязвимость паролей решается формированием строгой политики паролей, которая будет требовать от пользователя создания сложных паролей, установит срок действия пароля в 1 месяц и поставит ограничение на количество неудачных попыток и время блокировки учетной записи после серии последовательных неудачных попыток авторизации значительно усложнив внедрение злоумышленника в сеть. А также, заставив персонал не хранить пароль на бумажных носителях на рабочем месте и в электронном виде на компьютере, дополнительно обезопасит кражу легитимного пользователя.
Для нейтрализации угрозы со стороны социальной инженерии необходимо проводить семинары раз в 6 месяцев с персонала с целью повышения уровня осведомленности сотрудников в вопросах информационной безопасности. А также установка контроля посещения сайтов и антивирусов.
Для противодействия внедрению злоумышленника внутрь компании самому или через посредников в лице сотрудников необходимо использовать разграничение доступа к аппаратуре и информационным ресурсам, удаление учетных записей, паролей и изъятие ключ-карт уволенных сотрудников. А также напомнить сотрудникам о уголовной ответственности за промышленный шпионаж согласно статье 183 Уголовного Кодекса РФ о незаконном получении и разглашении сведений, составляющих коммерческую, налоговую или банковскую тайну. И что максимальное наказание, предусмотренное данной статьей, – лишение свободы сроком до десяти лет.
Заключение
Подводя итоги можно заметить, что больше всего внутренних уязвимостей происходят от не подготовленности сотрудником, а также неправильное администрирование корпоративной сети, но и меры устранения данных уязвимостей не являться трудно реализуемые. И поэтому что бы корпоративная сеть была полностью защищена, нужно проводить семинары по информационной безопасности с сотрудниками, а также проводить периодический аудит сети на наличие возможны угроз.

Список используемой литературы

[1] Корячко В.П., Перепелкин Д.А. Корпоративные сети. Технологии, протоколы, алгоритмы. -- М.: Изд-во Горячая Линия - Телеком, 2011. --220с.

[2] Thomas David,Gerarda Westerhuis The Power of Corporate Networks: A Comparative and Historical Perspective -- M.: Routledge, 2014. -- 350 с.

[3] Таненбаум Э., Уэзеролл Д. Компьютерные сети -- М.: Питер СПб, 2016. -- 960 с.

[4] Positive Technologies, Уязвимости корпоративных информационных систем — 2015: Дата обращения:29.11.18 Электронный ресурс: https://www.securitylab.ru/analytics/483024.php.

[5] Positive Technologies.,Уязвимости корпоративных информационных систем. Дата обращения:02.12.18 Электронный ресурс: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2018/

[6] InfoWatch, Исследование утечек конфиденциальной информации в компаниях сферы розничной торговли, гостиничного бизнеса и общественного питания», Дата обращения: 02.12.18 Электронный ресурс: https://www.infowatch.ru/presscenter/news/21243

List of references

[1] Koryachko V.P., Perepelkin D.A. Corporate networks. Technologies, protocols, algorithms. - M .: Hot Line Publishing House - Telecom, 2011. - 220c.

[2] Thomas David, Gerarda W. The Comparative and Historical Perspective - Moscow: Routledge, 2014. - 350 p.

[3] Tanenbaum E., Weatheroll D. Computer networks - Moscow: Peter SPb, 2016. - 960 p.

[4] Positive Technologies, Corporate Information Systems Vulnerabilities - 2015: Appeal: 11/29/18 Electronic resource: https: //www.securitylab.ru/analytics/483024.php.

[5] Positive Technologies., Vulnerabilities of corporate information systems. Appeal date: 02.12.18 Electronic resource: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2018/

[6] InfoWatch, Investigation of confidential information leaks in retail, hospitality and catering companies “Date of treatment: 02.12.18 Electronic resource: https://www.infowatch.ru/presscenter/news/21243

Секция 4. «Робототехнические системы»

РАЗРАБОТКА ПОДСИСТЕМЫ СЕНСОРОВ МОБИЛЬНОГО БАЛАНСИРУЮЩЕГО РОБОТА

Абелян А. А.[1]
ar.abelyan@yandex.ru

Уварова А. А.[1]
nastya.uvarova@mail.ru

Исаев А. М.[2]
isaev@stilsoft.ru

[1] Северо-Кавказский Федеральный Университет, Ставрополь, 355009, Россия
[2] Межинститутская базовая кафедра ФГАОУ ВО СКФУ, Ставрополь, 355009, Россия

Аннотация

Данная статья посвящена разработке подсистемы сенсоров мобильного балансирующего робота, являющейся частью комплекса MBR (mobile balancing robot – мобильный балансирующий робот). Главная задача подсистемы – получение данных с ультразвукового датчика и расчет расстояния до препятствий. Далее эта информация отправляется подсистеме управления роботом, которая, используя полученные данные, предотвращает столкновение роботизированного комплекса с препятствиями. Основой подсистемы сенсоров является микроконтроллер семейства STM32 модель F103. В качестве ультразвукового датчика расстояния используется дальномер HC-SR04. Контроллер запрограммирован на языке C. Программные модули включают в себя алгоритмы тактирования программы, виртуальных таймеров, опроса ультразвукового дальномера, а также конфигурирования модуля USART, который предназначен для преобразования входящей и исходящей информации для ее последующей передачи.

Abstract

This article is devoted to the development of a subsystem of sensors of the mobile balancing robot, which is part of the MBR complex (mobile balancing robot). The main task of the

subsystem is to obtain data from the ultrasonic sensor and calculate the distance to obstacles. Further, this information is sent to the robot control subsystem, which, using the data obtained, prevents the collision of the robotic complex with obstacles. The basis of the sensor subsystem is a microcontroller family STM32 model F103. The range finder HC-SR04 is used as an ultrasonic distance sensor. The controller is programmed in the language of the program. The software modules include the algorithms of the program, virtual timers, the survey of the ultrasonic rangefinder, as well as the configuration of the USART module, which is designed to convert the incoming and outgoing information for its further transmission.

Ключевые слова: Робототехника, мобильный балансирующий робот, язык программирования C, микроконтроллер STM32F103, ультразвуковой датчик HC-SR04, модуль USART, DMA.

Keywords: Robotics, balancing robot, programming, C programming language, microcontroller, ultrasonic sensor, STM32F103, HC-SR04, USART, DMA.

Комплекс «Мобильный балансирующий робот» представляет собой робототехническую систему и состоит из трех подсистем:

1. Подсистема управления: отвечает за определение угла наклона робота, а также за управление электроприводами.
2. Подсистема сенсоров: необходима для сбора информации с ультразвукового датчика расстояния и отправки этой информации подсистеме управления.
3. Подсистема отладки: предназначена для отображения информации о состоянии системы в реальном времени.

В статье рассмотрены характеристики, модули и алгоритмы, использующиеся в подсистеме сенсоров.

Подсистема сенсоров состоит из микроконтроллера STM32F103C8, а также ультразвукового дальномера HC-SR04.

Микроконтроллер STM32 был выбран в качестве аппаратной базы из-за оптимального соотношения «цена-качество». В частности, семейство STM32F103x6 обладает следующими характеристиками [8]:

– высокопроизводительное 32-битное RISC-ядро ARM Cortex-M3;
– тактовая частота: до 72 МГц;
– объем флэш-памяти: до 32 Кбайт;
– объем SRAM: до 6 Кбайт;

- поддержка широкого спектра интерфейсов ввода-вывода и периферийных устройств, подключенных к двум APB шинам;
- два 12-разрядных АЦП, три 16-битных таймера общего назначения, а также один таймер ШИМ;
- коммуникационные интерфейсы: SPI, I2C, USART, USB 2.0, CAN.

Микроконтроллеры STM32 программируются на языке С.

Дальномер HC-SR04 обеспечивает определение расстояния до объектов в радиусе четырех метров. Датчик имеет четыре выходных контакта (пина): Vcc – питание, положительный контакт, Trig – цифровой вход, Echo – цифровой выход, GND – питание, отрицательный контакт.

HC-SR04 имеет следующие характеристики [7]:

- напряжение питания: 5 В;
- потребление в режиме тишины: 2 мА;
- потребление при работе: 15 мА;
- диапазон расстояний: 2-400 см;
- эффективный угол наблюдения: 15°;
- рабочий угол наблюдения: 30°;

Для работы микроконтроллера необходимо обеспечить тактирование системы. Тактовый сигнал применяется для синхронизации цифровых схем. Для тактирования в микроконтроллере STM32 широко используются встроенные таймеры общего назначения. Для эффективной работы таймера необходимо настроить его конфигурацию, в которую входят следующие параметры [9]:

- значение перезагрузки (Autoreload) – число «тиков» таймера, после которого подсчет начнется сначала;
- делитель часов (Clock division) – понижает частоту входящего импульса в определенное количество раз;
- режим подсчета (CounterMode) – определяет, каким образом будет вестись подсчет: снизу-вверх или сверху-вниз. В рассматриваемом случае счетчик должен считать от нуля до значения перезагрузки (то есть вверх);
- предварительный делитель (Prescaler) – предназначен для того, чтобы расширить диапазон формируемых частот. Внутренний сигнал процессора, пройдя через предделитель, будет поступать с определенной скоростью. В рассматриваемом случае скорость равна 1 импульс в микросекунду.

Результаты конфигурирования таймера представлены на рисунке 1.

```
void
HPT_InitTIMForProgTact(uint32_t ovefrlowVal)
{
    __HAL_RCC_TIM4_CLK_ENABLE();
    LL_TIM_InitTypeDef timInit_s;
    LL_TIM_StructInit(&timInit_s);

    timInit_s.Autoreload = ovefrlowVal;
    timInit_s.ClockDivision = LL_TIM_CLOCKDIVISION_DIV1;
    timInit_s.CounterMode = LL_TIM_COUNTERMODE_UP;
    timInit_s.Prescaler = 72u;

    LL_TIM_Init(
        TIM4,
        &timInit_s);
    LL_TIM_EnableCounter(TIM4);
    LL_TIM_EnableIT_UPDATE(TIM4);

    NVIC_SetPriority(
        TIM4_IRQn,
        1);
    NVIC_EnableIRQ(
        TIM4_IRQn);

}
```

Рисунок 1. Код конфигурации таймера тактирования

После настройки таймера, необходимо запрограммировать системное прерывание, которое будет начинать новый программный такт, когда таймер переполнится. Код обработчика прерывания представлен на рисунке 2.

```
void TIM4_IRQHandler(void)
{
    LL_TIM_ClearFlag_UPDATE(TIM4);

    HPT_status_s.newProgTactEn_flag ++;
}
```

Рисунок 2. Обработчик системного прерывания

После того, как было настроено тактирование системы, можно приступить к конфигурированию работы дальномера.

Принцип работы датчика следующий: на входной пин Trig подается сигнал (восходящий фронт), который запускает устройство. Датчик посылает ультразвуковую волну, которая отражается от препятствия и попадает на приемник датчика. Это вызывает возникновение сигнала на выходном пине Echo (нисходящий фронт). Измерив время между подачей сигнала на Trig и приемом на Echo, можно вычислить расстояние между роботом и препятствием.

Для работы с изменением входного сигнала в STM32 предусмотрен механизм внешних прерываний (EXTI) [6]. Чтобы воспользоваться данным функционалом, необходимо настроить нужные пины, внешнее прерывание (будет ли оно вызываться на восходящем, нисходящем фронте, или на обоих), а также запрограммировать обработчик прерывания.

На рисунке 3 представлен код конфигурации интерфейса GPIO, соединенных с входами Trig и Echo дальномера [10].

```
/* Настройка тригера (Trig), который запустит датчик */
LL_GPIO_InitTypeDef GpioTrigCnfg_s;
LL_GPIO_StructInit(&GpioTrigCnfg_s);

GpioTrigCnfg_s.Pin = LL_GPIO_PIN_15;
GpioTrigCnfg_s.Mode = LL_GPIO_MODE_OUTPUT;
GpioTrigCnfg_s.OutputType = LL_GPIO_OUTPUT_PUSHPULL;
GpioTrigCnfg_s.Speed = LL_GPIO_MODE_OUTPUT_2MHz;
GpioTrigCnfg_s.Pull = LL_GPIO_PULL_UP;

LL_GPIO_Init(GPIOB, &GpioTrigCnfg_s);

/* Настраиваем пин 0 как вход (получит данные с Echo) */

LL_GPIO_InitTypeDef GpioEchoCnfg_s;
LL_GPIO_StructInit(&GpioEchoCnfg_s);

GpioEchoCnfg_s.Pin = LL_GPIO_PIN_0;
GpioEchoCnfg_s.Mode = LL_GPIO_MODE_ALTERNATE;
GpioEchoCnfg_s.Speed = LL_GPIO_MODE_OUTPUT_2MHz;
GpioEchoCnfg_s.Pull = LL_GPIO_PULL_UP;
GpioEchoCnfg_s.OutputType = LL_GPIO_OUTPUT_PUSHPULL;

LL_GPIO_Init(GPIOB, &GpioEchoCnfg_s);
```

Рисунок 3. Конфигурация пинов микроконтроллера

Рисунок 4 содержит код конфигурации внешнего прерывания.

```
/* Конфигурация контроллера внешнего прерывания */
LL_EXTI_InitTypeDef ExtiInit_s;
LL_EXTI_StructInit(&ExtiInit_s);

LL_GPIO_AF_SetEXTISource(LL_GPIO_AF_EXTI_PORTB, LL_GPIO_AF_EXTI_LINE0);

/* Задействуем линию 0 */
ExtiInit_s.Line_0_31 = LL_EXTI_LINE_0;
/* Разрешаем прерывание */
ExtiInit_s.LineCommand = ENABLE;
/* Настраиваем работу линии в режиме прерывания */
ExtiInit_s.Mode = LL_EXTI_MODE_IT;
ExtiInit_s.Trigger = LL_EXTI_TRIGGER_RISING_FALLING;
LL_EXTI_Init(&ExtiInit_s);

LL_EXTI_EnableIT_0_31(LL_EXTI_LINE_0);

NVIC_SetPriority(EXTI0_IRQn, 3);
NVIC_EnableIRQ(EXTI0_IRQn);
```

Рисунок 4. Конфигурация внешнего прерывания

Две последние строчки кода, представленного выше, устанавливают приоритет прерывания в векторе прерываний.

Последний этап работы дальномера – программирование обработчика прерывания – представлен на рисунке 5. В нем используется виртуальный таймер, который запускается при восходящем фронте и останавливается на нисходящем.

```
void EXTI0_IRQHandler(void)
{
    if(LL_EXTI_IsActiveFlag_0_31(LL_EXTI_LINE_0))
    {
        VTMR_InitTimerStruct(&VirtTmr_s, NULL, VT_LOWER_CNT);
        if(HAL_GPIO_ReadPin(GPIOB, LL_GPIO_PIN_0) != 0)
        {
            // Возрастающий фронт. Запускаем таймер
            VTMR_StartTimer(&VirtTmr_s);

        }
        else if(HAL_GPIO_ReadPin(GPIOB, LL_GPIO_PIN_0) == 0)
        {
            // Спадающий фронт. Возвращаем значение таймера
            SonarValue = VTMR_GetTimerValue(&VirtTmr_s);

        }
        LL_EXTI_ClearFlag_0_31(LL_EXTI_LINE_ALL);
    }

}
```

Рисунок 5. Обработчик внешнего прерывания

Для отображения на компьютере измеряемых дальномером данных был использован USB-UART (COM-порт) конвертер. Периферийное устройство микроконтроллера, преобразующее входящие и исходящие байты в последовательный поток данных таким образом, чтобы было возможно передать их по одной физической цифровой линии другому аналогичному устройству – это универсальный синхронный / асинхронный приемник / передатчик USART (Universal Synchronous / Asynchronous Receiver / Transmitter) [2].

Схема подключения между микроконтроллером STM32F103, имеющего три последовательных USART порта, и USB-UART конвертером приведена на рисунке 6. Данные от передающего пина (Tx) одного модуля поступают на вход принимающего пина (Rx) другого модуля. Также необходимо наличие общей земли и подключения питания.

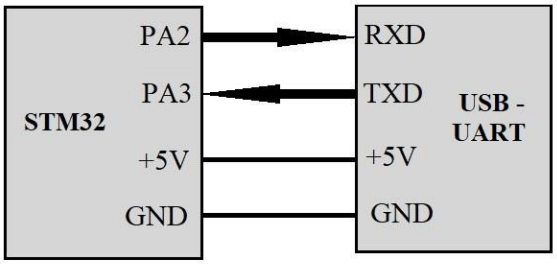

Рисунок 6. Схема подключения по USART между двумя устройствами

Для того, чтобы работать с USART необходимо настроить интерфейс ввода / вывода общего назначения GPIO (General-purpose Input / Output) [4]. Это контакты микроконтроллера Tx и Rx. Так как используется USART2, то тогда необходимо настроить пины PA2 на выход и PA3 на вход и назначить для них альтернативную функцию [1]. Конфигурация интерфейса ввода / вывода представлена на рисунке 7, а конфигурирование модуля USART2 – на рисунке 8.

```
static void
UFD_Init_IO_Ports(
    void)
{
    __HAL_RCC_GPIOA_CLK_ENABLE();

    LL_GPIO_InitTypeDef GPIO_init_s;
    GPIO_init_s.Mode        = LL_GPIO_MODE_ALTERNATE;
    GPIO_init_s.OutputType  = LL_GPIO_OUTPUT_PUSHPULL;
    GPIO_init_s.Pin         = LL_GPIO_PIN_2 | LL_GPIO_PIN_3;
    GPIO_init_s.Pull        = LL_GPIO_PULL_UP;
    GPIO_init_s.Speed       = LL_GPIO_MODE_OUTPUT_50MHz;

    LL_GPIO_Init(
        GPIOA,
        &GPIO_init_s);
}
```

Рисунок 7. Конфигурирование GPIO

```
static void
UFD_Init_USART2_TxRx(
    uint32_t baudrate)
{
    __HAL_RCC_USART2_CLK_ENABLE();

    LL_USART_InitTypeDef USART_init_s;
    USART_init_s.BaudRate               = (uint32_t) baudrate;
    USART_init_s.DataWidth              = LL_USART_DATAWIDTH_8B;
    USART_init_s.HardwareFlowControl    = LL_USART_HWCONTROL_NONE;
    USART_init_s.Parity                 = LL_USART_PARITY_NONE;
    USART_init_s.StopBits               = LL_USART_STOPBITS_1;
    USART_init_s.TransferDirection      = LL_USART_DIRECTION_TX_RX;

    LL_USART_Init(
        USART2,
        &USART_init_s);

    LL_USART_Enable(USART2);

    /* Конфигурирование источников прерываний */
    LL_USART_EnableIT_RXNE(USART2);

    /* Конфигурирование вектора прерываний */
    NVIC_SetPriority(USART2_IRQn, 5);
    NVIC_EnableIRQ(USART2_IRQn);
}
```

Рисунок 8. Конфигурирование модуля USART2

Для передачи данных на аппаратном уровне между памятью и периферией без участия процессора будет использоваться прямой доступ к памяти DMA (Direct Memory Access) [3], с помощью которого скорость передачи измеряемых данных увеличивается, что позволит системе управления после получения сообщения о возникшем препятствии остановить робота.

В STM32F103 только один 7-канальный DMA контроллер. Так как используется USART2 для передачи данных, то, согласно документации микроконтроллера, будет задействован седьмой канал [1]. Рисунок 9 демонстрирует инициализацию канала DMA1_Channel7 для UART2_Tx.

```
static void
UFD_Init_DMA1_Channel7_For_USART2_Tx(
    void)
{
    __HAL_RCC_DMA1_CLK_ENABLE();

    LL_DMA_InitTypeDef DMA_init_s;
    DMA_init_s.Direction               = LL_DMA_DIRECTION_MEMORY_TO_PERIPH;
    DMA_init_s.MemoryOrM2MDstAddress   = 0u;
    DMA_init_s.MemoryOrM2MDstDataSize  = LL_DMA_MDATAALIGN_BYTE;
    DMA_init_s.MemoryOrM2MDstIncMode   = LL_DMA_MEMORY_INCREMENT;
    DMA_init_s.Mode                    = LL_DMA_MODE_NORMAL;
    DMA_init_s.NbData                  = 0u;
    DMA_init_s.PeriphOrM2MSrcAddress   = (uint32_t) &USART2->DR;
    DMA_init_s.PeriphOrM2MSrcDataSize  = LL_DMA_PDATAALIGN_BYTE;
    DMA_init_s.PeriphOrM2MSrcIncMode   = LL_DMA_PERIPH_NOINCREMENT;
    DMA_init_s.Priority                = LL_DMA_PRIORITY_LOW;

    LL_DMA_Init(
        DMA1,
        LL_DMA_CHANNEL_7,
        &DMA_init_s);

    /* Конфигурирование источников прерываний */
    LL_DMA_EnableIT_TC(DMA1, LL_DMA_CHANNEL_7);
    LL_DMA_EnableIT_TE(DMA1, LL_DMA_CHANNEL_7);

    /* Конфигурирование вектора прерываний */
    NVIC_SetPriority    (DMA1_Channel7_IRQn, 5);
    NVIC_EnableIRQ      (DMA1_Channel7_IRQn);
}
```

Рисунок 9. Конфигурация канала DMA1_Channel7

Для передачи данных по модулю USART2 с помощью канала DMA была создана функция, представленная на рисунке 10.

```
void
UFD_StartForceDMATransmit(
    uint32_t *pMemSource,
    uint16_t cnt)
{
    /* Отключение модуля USART2 */
    LL_USART_Disable(USART2);

    /* Отключение канала DMA */
    LL_DMA_DisableChannel(
        DMA1,
        LL_DMA_CHANNEL_7);

    /* Установить адрес, откуда начнется передача */
    LL_DMA_SetMemoryAddress(
        DMA1,
        LL_DMA_CHANNEL_7,
        (uint32_t) pMemSource);

    /* Восстановить количество байт, которое необходимо передать по каналу DMA */
    LL_DMA_SetDataLength(
        DMA1,
        LL_DMA_CHANNEL_7,
        cnt);

    /* Включить в USART запрос на передачу DMA */
    LL_USART_EnableDMAReq_TX(USART2);

    /* Включить канал DMA */
    LL_DMA_EnableChannel(DMA1, LL_DMA_CHANNEL_7);

    /* Включить USART */
    LL_USART_Enable(USART2);
}
```

Рисунок 10. Функция для передачи данных по модулю USART2 с помощью канала DMA

Таким образом, в ходе выполненных работ была создана подсистема сенсоров. Данные с датчика используются для расчета расстояния до препятствия, после чего это расстояние помещается в специальный буфер, в котором хранятся последние измерения. Наиболее актуальное из них по команде отправляется через модуль USART подсистеме управления.

Список используемой литературы

[1] STMicroelectronics Справочное руководство [Электронный ресурс]. URL: https://www.st.com/content/ccc/resource/technical/document/reference_manual/59/b9/ba/7f/11/af/43/d5/CD00171190.pdf/files/CD00171190.pdf/jcr:content/translations/en.CD00171190.pdf (Дата обращения: 28.11.2018).

[2] Программирование STM32F103. USART [Электронный ресурс]. URL: http://www.avislab.com/blog/stm32-usart_ru/ (Дата обращения: 28.11.2018).

[3] DMA (прямой доступ к памяти) [Электронный ресурс]. URL: http://www.rotr.info/electronics/mcu/stm32_dma.htm (Дата обращения: 28.11.2018).

[4] Понимание GPIO у STM32F0, часть 1 [Электронный ресурс]. URL: http://hertaville.com/stm32f0-gpio-tutorial-part-1.html (Дата обращения: 28.11.2018).

[5] STMicroelectronics Справочное руководство // STM32F103x8, STM32F103xB. – 2015. – 117 с.

[6] Программирование STM32F103. EXTI [Электронный ресурс]. URL: http://www.avislab.com/blog/stm32-exti_ru/ (Дата обращения 28.11.2018).

[7] Руководство пользователя – HC-SR04 ультразвуковой датчик// Cytron Technologies – 2013 – 10 с.

[8] STM32F103C8. Описание устройства [Электронный ресурс]. URL: https://www.st.com/content/st_com/en/products/microcontrollers/stm32-32-bit-arm-cortex-mcus/stm32-mainstream-mcus/stm32f1-series/stm32f103/stm32f103c8.html (Дата обращения 28.11.2018)

[9] Программирование STM32F103. Тактирование [Электронный ресурс]. URL: http://www.avislab.com/blog/stm32-clock_ru/ (Дата обращения 28.11.2018).

[10] Программирование STM32F103. GPIO [Электронный ресурс]. URL: http://www.avislab.com/blog/stm32-gpio_ru/ (Дата обращения 28.11.2018).

[11] D.S. Vidhya, D.P. Rebelo, C.J. D'Silva Obstacle Detection using Ultrasonic Sensors (Обнаружение препятствий с использованием ультразвуковых датчиков) // International Journal for Innovative Research in Science & Technology, Volume 2, Issue 11, April 2016 – 850 с.

List of references

[1] STMicroelectronics Reference manual [Electronic resource]. URL: https://www.st.com/content/ccc/resource/technical/document/reference_manual/59/b9/ba/7f/11/af/43/d5/CD00171190.pdf/files/CD00171190.pdf/jcr:content/translations/en.CD00171190.pdf (Date of the application: 28.11.2018).

[2] Programming of STM32F103. USART [Electronic resource]. URL: http://www.avislab.com/blog/stm32-usart_ru/ (Date of the application: 28.11.2018).
[3] DMA (Direct Memory Access) [Electronic resource]. URL: http://www.rotr.info/electronics/mcu/stm32_dma.htm (Date of the application: 28.11.2018).
[4] Understanding the STM32F0's GPIO, part 1 [Electronic resource]. URL: http://hertaville.com/stm32f0-gpio-tutorial-part-1.html (Date of the application: 28.11.2018).
[5] STMicroelectronics Reference manual // STM32F103x8, STM32F103xB. – 2015. – 117 p.
[6] Programming STM32F103. EXTI [Electronic resource]. URL: http://www.avislab.com/blog/stm32-exti_ru/ (Date of the application: 28.11.2018).
[7] Product User's Manual – HC-SR04 Ultrasonic Sensor // Cytron Technologies – 2013 – 10 p.
[8] STM32F103C8. Device's description [Electronic resource]. URL: https://www.st.com/content/st_com/en/products/microcontrollers/stm32-32-bit-arm-cortex-mcus/stm32-mainstream-mcus/stm32f1-series/stm32f103/stm32f103c8.html (Date of the application: 28.11.2018)
[9] Programming STM32F103. Clocking [Electronic resource]. URL: http://www.avislab.com/blog/stm32-clock_ru/ (Date of the application: 28.11.2018).
[10] Programming STM32F103. Clocking [Electronic resource]. URL: http://www.avislab.com/blog/stm32-gpio_ru/ (Date of the application: 28.11.2018).
[11] D.S. Vidhya, D.P. Rebelo, C.J. D'Silva Obstacle Detection using Ultrasonic Sensors // International Journal for Innovative Research in Science & Technology, Volume 2, Issue 11, April 2016 – 850 p.

ПРОЕКТИРОВАНИЕ МОБИЛЬНОГО ДВУХКОЛЕСНОГО БАЛАНСИРУЮЩЕГО РОБОТА В СРЕДЕ SOLIDWORKS

Важенская И. А.[1]
i-vazhenskaya@mail.ru

Тупикина М. А.[1]
masha5550123@gmail.com

Исаев А. М.[2]
старший преподаватель межинститутской кафедры
isaev@stilsoft.ru

[1] Северо-Кавказский Федеральный Университет, Ставрополь, 355029, Россия

[2] Северо-Кавказский Федеральный Университет, Ставрополь, 355029, Россия

Аннотация

На сегодняшний день 3D-моделирование активно используется во множестве сфер человеческой деятельности, включая промышленность и робототехнику. Возможности трехмерного моделирования позволяют продемонстрировать прототип будущего коммерческого продукта в объемном формате. Целью работы является проектирование трехмерной модели двухколесного балансирующего робота, предназначенного для имитации перевернутого маятника. Разрабатываемая модель используется для отладки программного кода. Используемый метод проектирования – поэтапное моделирование деталей робота в системе автоматизированного проектирования, в число основных направлений развития которой вошло трехмерное (твердотельное) проектирование. В ходе выполнения проекта использовался SolidWorks – программный продукт, обеспечивающий разработку изделий любой сложности и назначения. Выбранная среда проектирования является одним из наиболее эффективных и удобных методов твердотельного моделирования, широкий спектр

возможностей которого позволяет создавать модели деталей, сборочных единиц различного типа и уровней сложности. Результатом проделанной работы стала трехмерная модель двухколесного балансирующего робота, состоящего из двух узлов: управления и двигателей. Каждая из подсборок в свою очередь для простоты проектирования была предварительно разделена на дополнительные сборочные единицы различного типа и уровней сложности. Помимо самостоятельно смоделированных деталей, были использованы стандартные изделия из библиотек, прилагаемых к среде проектирования или онлайн каталоги 3D-моделей, поддерживаемые компанией SolidWorks Corp.

Abstract

Today 3D-modeling is actively used in a set of spheres of human activity, including the industry and robotics. Possibilities of three-dimensional modeling allow to show a prototype of future commercial product in a volume format. The purpose of work is design of three-dimensional model of the two-wheeled balancing robot intended for simulation of the inverted pendulum. The developed model is used for debugging of a program code. The used design method – step-by-step modeling of details of the robot in an automated design engineering system which main directions of development three-dimensional (solid-state) design was among. During execution of the project SolidWorks – the software product providing development of products of any complexity and assignment was used. The selected design-time environment is one of the most effective and convenient methods of solid modeling which wide range of possibilities allows to create models of details, assembly units of different type and levels of complexity. The three-dimensional model of the two-wheeled balancing robot consisting of two nodes became result of the done work: management and engines. Each of subassemblies in turn for simplicity of design was previously divided into additional assembly units of different type and levels of complexity. In addition to independently simulated details, standard products from the libraries attached to design-time environment or online the directories of 3D models supported by the SolidWorks Corp company were used.

Ключевые слова: моделирование, САПР, трехмерное моделирование, робототехника, робот, SolidWorks, сборка, узел сборки, 3D-модель, проектирование.

Keywords: modeling, CAD, three-dimensional modeling, robotics, robot, SolidWorks, assembly, assembly node, 3D model, design.

Развитие современного информационного общества не стоит на месте, поэтому нет ничего удивительного в том, что в след за ним развиваются и информационные системы (ИС). Одной из таких является система автоматизированного проектирования (САПР), в число основных направлений развития которой вошло трехмерное (твердотельное) проектирование [2].

На сегодняшний день 3D-моделирование активно используется во множестве сфер человеческой деятельности, включая промышленность и робототехнику. Его возможности позволяют продемонстрировать прототип будущего коммерческого продукта в объемном формате, что играет большую роль при демонстрации какого-либо проекта или проведении презентации.

3D-моделирование – проектирование трехмерной модели по заранее подготовленному чертежу или эскизу. Построение объемных моделей происходит в программных комплексах САПР для работ промышленных предприятий на этапах конструкторской и технологической подготовки производства.

Для выполнения трехмерной модели придерживаются следующего плана:

1. Моделирование элементов конструкции.
2. Задание материалов моделей.
3. Построение сборки из разработанных элементов.
4. Симуляция динамики (используется для проверки взаимодействия частей модели).
5. Проверка разработанной модели.
6. Подготовка модели для изготовления.

В ходе выполнения проекта использовался SolidWorks – программный продукт, вышеописанной категории, обеспечивающий разработку изделий высокой сложности и назначения. К решаемым им задачам относятся конструкторская подготовка производства (КПП), технологическая подготовка производства (ТПП) и управление данными и процессами. Система включает в себя программные модули собственной разработки и сертифицированное программное обеспечение (ПО) от специализированных разработчиков (SolidWorks Gold Partners).

Программный комплекс SolidWorks включает в себя не только базовые конфигурации (Standard, Professional и Premium), но и различные прикладные модули: инженерные расчеты и управление инженерными данными, электротехническое проектирование и разработка интерактивной документации, контроль качества, анализ технологичности, безбумажные технологии и другие. Производитель предоставляет коммерческие и учебные лицензии [1].

Выбранная среда проектирования является одной из наиболее эффективных и удобных методов твердотельного моделирования, широкий спектр возможностей которой позволяет создавать модели деталей, сборочных единиц различного типа и уровней сложности.

Целью работы стало проектирование трехмерной модели двухколесного балансирующего робота для отладки программного кода. Так как данный робот является обучающей моделью, было решено спроектировать только каркас, на который в последствии планировалось закрепить управляющую электронику и датчики. Корпус для данной модели будет разрабатываться на следующем этапе работ.

В первую очередь было решено разработать алгоритмы проектирования трехмерной модели, благодаря которому стало возможным последующее деление задач между конструкторами. В результате алгоритм приобрел следующий вид:

1. Разделение модели на узлы сборки.
2. Выделение подзадач в проектировании каждого узла.
3. Моделирование узлов в независимые подсборки.
4. Объединение узлов в общую сборку.
5. Финальная проверка готовой модели.
6. Рендеринг (визуализация).
7. Изготовление разработанных деталей.
8. Сборка шасси робота.

Следуя оговоренному плану, модель была условно разделена на узел управления и узел двигателей. После этого каждый из проектировщиков разделил работу над выбранным узлом на несколько подзадач. На следующем шаге было решено обратиться к проектам более опытных проектировщиков, в результате чего процесс моделирования был разделен на несколько этапов:

1. Составление технического задания.
2. Сбор информации (наименование, назначение, характеристики уже существующих коммерческих проектных решений) и анализ конструкторско-технологической документации изделий (описание, чертежи, схемы и алгоритмы сборки).
3. Разработка 3D моделей имеющихся для сборки деталей (электромоторы, колеса).
4. Моделирование деталей малых размеров и простой конструкции (втулка, крепления для платы Bluetooth-модуля и аккумулятора).
5. Моделирование деталей средних размеров, обладающих достаточно сложной геометрической конфигурацией (крепления для электромоторов и контроллеров векторного регулятора).
6. Поиск и использование стандартных изделий из библиотек, прилагаемых к среде проектирования или онлайн каталогов 3D-моделей, поддерживаемых компанией SolidWorks Corp (платы и модули).
7. Сборка выполненных моделей в отдельные узлы (подсборки узлов двигателей и управления).
8. Окончательная сборка узлов.
9. Рендеринг готовой модели.

Первые два этапа очень важны, потому что от верной постановки задачи и достаточного количества собранной информации зависит результат работы. В процессе их выполнения был определен объект моделирования, выявлены не только его техническое назначение в целом, но и его отдельных элементов. Именно эти данные легли в основу требований к конечному результату. К сбору информации об объекте, в число которой вошли чертежи, ГОСТы, эскизы и конструкторско-технологические спецификации (КТС) и т. д.

В нашем случае в качестве объекта моделирования был выбран двухколесный балансирующий робот, предназначенного для имитации перевернутого маятника и отладки программы управления. Он приводится в движение двумя электромоторами, управляемыми контролерами методом векторного регулирования. Принцип балансирования в данном случае заключается в противодействии двигателями падению робота.

Не меньшее внимание стоит обратить и на третий этап, результаты выполнения которого в случае ошибки повлияют на сборку в целом. Разработка 3D-модели проводится в тех случаях, когда найти готовую в свободном доступе не удается. В этом случае в первую очередь проводятся замеры детали, учитывая не только такие характеристики, как высота, длина и ширина, но и расстояние между винтовыми отверстиями, важными для модели вырезами. Размеры самих отверстий под резьбу также учитываются. Только после этого, сравнив полученные результаты с размерами указанным на чертеже, если таковой имеется, и проанализировав сам процесс моделирования детали, приступают к ее воплощению.

В контексте описываемого проекта, таковой деталью стал электромотор модели GBM4108-015 130T, чертеж которого представлен на рис. 1.

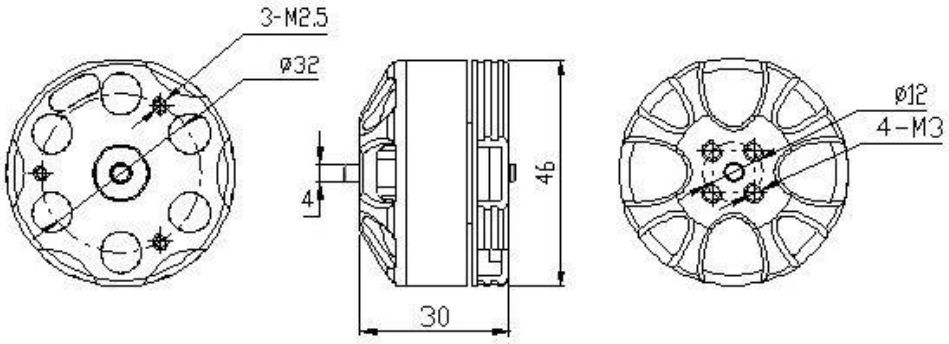

Рисунок 1. Чертеж бесщеточного мотора GBM4108-015 130T.

Следуя вышеописанному плану, были произведены фактические замеры, которые затем использовались при проектировании модели. Так как конструкция двигателя состояла из двух деталей: статора и нижней части статора наиболее логичным решением стало разделение сборки на две самостоятельные одноименные сборочные единицы. 3D-модель ротора – подвижной части мотора, представлена на рис. 2, а нижней части статора изображенной на рис. 3. Внутренние элементы конструкции электродвигателя не моделировались.

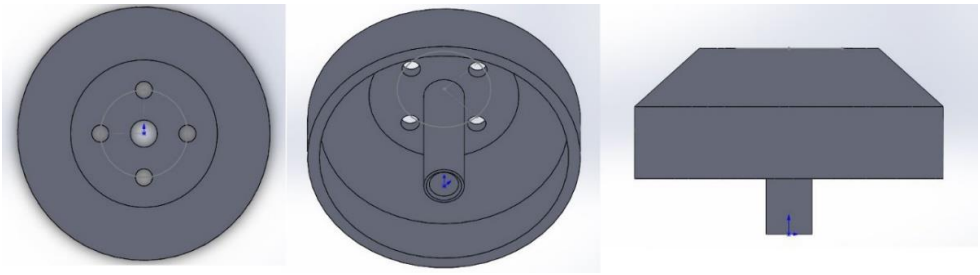

Рисунок 2. Трехмерная модель ротора электромотора GBM4108-015 130T.

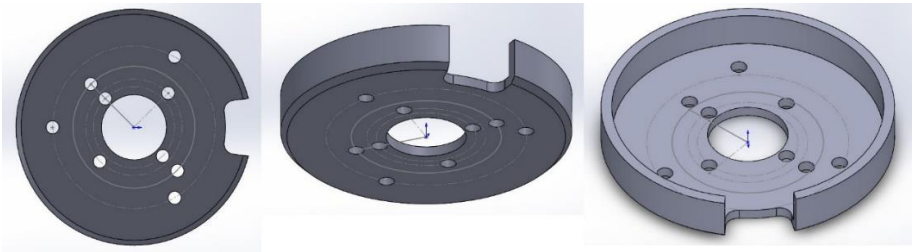

Рисунок 3. Трехмерная модель нижней части статора электромотора GBM4108-015 130T.

После того, как обе сборочные единицы были смоделированы, их объединили в общую сборку. Вид получившейся модели представлен на рис. 4.

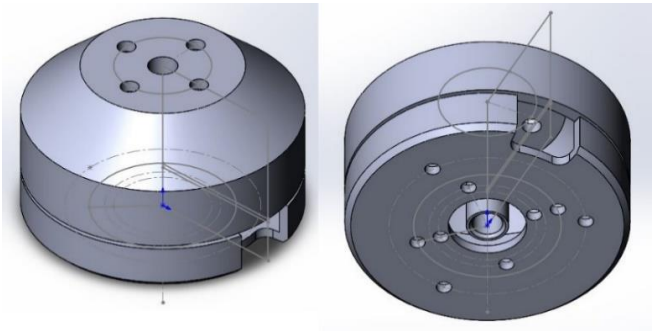

Рисунок 4. Трехмерная модель электромотора GBM4108-015 130T (сборка).

На этапе четвертом были спроектированы детали простой конструкции. Большая их часть моделировалась для узла управления и затем отфрезерована из стеклотекстолита толщиной 2 мм на станке с ЧПУ. В результате были получены крепления для аккумулятора и платы Bluetooth-модуля, представленных на рис. 5. Для большей наглядности была смоделирована аккумуляторная батарея. Ее можно будет увидеть на изображении общей сборки всего робота на рис. 12.

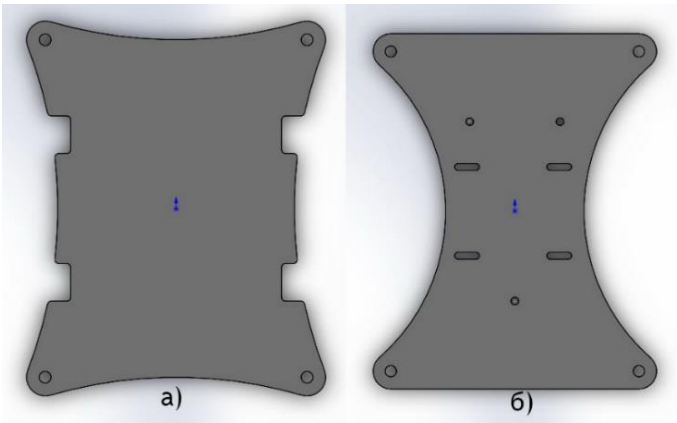

Рисунок 5. а) модель крепления для аккумулятора для узла управления;
б) модель крепления для платы Bluetooth-модуля для узла управления.

Для узла управления проектировались втулка для крепления магнита. Разработанная модель предназначалась для удерживания магнита напротив контроллера векторного регулятора и была распечатана на 3D-принтере. Ее модель продемонстрирована на рис. 6.

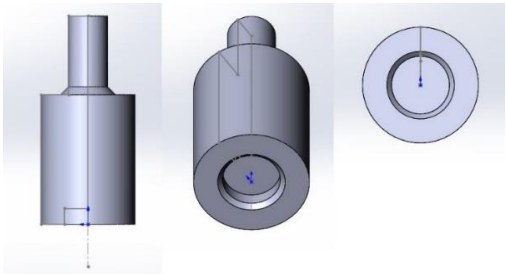

Рисунок 6. Трехмерная модель втулки для крепления магнита.

Помимо этого, для вышеупомянутого узла было смоделировано и вспомогательное крепление для векторного регулятора, представленного на рис. 7. Плата прикреплялась к нему вспомогательными втулками.

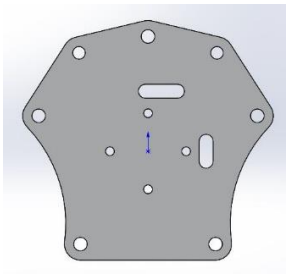

Рисунок 7. Модель вспомогательного крепления для контроллера векторного регулятора.

По завершению предыдущего этапа, привели в исполнение следующий – пятый. Так как одной из задач по конструированию узла двигателей было моделирование вспомогательного крепления для электромоторов, именно эта деталь проектировалась на этом шаге. Предполагалось, что на нее же в последствии будут крепиться вспомогательное крепление для контроллера векторного регулятора и узел управления. На рис. 8 представлен итоговый результат моделирования детали. В качестве материала для фрезеровки использовался поликарбонат толщиной 10 мм.

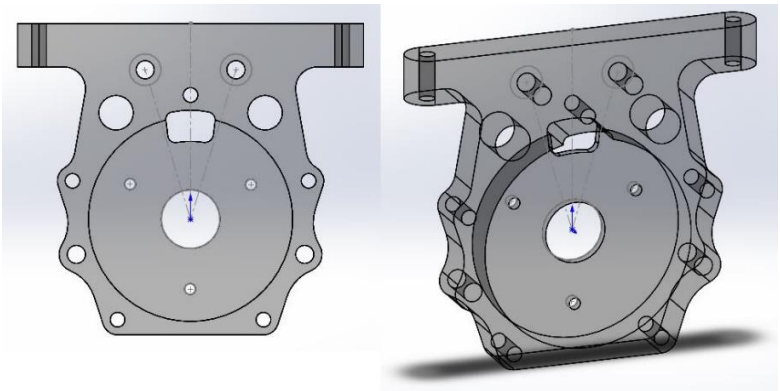

Рисунок 8. Вспомогательное крепления для электромотора.

По окончанию проектирования всех необходимых деталей и поиска недостающих готовых сборочных единиц, узлы были собраны. Для моделирования узла управления потребовались описанные выше вспомогательные крепления, смоделированные на четвертом этапе, Bluetooth-модуль и плата с управляющим контроллером, модели которых взяты у разработчика контроллера. Между собой вспомогательные крепления скреплялись соединительными втулками, аккумулятор и платы закреплялись с помощью пластиковых стяжек. Результат сборки узла управления представлен на рис. 9.

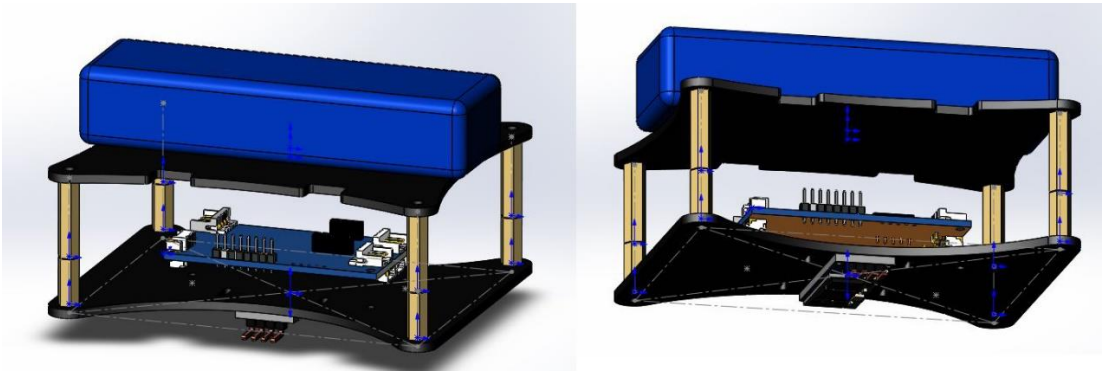

Рисунок 9. Трехмерная модель узла управления двухколесного балансирующего робота.

Так как проектируемый робот двухколесный, в конструкции его узла двигателей использовалось по два электромотора и контроллера векторного регулятора. Соответственно, для каждой пары «мотор-контроллер» потребовалось по два вспомогательных крепления для двигателя и платы. Между собой они соединялись втулками на фиксированном расстоянии, как представлено на рис. 10 и на рис. 11.

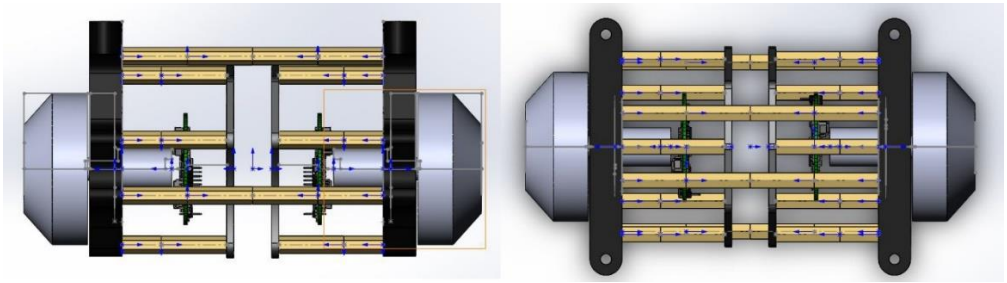

Рисунок 10. Трехмерная модель узла двигателей двухколесного балансирующего робота (вид сверху и спереди).

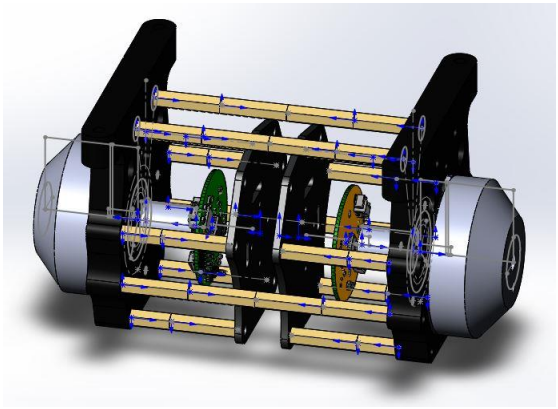

Рисунок 11. Трехмерная модель узла двигателей двухколесного балансирующего робота.

По завершению сборки узлов, они были объединены в одну модель и дополнены моделями колес. Этот этап стал завершающим в моделировании мобильного двухколесного балансирующего робота. Конечный результат сборки в формате рендеринга и фото собранного каркаса представлены на рис. 12 и рис. 13.

Рисунок 12. Рендеринг мобильного двухколесного балансирующего робота.

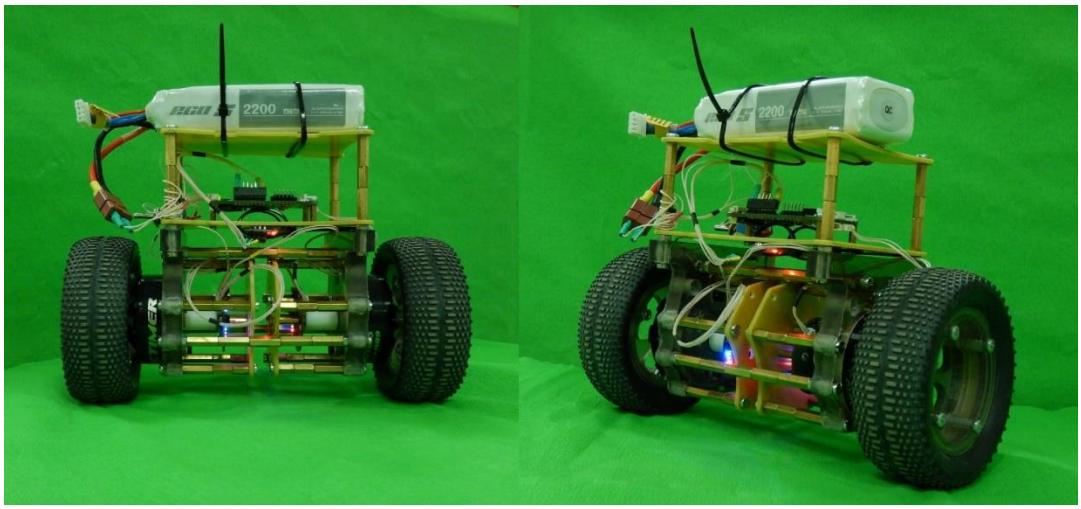

Рисунок 13. Фото мобильного двухколесного балансирующего робота.

Итак, как и планировалось, в результате выполнения проекта был сконструирован двухколесный балансирующий робот. На выполнение работы потребовался месяц. В качестве материалов по большей части был использован стеклотекстолит разной толщины, что обуславливалось назначением фрезеруемой детали. Между собой все элементы конструкции скреплялись винтами М3 и М4.

Исходя из того, что разработанный проект является имитацией обратного маятника, было решено распределить веса так, чтобы те в итоге располагались в максимальной высшей точке, благодаря чему выполняется условие балансировки.

Так как все поставленные задачи были выполнены, можно сделать вывод, что проект имеет право считаться завершенным. На момент написания статьи робот находится в эксплуатации на протяжении двух месяцев.

Список используемой литературы

[1] Статья «SolidWorks» [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/SolidWorks

[2] Статья «Система автоматизированного проектирования» [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Система_автоматизированного_проектирования

List of references

[1] Article "SolidWorks" [Electronic resource] – Access mode: https://ru.wikipedia.org/wiki/SolidWorks

[2] Article "Automated design engineering system" [Electronic resource] – Access mode: https://ru.wikipedia.org/wiki/Система_автоматизированного_проектирования

ИССЛЕДОВАНИЕ ВИБРАЦИЙ КОНСТРУКЦИИ МУЛЬТИРОТОРНОГО БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА МЕТОДАМИ СПЕКТРАЛ ЬНОГО АНАЛИЗА

Исаев М.А.[1]
mrraptor26@gmail.com

Исаев А.М.[1]
isaev@stilsoft.ru

Линец Г.И.[1]
д.т.н, заведующий кафедрой «Инфокоммуникации»

kbytw@mail.ru

Адамчук А.С. [1]
Кандидат физ-мат. наук, доцент, профессор кафедры прикладной математики и компьютерной безопасности ИИТиТ

adamchuk_anna@mail.ru

[1] Северокавказский федеральный университет, г.Ставрополь, 355009, Россия

Аннотация

В данной статье исследуются частоты вибраций корпуса мультироторного беспилотного летательного аппарата (МрБЛА) «Альбатрос-П», готовящегося к серийному выпуску. В процессе полета МрБЛА в его корпусе возникают вибрации от работающих двигателей, частоты которых добавляются в выходной сигнал датчиков, информация от которых используется для оценки пространственной ориентации летательного аппарата. Проблема состоит в том, что вибрации от электродвигателей в выходном сигнале датчиков вносят погрешность в оценку пространственной ориентации. Поэтому датчики, информация от которых используется для оценки пространственной ориентации, следует устанавливать на виброразвязанную площадку. Подбор формы, месторасположения и материала демпферов виброразвязки является сложной задачей, для выполнения которой необходимо сравнивать различные варианты. В связи с этим актуальной задачей является разработка

методики и инструментов, позволяющих получать численные значения частотных характеристик при различных вариантах виброразвязанной площадки. Для исследования частот, возникающих в полете, использовался 3-х осевой акселерометр, установленный в датчике ICM20608G, данные с которого поступали с частотой в 4 кГц, затем, записанные в полете данные обрабатывались с помощью дискретного преобразования Фурье в программной среде «Matlab». В результате были получены частотные характеристики вибраций корпуса и виброразвязанной площадки в виде численных значений, по которым выполняется построение соответствующих графиков. Предлагаемая в статье методика позволяет оценить частоты вибраций корпуса и виброизоляционной площадки на уже готовом образце МрБЛА в процессе его тестового полета.

Abstract

In this article, all types of vibrations of the multi-rotor unmanned aerial vehicle (MBLA) "Albatros-P", preparing for serial production, are researching. In the course of the flight, an MBLA is in its case from vibration from the electrical motors, the frequencies of which are added to the output signal of the sensors, the information from which is used to estimate the spatial orientation of the aircraft. The problem is that the vibrations from the electric motors in the sensor output signal introduce an error in the spatial orientation estimate. Therefore, the sensors, the information from which is used to estimate the spatial orientation, should be installed on the vibro-uncoupled area. The selection of the shape, location and material of the vibration isolators is a difficult task, for which it is necessary to compare the various options. In this regard, the actual task is to develop methods and tools to obtain numerical values of the frequency characteristics for different variants of a vibro-bonded platform. To research the frequencies occurring in flight, we used a 3-axis accelerometer installed in the ICM20608G sensor, data from which was received at 4 kHz, then the data recorded in flight were processed using the discrete Fourier transform in the Matlab software environment. As a result, the frequency characteristics of the vibrations of the casing and the vibro-bound platform were obtained in the form of numerical values, which are used to construct the corresponding graphs. The technique proposed in

the article allows us to estimate the frequencies of the vibrations of the body and the vibration-isolation platform on the already prepared MBPLA sample during its test flight.

Ключевые слова: беспилотный летательный аппарат, спектральный анализ, преобразование Фурье, вибрация, демпфирование, воздушный винт.

Keywords: unmanned aerial vehicle, spectral analysis, Fourier transform, vibration, damping, propeller.

1 Введение

При проектировании корпуса мультироторного беспилотного летательного аппарата (МрБЛА) особое внимание должно уделяться тем аспектам конструкции, которые напрямую влияют на ее жесткость и, как следствие, на резонансные частоты, возникающие в процессе полета МрБЛА, в основном, из-за работы электродвигателей. Исследование частот колебаний корпуса важно в силу того, что инерциальные датчики расположены непосредственно внутри, и все вибрации корпуса попадают в выходной сигнал датчиков. Частоты вибраций более 500 герц не несут полезной информации о движении МрБЛА и поэтому должны быть удалены из выходного сигнала датчиков. Одним из способов удаления высокочастотных составляющих является применение виброразвязки, которая выполняет функцию фильтра нижних частот и уменьшает амплитуду вибраций. Подбор вязкости материалов виброразвязки является сложной задачей, т.к. применение демпферов, не обладающих оптимальной формой и жесткостью, приведет либо к пропуску высокочастотных вибраций в выходной сигнал датчика, либо наоборот, в выходной сигнал будет добавлена дополнительная низкочастотная составляющая, которая внесет ощутимую погрешность в оценку пространственной ориентации МрБЛА. В связи с этим, актуальной задачей является получение численных значений механических частот корпуса и виброразвязки конкретной модели МрБЛА, которые позволят наглядно сравнивать спектрограммы различных вариантов виброразвязки как между собой, так и относительно спектрограммы корпуса. Частоты элемента конструкции можно оценить с помощью дискретного преобразования Фурье [1] линейных ускорений, полученных с помощью установленного акселерометра на данном элементе конструкции.

2 Постановка задачи

Требуется получить численные значения амплитуд и частот вибраций корпуса и виброразвязанной платформы при использовании различных винтов на существующем образце МрБЛА «Альбатрос – П» для оценки эффективности используемой виброразвязанной

платформы. В качестве оценки эффективности положен спектр частот вибраций и их амплитуда.

3 Разработка методики

Частоты вибраций измеряем с помощью 3-х осевых измерителей линейных ускорений, установленных на корпусе МрБЛА и на платформе, связанной с корпусом через виброизолирующие элементы. Затем, измеренные линейные ускорения переводим из временной области в частотную в программном пакете Matlab с помощью дискретного преобразования Фурье [2,3]. По результатам преобразования строим графики и сравниваем их между собой.

В качестве измерителя использовался датчик ICM20608G [4], содержащий 3-х осевой акселерометр, выполненный по микроэлектромеханической технологии. Диапазон измерений линейных ускорений был установлен ±16g. Микроконтроллер STM32F301 [5] выполняет опрос 3-х осевого акселерометра в датчике ICM20608G с частотой в 4 кГц по интерфейсу SPI, работающему на частоте в 9 МГц, затем выполняет приведение «сырых» показаний датчика к масштабу гравитационной единицы и отправляет каждое масштабированное измерение по интерфейсу UART на скорости 1500000 бод один раз в 125 микросекунд. С персональным компьютером микроконтроллер соединяется с помощью USB–to–UART конвертора, выполненного на базе микросхемы CP2104. Формат передаваемого сообщения имеет следующую структуру: первые два байта имеют код 0xAAAA и нужны для обнаружения сообщения в буфере программой «SerialPlot», выполняемой на ПК, затем идет байт, в котором закодирована длина «полезной» информации, в конце идут 12 байт в которых закодированы 3 переменные типа «float», по одной переменной на каждую ось датчика. Таким образом длина передаваемого пакета составляет 15 байт. Программа «SerialPlot» записывает все передаваемые данные в текстовый файл. После окончания эксперимента данные из текстового файла обрабатываются в программном пакете «MatLab» с помощью дискретного преобразования Фурье на интервале в 20 секунд с применением оконной функции Блэкмана – Харриса к исходному сигналу от акселерометра. При частоте дискретизации в 4000 кГц, интервал преобразования в 20 секунд позволяет получить разрешающую способность спектрального преобразования в $\frac{1}{20}$ Гц.

Выполнялось три тестовых полета в режиме висения над одной точкой:

- полет с воздушными винтами фирмы «T-Motor»;
- полет с воздушными винтами фирмы «Tarot»;
- полет с воздушными винтами фирмы «Tarot» и наклеенным грузом на лопасти одного из воздушных винтов (в качестве груза использовалось три слоя малярного скотча шириной в 20 мм) с целью повысить уровень вибраций и оценить эффективность используемой виброразвязки.

В каждом полете данные записывались одновременно с двух датчиков, один был установлен на внешней стороне корпуса МрБЛА, второй был установлен на платформе с датчиками самого МрБЛА, связанной с корпусом при помощи шести резинометаллических

муфт. Аккумуляторная батарея, массой 1350 гр., крепится жестко не относительно корпуса, а относительно платформы с датчиками для увеличения массы виброразвязанной платформы. После всех преобразований сравниваются по 2 спектральные характеристики, полученные по результатам одного тестового полета, а именно:

- спектральная характеристики вибраций корпуса
- спектральная характеристики вибраций виброразвязаннйо платформы.

4 Результаты

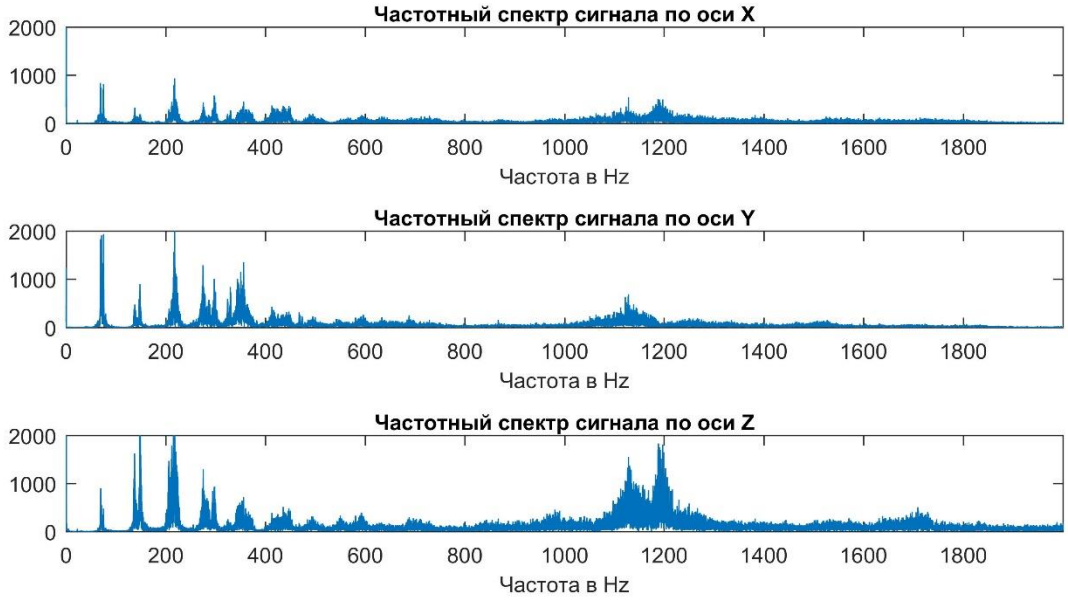

Рисунок 1. Частотный спектр вибраций корпуса. Воздушные винты фирмы «T- Motor».

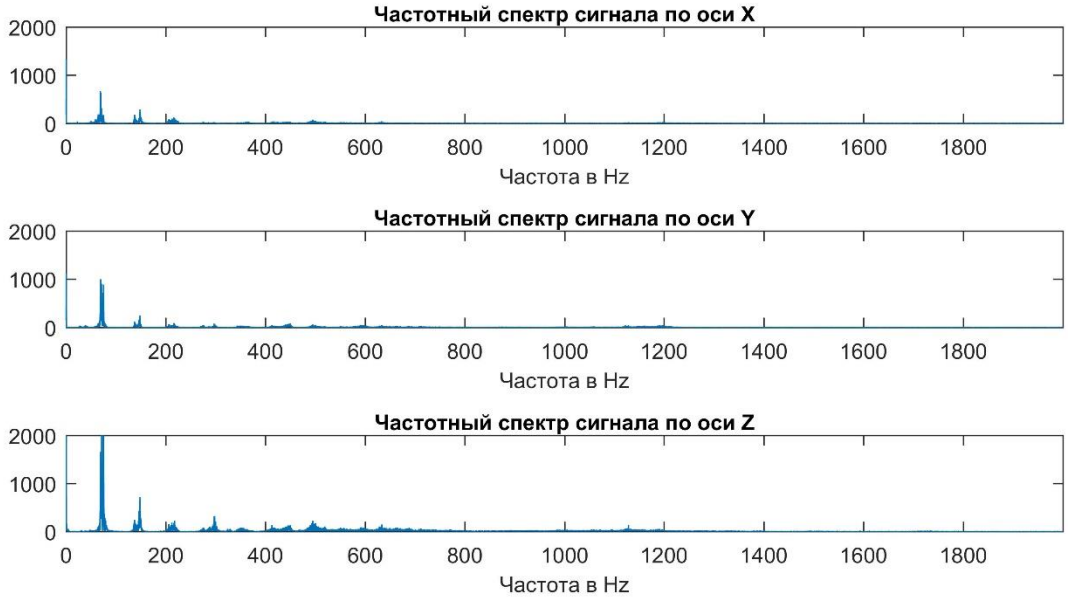

Рисунок 2. Частотный спектр вибраций платформы с оборудованием, установленным на виброизолирующих элементах. Воздушные винты фирмы «T-Motor».

Сравнив между собой частотные спектры на рисунке 1 (вибрации корпуса) и рисунке 2 (вибрации виброразвязанной платформы), видно, что виброразвязанная платформа существенно уменьшает амплитуду вибраций в диапазоне наблюдаемых частот. Но стоит отметить, что виброразвязка наоборот, увеличивает амплитуду вибрации по оси Z, пик которой находится на частоте в 72 Гц.

Частота в 72 Гц соответствует частоте вращения воздушного винта в 4320 об/мин. По заявленной производителем характеристике воздушного винта [6] можно сделать вывод, что данная частота вращения воздушного винта соответствует создаваемой электродвигателем тяги, которая необходима для поддержания исследуемого МрБЛА в режиме висения. Следовательно, можно сделать вывод, что виброразвязанная платформа входит в резонанс с частотой вращения воздушных винтов.

Для проверки данного предположения был выполнен тестовый полет с винтами другой фирмы, результаты которого представлены на рисунках 3 и 4. Если пиковая частота резонанса немного сместиться, т.к. винты другой фирмы будут иметь отличающуюся характеристику, то с большой долей вероятности резонанс возникает именно с частотой вращения воздушных винтов.

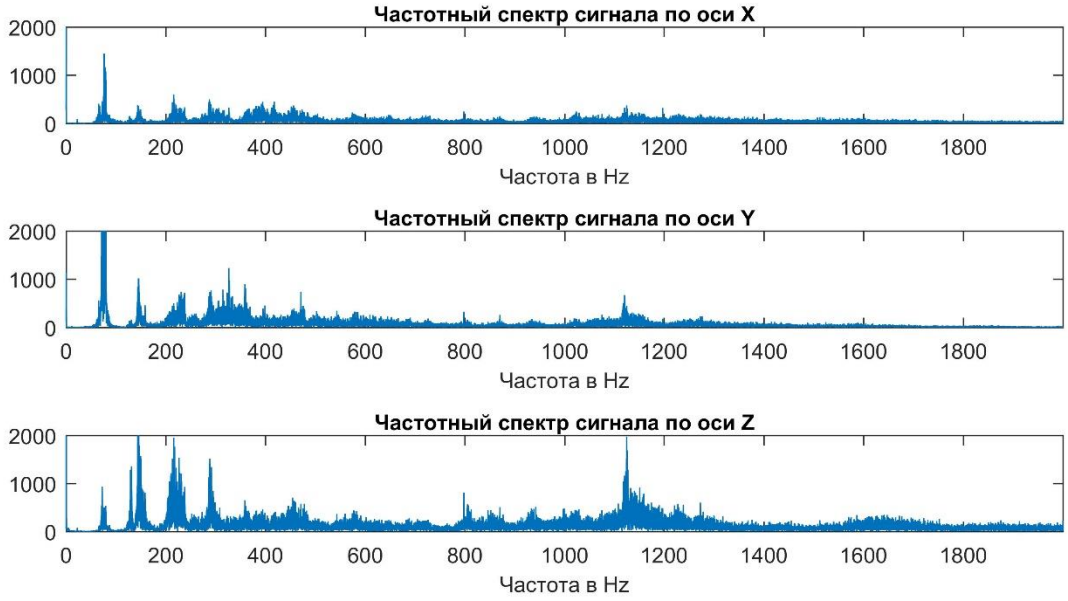

Рисунок 3. Частотный спектр вибраций корпуса МрБЛА. Воздушные винты фирмы «Tarot».

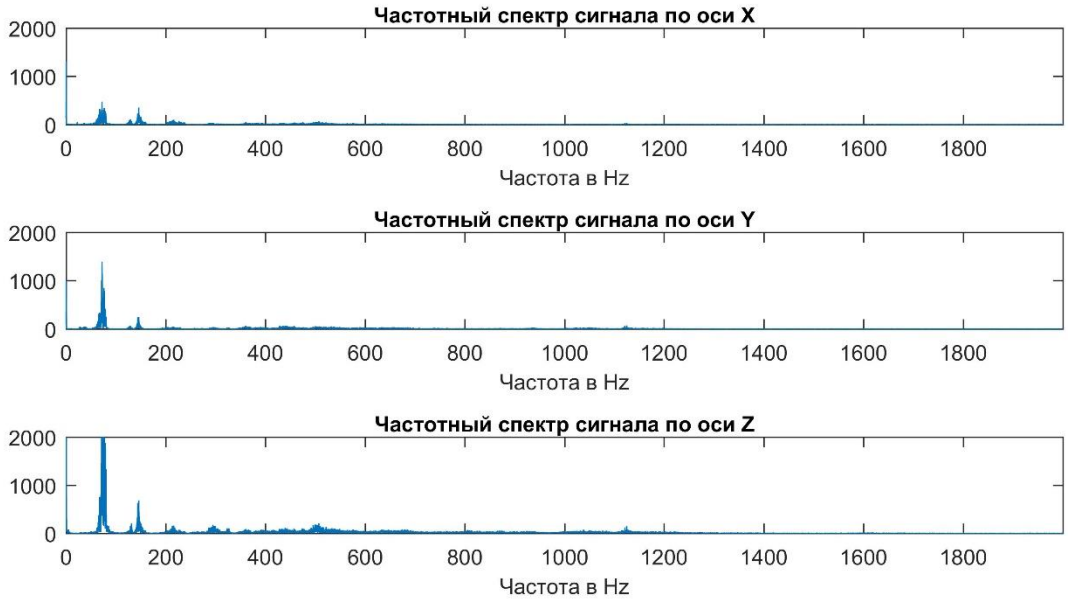

Рисунок 4. Частотный спектр вибраций платформы с оборудованием, установленной на виброизолирующих элементах. Воздушные винты фирмы «Tarot».

По частотным характеристикам на рисунках 3 и 4 видно, что виброразвязанная платформа так же существенно уменьшает амплитуду вибраций, но, как и во время 1-го тестового полета, возникает резонанс на частоте в 70.65 Гц по оси Z. Смещение пика вибрации при использовании другого типа винтов составляет 1.35 Гц. 2-й тестовый полет подтверждает то,

что резонанс виброразвязанной платформы возникает на частоте вращения винтов. В завершении эксперимента был выполнен 3-й тестовый полет с наклеенным грузом на одну из лопастей, результаты которого представлены на рисунках 5 и 6. Частота пика вибраций при использовании виброразвязки составляет:

- 72.45 Гц по оси X;
- 72.45 Гц по оси Y;
- 75.05 Гц и 71.8 Гц по оси Z (по оси Z выделяются два пика).

При использовании разбалансированного винта резонанс на виброразвязанной платформе возникает уже по 3-м осям, хотя амплитуда всех частот, в том числе и резонансной, уменьшается в несколько раз.

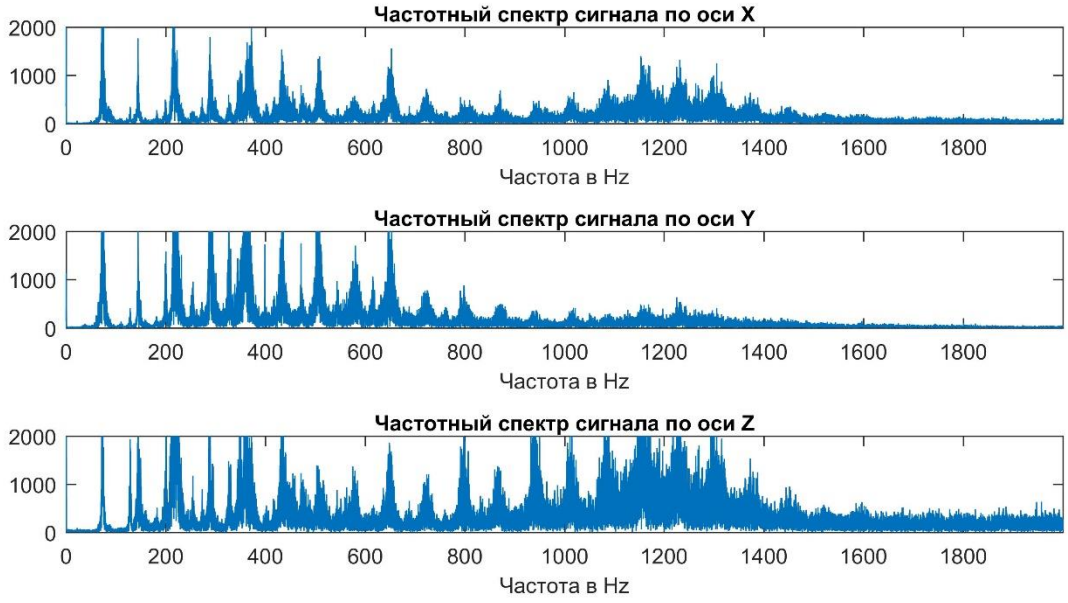

Рисунок 5. Частотный спектр вибраций корпуса МрБЛА. Воздушные винты фирмы «Tarot» с грузом, наклеенным на лопасть одного из винтов.

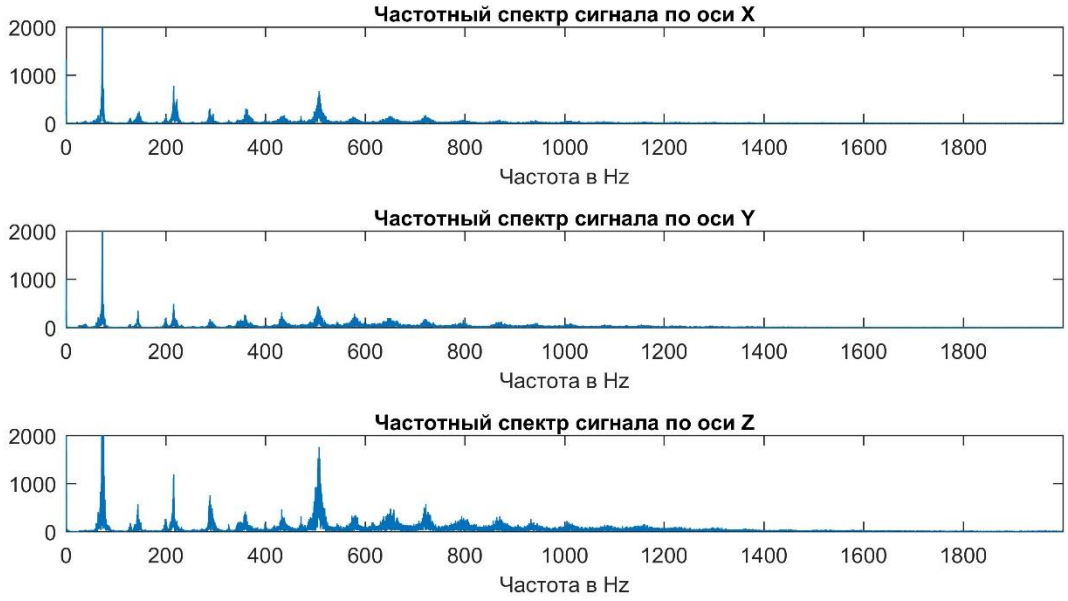

Рисунок 6. Частотный спектр вибраций платформы с оборудованием, установленном на виброизолирующих элементах. Воздушные винты фирмы «Tarot» с наклеенным грузом.

5 Обсуждение

Крепление аккумуляторной батареи неподвижно относительно виброразвязанной платформы, а не относительно самого корпуса, является, на наш взгляд, весьма удачным конструктивным решением т.к. в этом случае увеличивается масса виброразвязаннаной платформы без увеличения общей массы МрБЛА, что положительным образом сказывается на качестве виброизоляции. Используемая виброразвязанная платформа гасит амплитуды вибраций в несколько раз, но возникает резонанс на частоте вращения винтов. В силу того, что резонансная частота находится в области низких частот, её исключение из выходного сигнала является весьма сложной инженерной задачей, применение программного полосового фильтра не приведет к желаемым результатам, т.к. вместе с резонансной частотой будет исключен сигнал, содержащий полезную информацию.

6 Заключение

Был подготовлен весь необходимый инструментарий для проведения частотного анализа вибраций в МрБЛА. Проведенные эксперименты показали эффективность используемой виброразвязанной площадки и выявили её резонанс, возникающий на частоте вращения воздушных винтов.

Список используемой литературы

[1] Сергиенко А. Б. Цифровая обработка сигналов. — 2-е. — Спб: Питер, 2006. — С. 751. — ISBN 5-469-00816-9.
[2] Солонина А.И., Клионский Д.М., Меркучева Т.В., Перов С.Н., Цифровая обработка сигналов и MATLAB, 2013г.
[3] М. А. Павлейно, В. М. Ромаданов. Спектральные преобразования в MatLab. — СПб, 2007. — С. 160. — ISBN 978-5-98340-121-1.
[4] InvenSense. ICM-20608-G Datasheet // Revision 1.0
[5] STMicroelectronics STM32F301x6 STM32F301x8 Datashet
[6] T-MOTOR MN5208 KV340 [электронный ресурс]. – Режим доступа: https://www.foxtechfpv.com/t-motor-mn5208-kv340.html – Заглавие с экрана. – (дата обращения 02.12.2018).

List of references

[1] Sergienko A. B. Digital signal processing. – 2-nd – SPB: Piter, 2006. P.751. — ISBN 5-469-00816-9.
[2] Solonina A. I., Klionsky D.M., Merkucheva T.V., Perov S.N., Digital signal processing in MATLAB, 2013г.
[3] Pavleino M.A., Romadanov V.M. Spectral transform in MatLab. — SPB, 2007. — P. 160. — ISBN 978-5-98340-121-1.
[4] InvenSense. ICM-20608-G Datasheet // Revision 1.0
[5] STMicroelectronics STM32F301x6 STM32F301x8 Datashet
[6] T-MOTOR MN5208 KV340 [электронный ресурс]. – Access mode: https://www.foxtechfpv.com/t-motor-mn5208-kv340.html – (date of the application 02.12.2018).

Работа выполнена в рамках ФЦП ИР 2014-2020 (уникальный идентификатор RFMEFI57818X0222) при финансовой поддержке Министерства науки и высшего образования Российской Федерации по теме «Разработка роботизированного беспилотного летательного аппарата мультироторного типа с использованием бесплатформенной инерциальной навигационной системы».

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ АВИАТРАНСПОРТНОГО ПРЕДПРИЯТИЯ

Стадник Н.А.[1]
erter.live@gmail.com

Золотухин А.В.[1]
avol116@yandex.ru

Мокшин В.В.[1]
канд. техн. наук, доцент каф. АСОИУ
vladimir.mokshin@mail.ru

[1] Казанский национальный исследовательский технический университет имени А. Н. Туполева – КАИ, Казань, 420111, Российская Федерация

Аннотация

Актуальность исследования заключается в том, что в современном мире имитационное моделирование широко применяется в сфере логистики, перевозок и цепочек поставок. Однако имитационное моделирование в сфере проектирования объектов инфраструктуры, таких как дороги, и систем массового обслуживания, таких как метро, ж/д станции и аэропорты применяется достаточно редко. Особенно исключаются при моделировании работы систем массового обслуживания стохастические события и ЧП. Например, аэропорт города Казани не был готов к огромному наплыву туристов во время проведения Чемпионата Мира по футболу. В ходе анализа данного события была сформулирована проблема исследования: Как оптимизировать работу Казанского аэропорта в условиях максимального потока пассажиров? Для решения данной проблемы была поставлены следующие цели исследования: 1. Определение эффективности применения имитационного моделирования при проектировании авиационных предприятий и моделировании их работы в экстремальных условиях; 2. Проверка гипотезы, что изначальное проектирование Казанского аэропорта не предусматривало высокую пропускную способность; 3. Проверка гипотезы,

что имитационные модели позволяют провести подробные и высокоточные исследования работы технических процессов, а также их влияния на работу модели в условиях высочайшей загруженности. В данной работе в качестве метода исследования было проведено имитационное моделирование авиатранспортного предприятия. В результате была построена имитационная модель работы аэропорта, доказана гипотеза, что изначальное проектирование Казанского аэропорта не предусматривало высокую пропускную способность, и показана практическая значимость имитационного моделирования.

Abstract

The relevance of the study lies in the fact that in the modern world simulation modeling is widely used in the field of logistics, transportation and supply chains. However, simulation modeling in the design of infrastructure, such as roads, and queuing systems, such as subways, railway stations, and airports, is rarely used. Stochastic events and a state of emergency are especially excluded when modeling the operation of queuing systems. For example, the airport of Kazan was not ready for a huge influx of tourists during the World Cup. During the analysis of this event, the following research problem was formulated: How to optimize the work of Kazan Airport in the conditions of the maximum flow of passengers? To solve this problem, the following research objectives were set: 1. Determination of the effectiveness of the use of simulation in the design of aviation enterprises and the simulation of their work in extreme conditions; 2. Testing the hypothesis that the initial design of Kazan Airport did not provide for high capacity; 3. Testing the hypothesis that simulation models allow for detailed and high-precision studies of the operation of technical processes, as well as their influence on the operation of the model under the conditions of the highest workload. In this paper, a simulation of an air transport enterprise was conducted as a research method. As a result, a simulation model of the airport was built, a hypothesis was proved that the initial design of Kazan Airport did not provide for high capacity, and the practical significance of simulation modeling was shown.

Ключевые слова: Имитационное моделирование, проектирование, AnyLogic, система массового обслуживания, авиатранспортное предприятие, аэропорт, пассажирский поток, высочайшая загруженность.

Keywords: Simulation, design, AnyLogic, queuing system, air carrier, airport, passenger traffic, the highest workload.

1 Введение

В настоящее время имитационное моделирование используется во многих сферах деятельности человека – от производства до бизнеса. Активно оно применяется и в сферах массового обслуживания, в частности при строительстве аэропортов. Но зачастую при проектировании не учитывается множество параметров и не проверяется работа модели в нестандартных условиях. [1] Это отрицательно отражается на работе реальных предприятий. Например, аэропорт города Казани не был готов к огромному наплыву туристов во время проведения Чемпионата Мира по футболу. В среднем в период ЧМ в день аэропорт обслуживал больше 8 тысяч туристов, а максимальный дневной поток составил больше 26 тысяч. Всего за время проведения ЧМ Казанский Аэропорт обслужил больше 416 тысяч человек. В аэропорту работало все 3 терминала и еще один дополнительный пункт пропуска. Мы считаем, что его изначальное проектирование не предусматривало высокую пропускную способность. Нас эта проблема заинтересовала и легла в основу нашего исследования.

2 Постановка задачи

Таким образом, целью исследования стало определение эффективности применения имитационного моделирования при проектировании авиационных предприятий и моделировании их работы в экстремальных условиях. Нам было важно проверить гипотезу, что имитационные модели позволяют провести подробные и высокоточные исследования работы технических процессов, а также их влияния на работу модели в условиях высочайшей загруженности. Так были определены задачи исследования: 1. Анализ систем структурного и имитационного моделирования. 2. Выбор среды моделирования и изучение интерфейса системы. 3. Выбор объекта моделирования, изучение его основных характеристик. 4. Анализ моделируемой системы.

3 Разработка методики

В качестве объекта моделирования мы выбрали аэропорт с несколькими пунктами последовательного контроля и регистрации посетителей. В качестве среды моделирования выбрано программное обеспечение для имитационного моделирования AnyLogic, использующее графический язык моделирования. [2] Среда моделирования обеспечивает построение проектируемой модели из 2D и 3D объектов, представленных в AnyLogic агентами. Каждому агенту пользователь может присвоить переменные, параметры, функции, события и информационные связи с другими агентами. Встроенные средства рисования

позволяют быстро спроектировать необходимые 3D модели. Интерфейс программы представляет собой вид на окно настройки параметров, 2D и 3D модель объекта моделирования, а также окна статистики, и устройства логики модели. [3] Пример интерфейса программного обеспечения AnyLogic представлен на Рисунке 1.

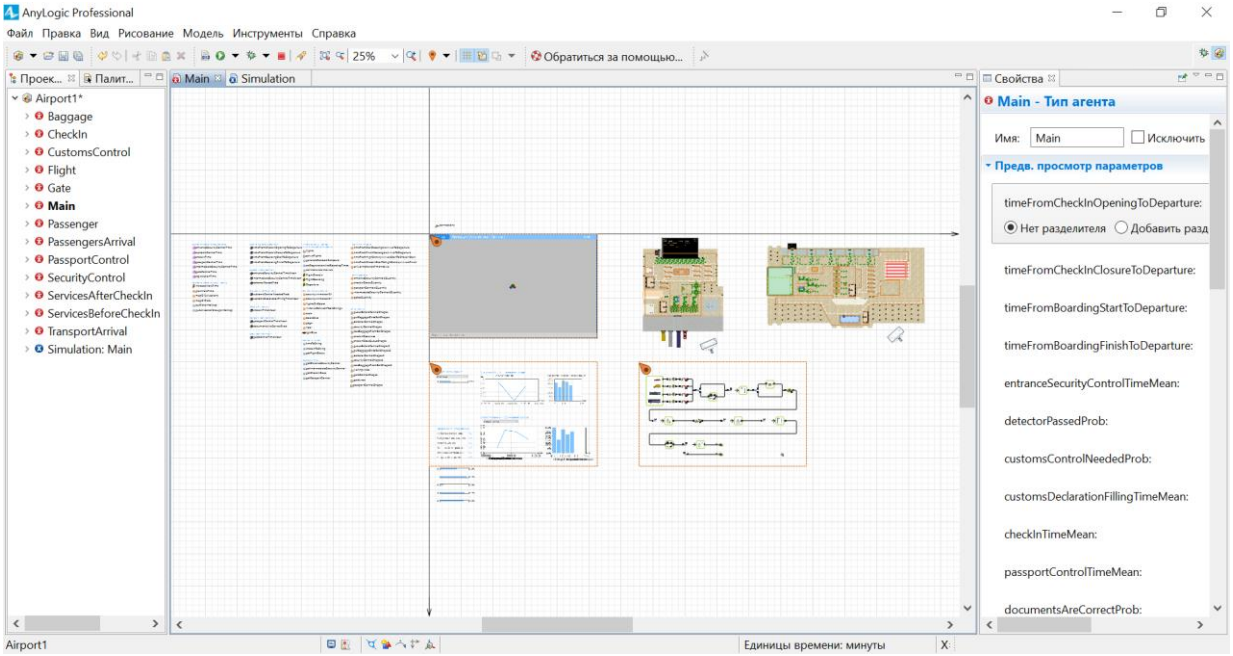

Рисунок 1. Интерфейс ПО AnyLogic

В качестве объекта моделирования выбрана точная копия системы работы Казанского аэропорта в условиях высочайшей загруженности во время проведения ЧМ. Посетителей аэропорта будем рассматривать как «заявки» на обслуживание, а транспорт доставки, металлорамки, пункты контроля и зоны сервиса, как «приборы», которые обрабатывают «заявки». Имитационная 3D модель Казанского Аэропорта представлена на Рисунке 2.

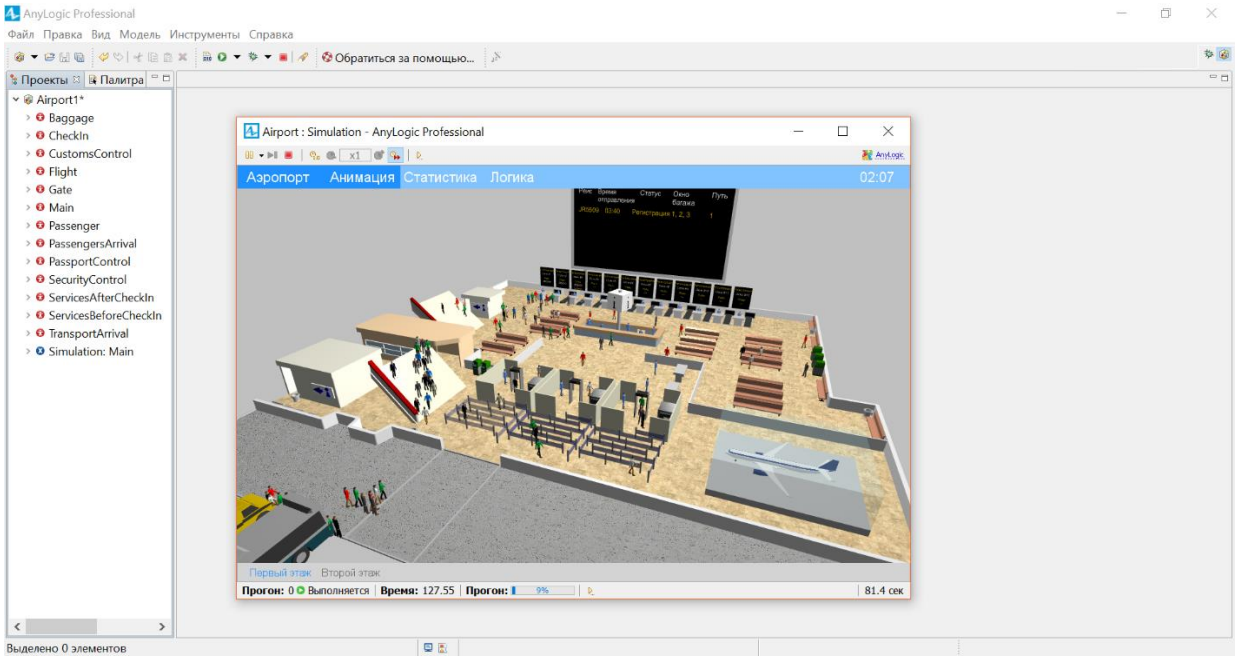

Рисунок 2. Имитационная 3D модель Казанского Аэропорта

В аэропорт посетители доставляются на четырех видах транспорта: личное авто, такси, пассажирский и туристический автобусы. До вылета они должны последовательно пройти через пять пунктов контроля: две металлические рамки безопасности, выборочную проверку содержимого багажа, окно регистрации, окно паспортного контроля и окно проверки билетов. [4]

4 Результаты

В ходе моделирования было определено, что поток заявок не однороден. Были отобраны результативные показатели эффективности работы аэропорта: среднее время досмотра посетителей на входе и вторичного досмотра посетителей, среднее время регистрации, паспортного контроля и контроля билетов, а также влияющие на них факторы: количество пунктов досмотра, количество окон регистрации и контроля билетов. [5]

Результаты моделирования представлены в Таблице 1. Пропускная способность определяет то, с какой скоростью система может обрабатывать заявки. В нашем случае, то, как быстро и качественно наш аэропорт справится с большим потоком посетителей. По результатам тестирования пропускная способность нашей модели недостаточно высока. Общее количество заявок – это общее количество посетителей аэропорта, из них обслужено было всего около 90%, и получено 10% отказов. [6] Эти посетители опоздали на свой рейс из-за очередей, либо не были пропущены каким-либо пунктом контроля.

Таблица 1. Результаты моделирования

№	Параметр	Значение
1	Пропускная способность	5,1104
2	Количество всех заявок в системе	7359
3	Количество обслуженных заявок	6578
4	Количество отказов	780
5	Вероятность отказа (%)	10,59
6	Общее время тестирования (мин.)	1440

5 Обсуждение

На Рисунке 3 представлена общая модель работы аэропорта. Каждому пункту контроля и регистрации соответствуют свои показатели загруженности. Загруженность более 50% говорит о длинных очередях и высокому времени обслуживания посетителя. Пункты входного и вторичного контроля, а также пункты паспортного контроля и контроля билетов не справляются со своей задачей, потому что их количество недостаточно для большого потока клиентов. [7] Во время проведения моделирования в проходах к данным пунктам досмотра и контроля были замечены очереди, превышающие средние значения по своей площади и плотности. Справились с нагрузкой и не вызвали длинных очередей только окна регистрации, которых было 12. Именно высокая многопоточность данного сегмента массового обслуживания аэропорта позволила удерживать средние показатели времени регистрации и не допускать высокого коэффициента простаивания «заявок». [8]

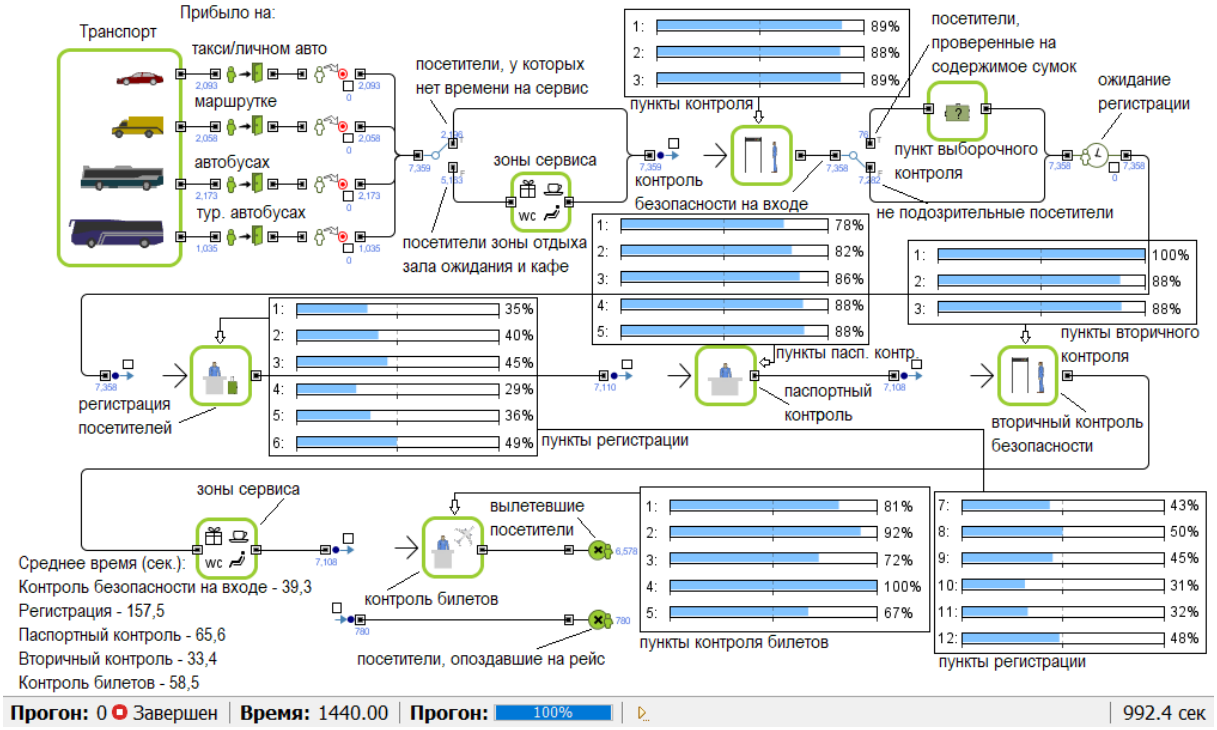

Рисунок 3. Модель работы аэропорта

6 Заключение

Из проведенного нами моделирования работы аэропорта мы можем сделать вывод, что для качественной работы аэропорта в условиях проведения ЧМ требуется увеличить количество металлорамок, окон паспортного контроля и контроля билетов. [9] Эти выводы могут помочь в будущем Красноярскому аэропорту подготовится к Универсиаде 2019 года. На их основе мы убедились, что имитационное моделирование позволяет точно отслеживать многие показатели эффективности работы аэропорта, проводить анализ этих показателей и, таким образом, выносить верное решение, касательно улучшения его работы. [10] Мы считаем, что в дальнейшем имитационное моделирование будет применяться все в более разнообразных сферах деятельности человека и значительно упростит его задачи в строительстве предприятий.

Список используемой литературы

[1] Мокшин В.В., Якимов И.М. Метод формирования модели анализа сложной системы. Информационные технологии, №5, 2011, С.46-51.

[2] Якимов И.М., Кирпичников А.П., Мокшин В.В. Сравнение систем структурного и имитационного моделирования по модели M/M/5. Вестник Казан. технол. ун-та, Казань, Т.20, №16, 2017, С.113.

[3] Боев В.Д. Исследование адекватности GPSS World и AnyLogic при моделировании дискретно-событийных процессов: Монография. ВАС, СПб, 2011, С.349-351.

[4] Кирпичников А.П. Методы прикладной теории массового обслуживания. Изд-во Казанского университета, Казань, 2011, С.194.
[5] Мезенцев К.Н. Моделирование в примерах и задачах в среде AnyLogic. LAP Lambert Academic Publishing, 2013, С.143.
[6] Девятков В.В. Имитационное моделирование: Учебное пособие. М.: КУРС, НИЦ ИНФРА-М, 2013, С.254-256.
[7] Лычкина Н.Н. Имитационное моделирование экономических процессов: Учебное пособие. М.: НИЦ ИНФРА-М, 2012, С.168.
[8] Чикуров Н.Г. Моделирование систем и процессов: Учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013, С.289.
[9] Харитонов С.В. Автоматизация оценки эффективности аэропортовой инфраструктуры. Синергия, 2014, С.115-121.
[10] Ярошевич Н.Ю. Консолидация аэропортовой отрасли: зарубежный опыт и российская практика. Синергия, 2012, С.15-17.

List of references

[1] Mokshin V.V., Yakimov I.M. Method of forming a complex system analysis model. Information technologies, No. 5, 2011, P.46-51.
[2] Yakimov I.M., Kirpichnikov A.P., Mokshin V.V. Comparison of structural and simulation systems for the model M / M / 5. Bulletin Kazan. tehnol. Un-one, Kazan, T.20, No. 16, 2017, P.113.
[3] Boyev V.D. Investigation of the adequacy of GPSS World and AnyLogic in the simulation of discrete-event processes: Monograph. YOU, St. Petersburg, 2011, P.349-351.
[4] Kirpichnikov A.P. Methods of applied queuing theory. Publishing house of Kazan University, Kazan, 2011, P.194.
[5] Mezentsev K.N. Modeling in examples and problems in the AnyLogic environment. LAP Lambert Academic Publishing, 2013, P.143.
[6] Devyatkov V.V. Simulation: Tutorial. M .: KURS, SIC INFRA-M, 2013, P.254-256.
[7] Lychkina N.N. Simulation modeling of economic processes: Tutorial. M .: SIC INFRA-M, 2012, P.168.
[8] N. Chikurov Modeling systems and processes: Tutorial. M .: ITs RIOR, SIC INFRA-M, 2013, P.289.
[9] Kharitonov S.V. Automate the assessment of airport infrastructure. Synergy, 2014, P.115-121.
[10] Yaroshevich N.Yu. Consolidation of the airport industry: international experience and Russian practice. Synergy, 2012, P.15-17.

РАЗРАБОТКА РОБОТОТЕХНИЧЕСКОЙ ПЛАТФОРМЫ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОГО РЕМОНТА ДОРОЖНОГО ПОЛОТНА

В.А. Рачис[1]
seva-ra4is@mail.ru

Э.И. Бейшенбаев[1]
erzaman_kg@mail.ru

Г.М. Медетова[1]
gaukhar_medetova@mail.ru

В.А. Галлингер[1]
Gallinger_Vladislav1916@mail.ru

Мыцко Е.А.[1]
ассистент ОИТ ТПУ
evgenvt@tpu.ru

[1] Национальный исследовательский Томский политехнический университет, Томск, 634050, Россия

Аннотация

Работа посвящена созданию робототехнического комплекса, способного к автоматизированному ремонту дорожного полотна, в частности ям. Робот должен быть автономным, однако нужно учесть возможность моментального перехвата управления

Abstract

The work is devoted to the creation of a robotic complex capable of automated repair of the roadway, in particular pits. The robot should be autonomous, but you need to take into account the possibility of instant interception of control

Ключевые слова: дороги, ремонт, автоматизация, выбоины, беспилотный транспорт.

Keywords: roads, repairs, automation, potholes, unmanned vehicles.

Ни для кого не секрет, что современное состояние российских дорог далеко не на высшем уровне. Данные «глобального рейтинга конкурентоспособности», в котором сравнивают 140 стран, свидетельствуют, что их рейтинг очень низкий. В период с 2009 по 2016 годы позиции таковы: 118, 125, 130, 136, 136, 124, 124, 123 [1,2].

Любая проблема приводит к последствиям. В данном случае самым опасным являются автомобильные аварии, в которых гибнут люди. Рассмотрим для примера статистику за первые 9 месяцев 2017 года. По данным ГИБДД 14000 из 133203 (10,5%) аварий произошли по причине низкого качества дорожного плотина. Также стоит отметить, что в ДТП умерло 16638 (1:8) и было ранено 168146 (10:8) человек [3]. Таким образом, если сделать грубый пересчёт, то можно получить, что ежегодно в России в авариях из-за плохого качества дорог умирают ~2500 человек, а получают ранения ~23500 человек.

Рассмотри причины плохих дорог [4,5,6]:

- Недостаточное финансирование
- Монополия в крупных городах
- Несоблюдение технологий
- Отсутствие системного контроля
- Ненормативные нагрузки на дороги
- Устаревшая нормативная документация
- Низкоквалифицированный персонал
- Отсутствие ремонта дорог
- Некачественное проектирование
- Коррупция в системе финансирования
- География страны
- Низкое качество строительных материалов

Техническими из них являются: отсутствие ремонта дорог и системного контроля. Эти проблемы можно решить путём автоматизации процесса контроля и ремонта дорожного полота. Также

при роботизации решаются проблема несоблюдения технологий и низкоквалифицированного персонала.

Рассмотрим технологии ремонта. Для того чтобы отремонтировать дорогу горячими смесями требуется [7]:

1. провести разметку
2. удалить небольшие выбоины при помощи отбойного молотка
3. удалить длинные и узкие выбоины больших трещин при помощи фрезы
4. полученную яму отчистить от мелких крошек, пыли компрессором
5. обработать стенки дна битумом

И лишь после этого можно приступать к ремонту. Бесспорно, такая технология более долговечная и не имеет ограничений по размеру ямы, однако явно видны недостатки: она занимает большое количество времени и сил, в том числе на подготовку, так как нужно привлекать большое количество техники и персонала.

Однако существует огромное количество ям менее 10х10 см², которые со временем постепенно расширяются. Для их ремонта в Европе и Америке уже давно используется струйно-инъекционный метод ямочного ремонта, однако в России он только начал применяться [8]. Рассмотрим алгоритм ремонта этим методом [9]:

1. Подготовка покрытия. Для подготовки покрытия к ремонту, ямы и трещины продувают. Затем необходимо обработать место проведения специальной эмульсией. Это улучшит сцепление заплатки с основным слоем.
2. Укладка щебня. Качество щебня должно соответствовать ГОСТ 8269.0-97 [10]. Используют очищенный щебень твердых горных пород примерно 5-10 мм. Использование более крупного приведет к снижению качества ремонта, в частности меньшей крепости отремонтированного участка. Перед укладкой щебень обрабатывают водно-бетонной эмульсией, после чего его высыпают и разравнивают.
3. Обработка эмульсией. Уложенный и уплотненный щебень тщательно пропитывают эмульсией так как в этом случае отремонтированное покрытие будет служить намного дольше.

Данный метод подходит для большого количества ситуаций, при этом он относительно просто реализуется. Также уже существуют некоторые наработки в данной области как в России, так и заграницей. Поэтому в качестве способа ремонта ям был выбран именно струйно-инъекционный метод, а не горячий асфальт. Решение проблем некачественного или полного отсутствия ремонта дороги, несоблюдения технологий, низко квалифицированный персонала, а также отсутствия системного контроля заключается в создании робототехнического комплекса способного к самостоятельному передвижения по городу, определению ям и их ремонту при помощи струйно-инъекционного метода. Такой робот должен обладать функциями:

- Подключение к серверу
- Перемещение по дороге
- Ориентирование в пространстве
- Нахождение ямы
- Очистка с помощью компрессора
- Сканирование ямы и составление карты глубины
- Засыпание ямы
- Уборка мусора за собой

Проект ожидает несколько основных этапов:

1. Поиск информации о проблеме, изучение способов её решение, включая анализ технологий, аналогов и их недостатков
2. Разработка концептуального прототипа, суть которого в базовой демонстрации технологии. Предполагается небольшой размер, а поиск ямы основан на маркерах (изначально ямы на дороге обведены красной линей). Этот прототип предназначен для демонстрации идеи разработки
3. После презентации концептуального прототипа требуется найти финансирование (грант, приз) на выполнение следующего этапа
4. Создание лабораторного прототипа, в течении создания которого будут проработаны более мелкие проблемы, кроме этого будут созданы более сложные алгоритма поиска. Размер робота примерно 1000x500x500 мм3, а видеоданные будут получены со специальной камеры, выдающей готовую карту глубины, например, Kinect или Intel RealSense.
5. После презентации лабораторного прототипа требуется найти стратегического партнёра, который не только обеспечит проект финансированием, но и поможет с выходом на рынок
6. Изготовление промышленный прототип, то есть окончательного варианта. Размер полномасштабный, алгоритмы поиска основываются на изображении с камер

На данный момент проект лабораторного прототипа завершён примерно на 25-30%. Уже были завершены следующие стадии:

- Проектирование каркаса робота
- Выбор деталей
- Изготовление некоторые основные и все вспомогательных элементы (рис. 3-
- Освоение среды программирования
- Написан алгоритм поиска ямы
- Передача данных в локальной сети
- Создание 3D модели (рис. 1-2)

Также некоторые задачи находятся в стадии разработки:

- Изготовление основных деталей
- Управление электроникой
- Алгоритм поиска знаков

Предстоит сделать:

- Программирование алгоритма поиска светофора
- Написание связующего алгоритма для робота
- Тестирование

Рис. 1. 3D модель основной версии

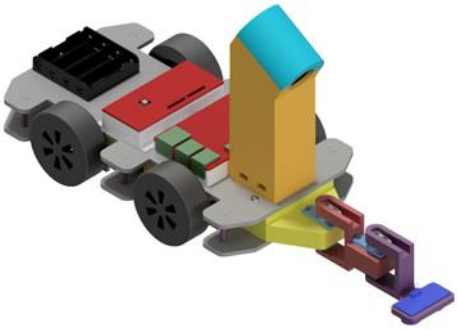

Рис. 2. 3D модель портативной версии

Программирование

Составлены алгоритмы робота, а также были написаны программы для:

- Поиска ямы при помощи камеры глубины на Kinect 2.0 (рис. 3)

Рис. 3. Поиск ям по карте глубины (нижняя левая)

- Поиска дорожных знаков по цветному изображению с камеры (рис. 4)

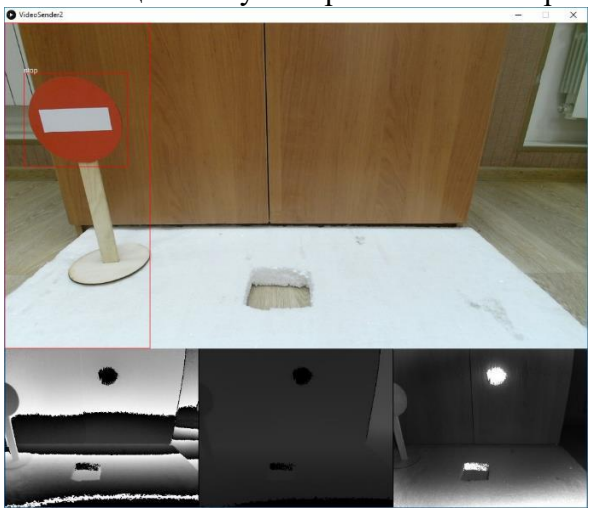

Рис. 4. Поиск дорожного знака по цветной картинке

- Поиск светофора и определение его сигналов (рис. 5)

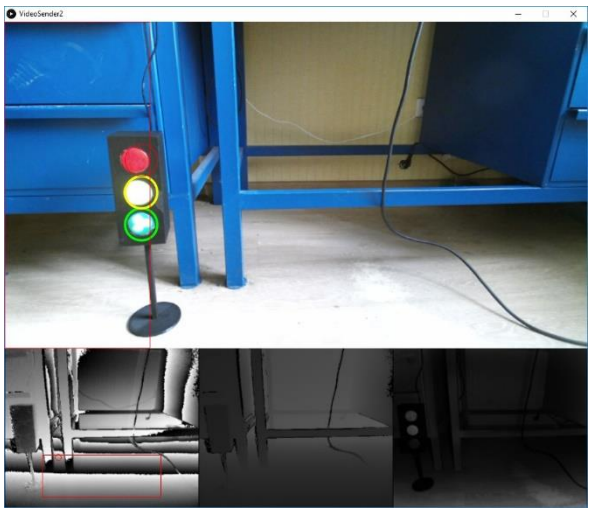

Рис. 5. Поиск светофора и определение его сигналов (красный выключен, остальные включены)

- Просчёта углов для позиционирования манипулятора «стрела»

Также реализованы программные модули передачи данных между роботом и пользователем:

- Видео с камеры при помощи UDP протокола
- Общение сервера с клиентом через TCP

Список используемой литературы

[1] Российские дороги заняли 123-е место в мировом рейтинге // Известия URL: https://iz.ru/news/598884 (дата обращения: 25.12.2017).

[2] Рейтинг качества дорог России // Автомобильные дороги URL: http://tomnosti.info/dorogi-kak-i-pochemu-2/reyting-kachestva-dorog-rossii.phtml (дата обращения: 25.12.2017).

[3] СТАТИСТИКА АВТОКАТАСТРОФ ЗА 2017 ГОД В РОССИИ // PROVodim24 URL: http://provodim24.ru/statistika-dtp.html (дата обращения: 25.12.2017).

[4] 10 причин, почему в России плохие дороги // VARLAMOV.RU URL: https://varlamov.ru/1256164.html (дата обращения: 25.12.2017).

[5] Учёные рассказали, почему в России плохие дороги // DRIVE2 URL: https://www.drive2.ru/c/298786/ (дата обращения: 25.12.2017).

[6] Почему в России плохие дороги? // pikabu URL: https://pikabu.ru/story/pochemu_v_rossii_plokhie_dorogi_2849813 (дата обращения: 25.12.2017).

[7] Какими способами выполняется ямочный ремонт дорог // НерудБКС URL: http://neruds.ru/staty/asfalt11.html (дата обращения: 25.12.2017).

[8] Струйно инъекционный метод ямочного ремонта // Компания СТК СтройИнвест URL: http://drimstroy.ru/stati-o-stroitelstve/dorog/29-struyno-inekcionnyy-metod-yamochnogo-remonta.html (дата обращения: 25.12.2017).

[9] Ямочный ремонт по струйно-инъекционной технологии // RoadMasters.ru URL: http://roadmasters.ru/remont-dorogi/yamochnyj/yamochnyj-remont-po-strujno-inekcionnoj-tehnologii.html (дата обращения: 25.12.2017).

[10] ЩЕБЕНЬ И ГРАВИЙ ИЗ ПЛОТНЫХ ГОРНЫХ ПОРОД И ОТХОДОВ // Портал ВАШ ДОМ - всё для строительства и ремонта URL: http://www.vashdom.ru/gost/8269.0-97/ (дата обращения: 25.12.2017).

List of references

[1] The Russian roads took the 123rd place in the world ranking//URL News: https://iz.ru/news/598884 (date of the address: 25.12.2017).

[2] Rating of quality of roads of Russia//Highways URL: http://tomnosti.info/dorogi-kak-i-pochemu-2/reyting-kachestva-dorog-rossii.phtml (date of the address: 25.12.2017).

[3] STATISTICS of ROAD ACCIDENTS FOR 2017 IN RUSSIA//PROVodim24 URL: http://provodim24.ru/statistika-dtp.html (date of the address: 25.12.2017).

[4] 10 reasons, why in Russia bad roads//VARLAMOV.RU URL: https://varlamov.ru/1256164.html (date of the address: 25.12.2017).

[5]Scientists told why in Russia bad roads//DRIVE2 URL: https://www.drive2.ru/c/298786/(date of the address: 25.12.2017).

[6]Why in Russia bad roads?//pikabu URL: https://pikabu.ru/story/pochemu_v_rossii_plokhie_dorogi_2849813 (date of the address: 25.12.2017).
[7]What ways carry out patching of roads//Nerudbks of URL: http://neruds.ru/staty/asfalt11.html (date of the address: 25.12.2017).
[8]Struyno injection method of patching//URL STK Stroyinvest Company: http://drimstroy.ru/stati-o-stroitelstve/dorog/29-struyno-inekcionnyy-metod-yamochnogo-remonta.html (date of the address: 25.12.2017).
[9]Patching on jet and injection technology//RoadMasters.ru URL: http://roadmasters.ru/remont-dorogi/yamochnyj/yamochnyj-remont-po-strujno-inekcionnoj-tehnologii.html (date of the address: 25.12.2017).
[10] CRUSHED STONE AND GRAVEL FROM DENSE ROCKS AND WASTE//the DOM YOUR Portal - all for construction and repair of URL: http://www.vashdom.ru/gost/8269.0-97/(date of the address: 25.12.2017).

АНАЛИЗ ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Операйло К.В.[1]
gladesinger18@gmail.com

Якимов М.А.[1]
maik3786@gmail.com

Новикова Е.Н.[1]
кандидат физико-математических наук, доцент
novikovaelena_nik@mail.ru

[1] Северо-Кавказский Федеральный Университет, Ставрополь, 355028, Российская Федерация

Аннотация

В данной статье проводится анализ перспектив развития искусственного интеллекта. Само понятие искусственного интеллекта подразумевает обучение машины творческим функциям, которые традиционно считаются прерогативой человека. Таким образом, искусственный интеллект призван симулировать часть мыслительного процесса человека при решении отдельно взятой задачи. Значение искусственного интеллекта, а также его потенциал, сложно переоценить. С каждым годом он затрагивает все больше областей, и продолжает захватывать все новые и новые области. Широкое развитие искусственного интеллекта, приводит к совершенствованию старых и появлению новых подходов и направлений. Он стал своеобразным научным фронтиром, ждущим своих покорителей. Как и любая научная дисциплина, вопрос искусственного интеллекта требует тщательного изучения. Поэтому так важно анализировать направления развития данной сферы, а также, пусть и приблизительно, предположить их актуальность.

В статье представлены материалы из различных источников и исследований, позволяющие проанализировать развивающиеся направления в области искусственного интеллекта, а также приведены определения ключевых понятий, их сравнительный анализ и потенциал развития

области искусственного интеллекта в целом, и отдельных его направлений в частности.

Abstract

This article analyzes the prospects for the development of artificial intelligence. The concept of artificial intelligence involves learning machines creative functions that are traditionally considered the prerogative of man. Thus, AI is designed to simulate a part of the human thought process when solving a single task. The value of artificial intelligence, as well as its potential is difficult to overestimate. Every year it affects more and more areas, and continues to capture more and more new areas. The wide development of artificial intelligence leads to the improvement of old and the emergence of new approaches and directions. AI has become a kind of scientific frontier, waiting for their explorers. As with any scientific discipline, the question of artificial intelligence requires careful study. Therefore, it is important to analyze the directions of development of this sphere, and also, even if approximately, to assume their relevance.

The article presents materials from various sources and studies that allow to analyze the developing areas in the field of artificial intelligence, as well as provide definitions of key concepts, their comparative analysis and the potential for the development of the field of artificial intelligence in general, and its individual areas in particular.

Ключевые слова: искусственный интеллект, вычислительные машины, нейронные сети, машинное обучение, глубокое обучение, компьютерное зрение, перспективы развития.

Keywords: artificial intelligence, computers, neural networks, machine learning, deep learning, computer vision, development prospects.

Введение

Искусственный интеллект (далее – ИИ) – это область наук, посвященных созданию вычислительных машин и систем на основе работы человеческого мозга, выполняющие аналогичные операции принятия решений и способные к обучению [1]. В любой конкретной реализации ИИ может сильно различаться, и термин не подразумевает работу на уровне человека.

Искусственный интеллект включает множество функциональных возможностей, таких как [2]:

- Обучение, которое включает в себя такие подходы как: глубокое обучение (deep learning), перенос обучения (transfer learning), обучение с подкреплением (reinforcement learning) и их сочетания.
- Понимание или представление глубоких знаний по предметной области, к примеру: кардиологии, бухгалтерского учета;
- Взаимодействия людей с машиной для выполнения поставленных задач и изучения окружения.

Идеи о создании «мыслящих машин» беспокоили умы еще с самой зари эры компьютеризации, которая началась после Второй Мировой Войны, однако, до осуществления этих дерзких планов было еще далеко. Первая конференция по ИИ была проведена в колледже Дартмута в 1956 году – предполагалось, что искусственный интеллект можно будет создать за одно лето интенсивных исследований. В 1960-ых и 1970-ых ученые предсказывали, что уже через десятилетие мы увидим машины, способные мыслить как люди [9]. В 1965, нобелевский лауреат Герберт Саймон предсказал, что «через двадцать лет машины будут способны выполнять любую человеческую работу». Нет нужды говорить, что время было несколько недооценено – более того, подобное положение дел сохраняется и по сей день. Однако в последние годы исследования ИИ сделали шаг вперед за счет разработки машинного обучения – ветви, фокусирующейся на разработке алгоритмов, способных на повторное автоматическое построение аналитических моделей из новых данных без подробных программных решений.

1 Постановка задачи

Из-за стремительного развития информационных технологий в целом и искусственного интеллекта в частности, в данной сфере появилось множество различных направлений. Для определения перспектив использования и внедрения ИИ в различные сферы жизни, необходимо произвести сравнительный анализ. Выявление самых перспективных направлений искусственного интеллекта призвано помочь как людям, решившим приспособить искусственный интеллект в том или ином виде для своих задач, так и специалистам, развивающимся в данной области.

2 Разработка методики

Рассмотрим типологию приложений, использующих искусственный интеллект. Подобных приложений масса, интеллектуальные алгоритмы используются практически везде, начиная с приложений для смартфонов, помогающих покупателям оформлять покупки, заканчивая моделями, ускоряющими поиск новых лекарств. В большинстве своем, применение ИИ выполняет хотя бы одну из семи функций [3]:

1. наблюдения;
2. открытия;
3. прогнозирования;
4. интерпретации;
5. взаимодействия с окружающей средой;
6. взаимодействия с человеком;
7. взаимодействия с машиной.

В соответствии с этими функциями, приложения, основанные на ИИ, принято классифицировать на:

- Приложения мониторинга. В таких приложениях ИИ быстро анализирует большое количество данных, устанавливая аномалии и закономерности. Из-за большей производительности ИИ в подобных вопросах (относительно людей), он очень хорошо подходит для использования в мониторинговых приложениях, таких как валютные операции, кибербезопасность, определение ранних признаков заболевания или важных изменений окружающей среды [4].
- Приложения открытия. В этом случае ИИ может получать довольно значимые детали из больших объемов данных – процесс, так же известный как data mining, и открывать новые решения через симуляции. В частности, из-за того, что ИИ использует обучающиеся и адаптирующиеся благодаря данным модели, он становится очень полезным в открытии абстрактных паттернов.
- Приложения прогнозирования. Эти приложения выполняют моделирование и прогнозирование возможных трендов в будущем. Один из наиболее популярных типов приложений, используемый, например, в рекомендациях на популярных стриминговых платформах и видеохостингах (Netflix, YouTube), анализирующих историю просмотров пользователей и строящих на их основе рекомендации [4].
- Приложения интерпретации. До недавнего времени, аналитика данных по большому счету работала лишь со структурированными данными – хорошо организованной информацией. Но из-за возможности ИИ изучать и определять закономерности, он может анализировать и неструктурированные данные – изображения, видео, аудио, текст. В результате, мобильные и настольные приложения теперь способны определять голосовые команды пользователей, а диагностические приложения способны анализировать рентгеновские снимки для нахождения аневризм.
- Приложения взаимодействия с окружающей средой – возможность использования ИИ для управления сенсорами, камерами, система GPS-навигации и др.

- Приложения взаимодействия с людьми. В узком смысле включают в себя приложения, способные имитировать базовые черты человеческого общения, к которым относятся различные чат-боты.
- Приложения взаимодействия с машинами – налаживание взаимодействия между двумя ранее не связанными устройствами.

В исследованиях искусственного интеллекта очень важно понятие машинного обучения. Машинное обучение представляет собой класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач [9]. Для построения таких методов используются средства математической статистики, численных методов, методов оптимизации, теории вероятностей, теории графов, а также различные техники работы с данными в цифровой форме.

Не менее важным является определение глубокого обучения.

Глубокое обучение – совокупность методов машинного обучения, основанных на обучении представлениям (feature/representation learning), а не специализированным алгоритмам под конкретные задачи [4]. Многие методы глубокого обучения были известны ещё в 1980-е годы, но результаты были невпечатляющими, пока продвижения в теории искусственных нейронных сетей и вычислительные мощности середины 2000-х (прежде всего, графических процессоров Nvidia, а в настоящее время и тензорных процессоров Google) не позволили создавать сложные технологические архитектуры нейронных сетей, обладающие достаточной производительностью и позволяющие решать широкий спектр задач, не поддававшихся эффективному решению ранее, например, в компьютерном зрении, машинном переводе, распознавании речи, причём качество решения во многих случаях теперь сопоставимо, а в некоторых случаях и превосходит эффективность человеческих экспертов [10].

3 Результаты исследования

По результатам опросов, проведенных Беном Лориком и Майклом Лукидесом, и опубликованных ими в статье «Как компании внедряют ИИ через глубокое обучение», одной из главных причин, удерживающих компании от использования технологий глубокого обучения является недостаток людей с достаточным уровнем навыков. Примерно 20% опрошенных заявили, что разница в навыках является одной из причин по задержке внедрения подобных технологий, также 75% опрошенных указали, что проводят необходимые тренировочные программы для решения данного вопроса [6].

Нами были продолжены исследования в областях знаний, соотносящихся с производством ИИ-основанных продуктов и систем, особенно те области, которые требуют развития навыков. В этой статье представлены результаты проведенных исследований. Данные были получены из нескольких источников:

- популярной зарубежной платформы онлайн-обучения O’Reilly, которая показывает приоритетные направления для специалистов;
- отчетов о рынке искусственного интеллекта с сайта Venture Scanner, позволяющие проанализировать важные направления ИИ для крупных компаний (более 2000 компаний);
- проведенных с помощью онлайн-сервисов опросов о перспективных направлениях развития искусственного интеллекта.

Результаты анализа в процентном соотношении приведены на рисунке 1.

Рисунок 1 – График востребованных направлений ИИ

Важнейшим направлением в области искусственного интеллекта является машинное обучение и нейронные сети. Это направление можно по праву считать самым перспективным. В результате опросов, машинное обучение и нейронные сети выбрали более 24% корреспондентов. Следовательно, это направление является перспективным как для компаний, так и для специалистов.

Также стоит отметить, что согласно платформе O’Reilly за 2018 год был замечен сильный рост интереса ко множеству тем, связанных с ИИ и машинным обучением [5]. График ниже (рисунок 2) дает приблизительное представление о том, какое количество контента предоставлено по ключевым темам, особенно по машинному обучению и глубокому обучению.

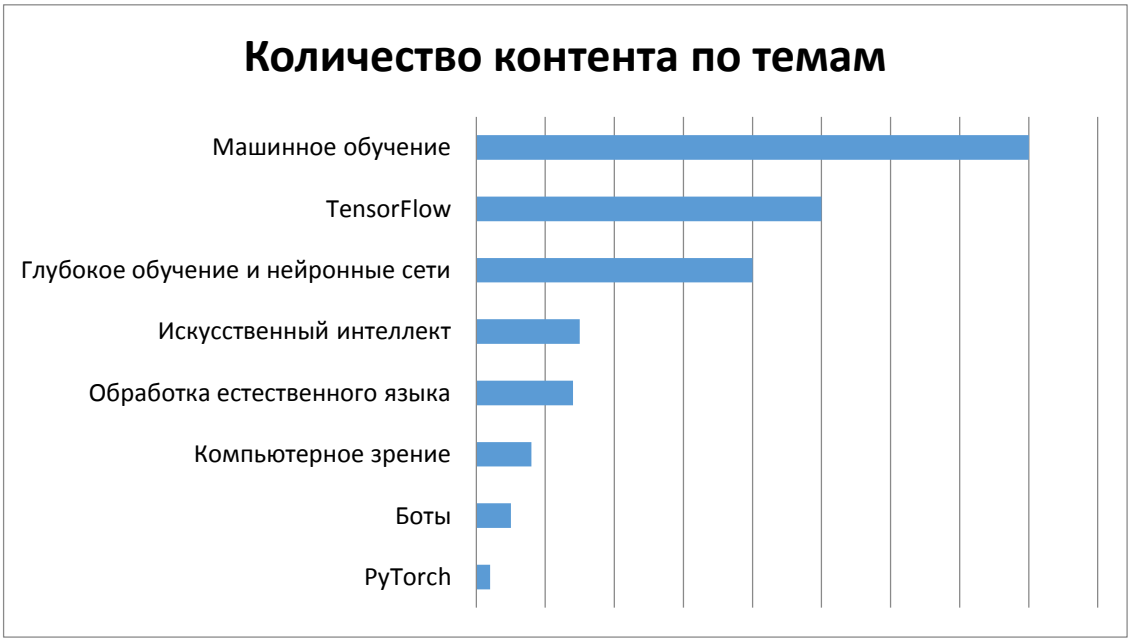

Рисунок 2 – График возросшего интереса к темам, связанным с ИИ

Можно увидеть большой интерес к машинному обучению, а также к библиотекам для машинного обучения TensorFlow от Google и PyTorch. Также специалистов интересуют способы обработки естественного языка, компьютерное зрение и создание ботов.

Машинное обучение представляет собой одно из самых наиболее быстро растущих направления для поиска за последний год. В качестве доказательства можно привести результаты анализа поисковых запросов на платформе O'Reilly за 2017 и 2018 годы, которые представлены на рисунке 3.

Запрос	Позиция 2018	Изменение относительно 2017
Python	1	-
Java	2	-
Aws	3	3
Kubernetes	4	15
Машинное обучение	5	2
Docker	6	-2
Angular	7	-4

Рисунок 3 – Статистика запросов

В общем, видна тенденция к росту популярности искусственного интеллекта и машинного обучения, но какие вопросы беспокоят производителей и потребителей в вопросах использования приложений, основанных на ИИ?

Среди ведущих инвесторов растет осведомленность о важности таких направлений, как безопасность данных, этика и тайна личности. Пользователи же начинают интересоваться вопросами прозрачности и контролем над их данными [7]. Результаты опросов пользователей и работников компаний приведены на рисунке 4.

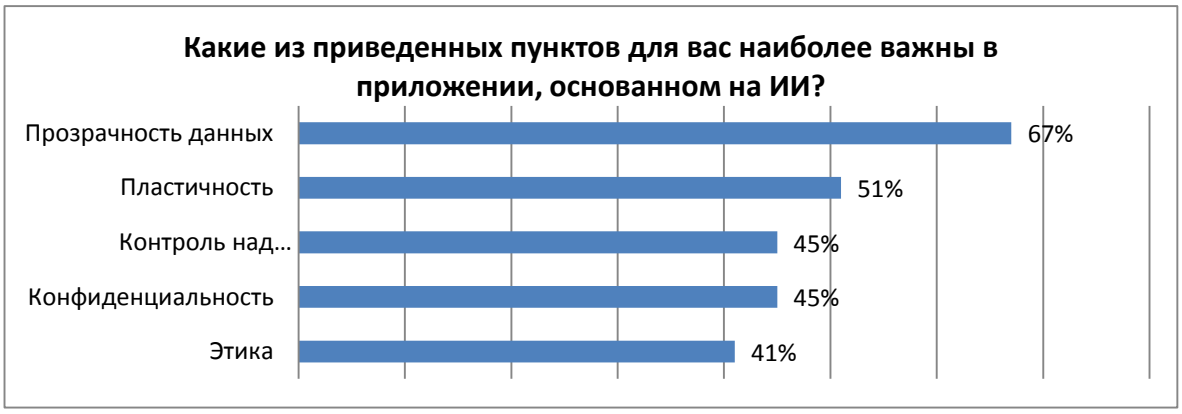

Рисунок 4 – Результаты опросов работников компаний и пользователей

Подобные результаты неудивительны, с ростом использования технологий машинного обучения вопрос безопасности данных встал как никогда остро.

К примеру, опросы, проведенные в США, Великобритании и Германии показывают, что 75%, 57% и 55% респондентов соответственно считают, что хакерские атаки увеличатся, как только злоумышленники начнут использовать технологии ИИ (рисунок 5).

Однако проблема возникает не только в связи с хакерскими атаками, многие пользователи обеспокоены отсутствием у ИИ этики и, как следствие, потенциалом использования систем, основанных на искусственном интеллекте для дискриминации некоторых групп населения [8]. Так, опросы в США показали, что около 57% населения думают, что системы, основанные на ИИ будут так или иначе ущемлять права людей.

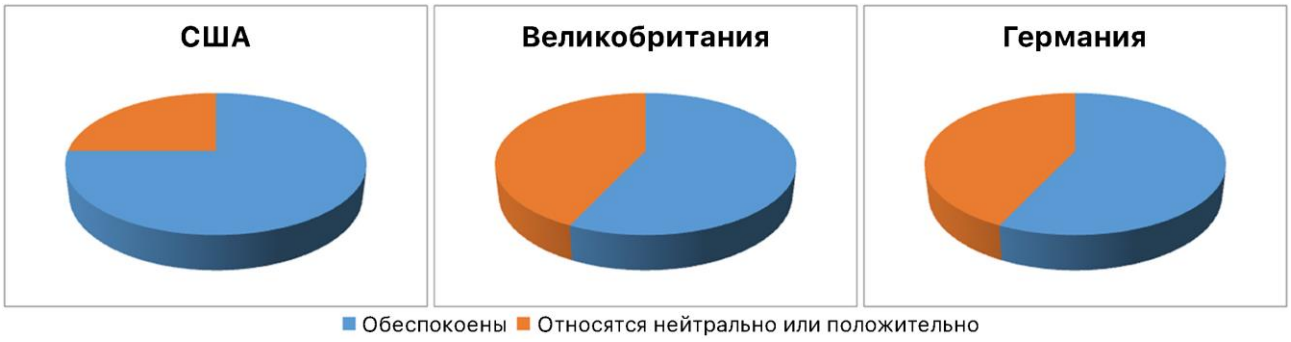

Рисунок 5 – Диаграммы, иллюстрирующие увеличение обеспокоенности хакерскими атаками в связи с развитием ИИ

4 Обсуждение

В ходе исследования было выяснено, что наибольший интерес для специалистов и работодателей представляют вопросы машинного обучения, глубокого обучения и

нейронных сетей. Рост интереса к этой теме в последнее время можно объяснить все большим и большим охватом области применения и, как следствие, растущим спросом на рынке труда.

С ростом использования ИИ и нейронных сетей, растет так же обеспокоенность населения относительно безопасности их данных. К сожалению, подобное беспокойство может быть также связано с низкой осведомленностью населения – так, к примеру, 47% опрошенных не видят разницы между понятиями Искусственный Интеллект и Машинное Обучение. Подобные ошибки связаны в первую очередь с медиа-источниками, часто путающими или искажающими данные определения. Однако, степень развития ИИ еще не находится на достаточном уровне для полной передачи ему управления безопасностью данных, а значит, беспокойство пока не обоснованно.

Заключение

В ходе проведенных исследований были выявлены перспективные направления развития искусственного интеллекта как для специалистов, желающих развиваться в этой области, так и для крупных компаний, желающих внедрить ИИ на своих предприятиях. Анализ направлений показал, что самым востребованным является направление машинного обучения. Самыми популярными направлениями, связанными с обучением, являются: глубокое обучение, нейронные сети, различные библиотеки для создания обучающихся систем. Наряду с этим, увеличивается интерес к направлениям, связанным с распознаванием, таким как: компьютерное зрение, обработка естественного языка, распознавание голоса.

В общем, прослеживается тенденция к увеличению интереса ко всем основным направлениям искусственного интеллекта за последний год, но самыми перспективными в ближайшее время останутся направления машинного обучения.

Список используемой литературы

[1] [Электронный ресурс] Потенциал Искусственного Интеллекта // Data innovation URL: http://www2.datainnovation.org/2016-promise-of-ai.pdf. (На английском языке)

[2] Бостром Н. Искусственный интеллект: Этапы, угрозы, стратегии // Н. Бостром - Оксфорд: Пресса университета Оксфорда, 2015. – 496 с. (На английском языке)

[3] Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных // П. Флах -ЛитРес, 2015 – 402с. (На английском языке)

[4] Шолле Ф. Глубокое обучение на Python // Ф. Шолле -Скб: Издательский дом «Питер», 2018 – 400с.

[5] [Электронный ресурс] O’Reilly Media – Технологии и бизнес // URL: https://www.oreilly.com. (На английском языке)

[6] [Электронный ресурс] Как компании внедряют ИИ через глубокое обучение // O'reilly URL: https://www.oreilly.com/data/free/how-companies-are-putting-aI-to-work-through-deep-learning.csp (На английском языке)

[7] [Электронный ресурс] Стартап: Как ИИ меняет киберзащиту // URL: https://medium.com/swlh/how-artificial-intelligence-is-changing-cyber-security-a243294ccdfe (На английском языке)
[8] [Электронный ресурс] Вычисления: Искусственный интеллект – не серебряная пуля для киберзащиты // URL: https://www.computing.co.uk/ctg/news/3037214/artificial-intelligence-is-not-a-silver-bullet-for-cyber-security. (На английском языке)
[9] [Электронный ресурс] Как искусственный интеллект меняет мир // Brookings URL: https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world. (На английском языке)
[10] [Электронный ресурс] «Мягкий» искусственный интеллект внезапно повсюду // The wall street journal URL: https://blogs.wsj.com/cio/2015/01/16/soft-artificial-intelligence-is-suddenly-everywhere. (На английском языке)

List of references

[1] [Internet Source] Castro D., New J. The Promise of Artificial Intelligence // Data innovation URL: http://www2.datainnovation.org/2016-promise-of-ai.pdf.
[2] Bostrom N. AI: Superintelligence: Paths, Dangers, Strategies // N. Bostrom –Oxford: Oxford University Press, 2015, 496 p.
[3] Flach P. Machine learning The Art and Science of algorithms that make sense of data // Cambridge University Press, 2015, 399p.
[4] Chollet F. Deep learning with Python // F. Chollet Manning Publications – 2017, 384 p. (In Russian)
[5] [Internet Source] O'Reilly Media – Technology and Business Training // URL: https://www.oreilly.com/
[6] [Internet Source] How companies are putting AI to work through deep learning // O'reilly URL: https://www.oreilly.com/data/free/how-companies-are-putting-aI-to-work-through-deep-learning.csp
[7] [Internet Source] The Startup: How Artificial Intelligence is Changing Cyber Security // URL: https://medium.com/swlh/how-artificial-intelligence-is-changing-cyber-security-a243294ccdfe
[8] [Internet Source] Computing: Artificial intelligence is not a silver bullet for cyber security // URL: https://www.computing.co.uk/ctg/news/3037214/artificial-intelligence-is-not-a-silver-bullet-for-cyber-security
[9] [Электронный ресурс] How artificial intelligence is transforming the world // Brookings URL: https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world.
[10] [Электронный ресурс] «Soft» Artificial intelligence is suddenly everywhere // The wall street journal URL: https://blogs.wsj.com/cio/2015/01/16/soft-artificial-intelligence-is-suddenly-everywhere.

Актуальность внедрения робототехники в образовательный процесс

Савенко Е. В.
Ставропольский Государственный Педагогический Институт,
г. Ставрополь, 355000, Российская Федерация,
savenko2266@mail.ru

Оленев А. А.
Ставропольский Государственный Педагогический Институт,
г. Ставрополь, 355000, Российская Федерация,
Кандидат технических наук, доцент кафедры математики и информатики,
olenevalexandr@gmail.com

Аннотация: Данная статья посвящена выявлению влияния робототехники на различные аспекты жизни человека, в том числе и образовательный процесс. В статье рассматриваются взаимосвязи робототехники с предметным содержанием информатики, физики и других естественнонаучных дисциплин. На основе применения различных робототехнических комплектов показан пример влияния робототехники на образовательный процесс по информатике, с решением вопросов развития коммуникативных навыков учащихся и их профессионального самоопределения. В связи с быстро идущим процессом информатизации в современном обществе внедрение робототехники и смежных с ней дисциплин в образовательный процесс становится как никогда актуальным. Ведь внедрение технологий в учебный процесс

способствует формированию личностных, регулятивных и познавательных универсальных учебных действий, являющихся важной составляющей ФГОС[1]. Также в статье рассматривается еще один из наиболее важных аспектов образовательной робототехники, дающий возможность выявления на ранних этапах обучения технических наклонностей обучающихся. Обсуждаются различные робототехнические конструкторы, которые могут быть использованы в образовательном процессе при изучении робототехники у разных возрастных групп школьников. Робототехника – это объект изучения, инструмент познания и средство обучения, развития и воспитания учащихся.

Ключевые слова: Информатизация, технологии, робототехника, конструирование, образовательный процесс, изучение, обучение, самоопределение.

Abstract: This article is devoted to identifying the impact of robotics on various aspects of human life, including the educational process. The article discusses the relationship of robotics with the subject content of computer science, physics and other natural sciences. Based on the use of various robotic kits, an example of the influence of robotics on the educational process in computer science is shown, with the solution of the issues of developing the communicative skills of students and their professional self-determination. In

connection with the fast-paced process of informatization in modern society, the introduction of robotics and related disciplines in the educational process becomes more relevant than ever. Indeed, the introduction of technology into the educational process contributes to the formation of personal, regulatory and cognitive universal educational activities, which are an important component of the FGOS[1]. The article also discusses another one of the most important aspects of educational robotics, which makes it possible to identify the technical inclinations of students in the early stages of training. Various robotic designers are discussed, which can be used in the educational process when studying robotics in different age groups of schoolchildren. Robotics is an object of study, a tool of knowledge and a means of teaching, developing and educating students.

Keywords: Informatization, technologies, robotics, design, educational process, study, training, self-determination.

Различные изменения в современном мире происходят так стремительно, что уследить за всеми становится просто невозможно.

Большая часть изменений в наш век цифровых технологий связана:

- С заменой человеческих ресурсов машинами (роботами);
- Появлением «умных» технологических новшеств, призванных облегчить жизнь и деятельность человека;
- Доступностью и открытостью информационных ресурсов.

Так, в процессе развития информатики, как прикладной науки, появились различные подходы к программированию, включая программирование

роботов.Роботами являются различные автоматические устройства, выполняющие определенную, заложенную в них операцию или же их набор.

Уже сейчас можно четко проследить различную направленность роботов по виду их деятельности: промышленные, военные (беспилотники и пр.), бытовые (робот пылесос, «умный» дом), медицинские, транспортные и другие [2].

Робототехника на сегодняшний день является одним из важнейших направлений в научно-техническом прогрессе, а также вносит не малый вклад в развитие образовательной системы.

В школы сейчас активно вводятся дополнительные часы по изучению робототехники. И если дети интересуются данной сферой с раннего возраста, то они смогут открыть для себя много нового в области конструирования роботов в дальнейшем [3].

Знания данной области открывают перед сегодняшними школьниками новые профессии в технической сфере. Так, популярным становится новое направление в ИТ-сфере – роботизированные технологические комплексы, позволяющие автоматизировать отдельные технологические операции[4].

Раннее знакомство школьника с основами конструирования роботов позволит ему легче сориентироваться профессионально.

Современные дети привыкли к вещам, воспринимаемым быстро и понятно. Сейчас дети быстро могут понять принципы работы смартфона, разобраться с интерфейсом новой, ранее незнакомой им программы. Следовательно, образовательный процесс для них должен проходить так же быстро и наглядно [5].

Раньше такие методы представлялись плохо, и уж тем более не осуществлялись. Но с появлением компьютерных технологий многое изменилось. Сейчас они могут быть встроены в робототехнические наборы, и образовался еще один инструмент для образовательных целей. При использовании данных наборов становится доступным создание практически любого наглядного пособия, оборудования для исследований или проектов.

Конструирование позволяет формировать и развивать у детей абстрактное мышление [6].

Так, например, векторное прямолинейное движение может быть проиллюстрировано учителем на примере запрограммированного движения робота.

Возвращаясь к информатике можно добавить, что робототехника в ней показывает наибольший потенциал – это и развитие алгоритмического, модельного мышления, и изучение детьми основ программирования и многое другое.

Представление учащимися собственных исследовательских проектов поможет им развить свои коммуникативные навыки, а сами проведенные исследования научат их понимать важность открытий, как старых, так и новых.

Все, о чем было сказано, - устройства, исследовательские работы и реквизит для них, - подготавливается и организовывается самими детьми, исходя из их собственного интереса. Учитель выступает лишь наставников в достижении поставленных целей, а школа – тем местом, где ребенок получает знания и навыки, в дальнейшем применяя их в жизни.

Самым важным вопросом в начале изучения робототехники является выбор робототехнического комплекта, при использовании которого и будут проводиться занятия. Именно он и является основой начала образовательной деятельности в робототехнике. К главным критериям выбора такого набора стоит отнести [7]:

- Разнообразие методических возможностей;
- Продолжительность использования;
- Количество учеников, работающих единовременно с этим набором.

Основное оборудование, которое применяется при изучении робототехники на ранних этапах, это наборы LEGO, в частности – LEGO MindStorms Education EV3 [8].

В основном эти наборы предназначены для групповой работы, что позволяет детям учиться на собственном опыте и раскрывать свой творческий потенциал, а также развивать коммуникативные и лидерские навыки.

Стоит говорить о том, что наборы LEGO являются достаточными лишь на начальных этапах изучения робототехники. Из-за своей структуры они быстро приходят в негодность, а отдельные детали конструктора просто изнашиваются в процессе занятий.

Более лучшим вариантом использования являются наборы «jimu от компании Ubtech. Помимо низкой стоимости, они обладают также хорошим качеством отдельных деталей набора, и более долговечны в целом.

В отличие от наборов LEGO, Jimu позволяет детям не только изучать основы конструирования роботов, но и дает возможность углубиться в изучение их программной составляющей.

Так, например, работая с роботом Jimu, учащиеся могут впоследствии задавать ему собственноручно написанные действия, или даже программу действий.

Программирование роботов Jimu происходит на визуальном языке программирования Google Blockly.

Данный язык позволяет писать программы без изучения правил синтаксиса, что, несомненно, подойдет для начального этапа изучения программирования [9].

В Blocky, чтобы задать программу действий для робота, достаточно соединять визуальные блоки друг с другом в соответствии с их формой. Это чем-то напоминает пазлы (рис. 1) [10].

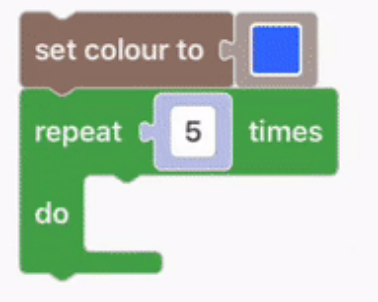

Рисунок 1. Соединение блоков.

Как уже говорилось раннее, по форме блоков можно понять, как они будут соединяться с другими. Если один блок является «Блоком задания условия», то в него можно поместить «Блок действия», тем самым расширив его (рис. 2).

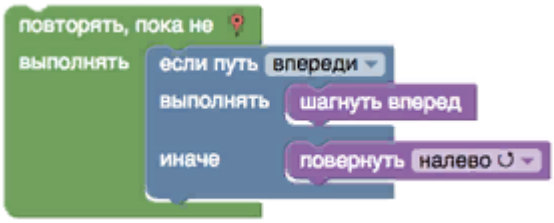

Рисунок 2. Расширение блоков.

Все шаги в Blockly выполняются последовательно, а текущее действие подсвечивается, тем самым позволяя выявить ошибку в написании программы и исправить ее (рис. 3).

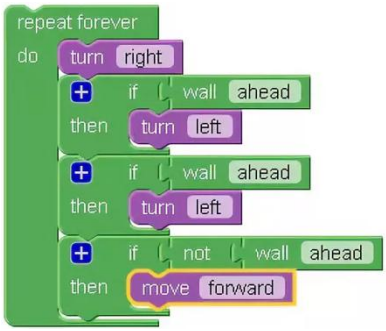

Рисунок 3. Выделение выполняемого блока.

Единственным исключением при внедрении Blockly в робототехнику является соблюдение правил изменения угла конкретного сервопривода. При неправильном задании изменения текущего угла сервопривода на другой может произойти сбой работы программы, а что еще хуже, выход из строя данной части робота из-за действия, непредусмотренного конструкцией конкретной модели.

В наборе Jimu «Tankbot» при использовании программного обеспечения «Jimu Robot» на Android может появиться информационное окно, уведомляющее об аномальном изменении положения сервопривода, при этом можно услышать характерный треск данной детали конструктора.

Поэтому перед полным написанием и проверкой программы, следует проводить «тестовые запуски» отдельных сцепок блоков, постепенно присоединяя к ним новые, дабы избежать преждевременной поломки.

Понимание строения программы в Blockly позволит учащимся понять структуру программ уже непосредственно на языках программирования более высокого уровня.

Разбор алгоритмов действий роботов, отладка программ управления ими даст учащимся возможность:

- Ознакомиться с влиянием ошибок измерений и вычислений на выполнение алгоритмов управления реальными объектами (на примере учебных моделей роботов);
- Познакомиться с учебной средой составления программ управления роботами и разобрать примеры алгоритмов управления, разработанными в среде Google Blockly при использовании наборов Jimu.

Подводя итоги, стоит сказать, что результаты освоения учениками курса ориентированы на расширенный вариант обучения информатике в основной школе с включением блока тем по робототехнике. Кроме этого, основы робототехники помогут детям, выбравшим путь изучения роботов, в дальнейшем обучении. Также не стоит забывать о том, что в ходе занятий повышается коммуникативная активность каждого ребёнка, формируется умение работать в паре, в группе, происходит развитие творческих способностей.

Список используемой литературы

1. Робототехника в образовании - https://nsportal.ru/npo-spo/obrazovanie-i-pedagogika/library/2017/06/20/robototehnika-v-obrazovanii – 23.11.2018.

2. Юревич Е. И, Основы робототехники, С. 42-45.

3. Тарапота В. В, Самылкина Н. Н. Робототехника в школе, Изд. «Лаборатория знаний», Москва, 2017. С. 4-10.

4. Инновации в практике образования - https://cyberleninka.ru/article/v/obrazovatelnaya-robototehnika-kak-innovatsionnaya-tehnologiya-realizatsii-politehnicheskoy-napravlennosti-obucheniya-fizike-v - 23.11.2018.

5. Шадронов Д. С., Крылов Н. В. Робототехника в современном образовании // Молодой ученый. — 2018. — №19. — С. 241-243. — URL: https://moluch.ru/archive/205/50145/ - 27.11.2018.

6. Шлямина Е. А. Робототехника в современной школе, 2016. – URL: http://www.openclass.ru/node/511263

7. Особенности изучения робототехники в школе - http://robot.uni-altai.ru/metodichka/publikacii/osobennosti-izucheniya-robototehniki-v-shkole - 24.11.2018.

8. Образовательные конструкторы по робототехнике для детей - https://robo-sapiens.ru/obzoryi/obrazovatelnyie-konstruktoryi-po-robototehnike-dlya-detey/ - 24.11.2018.

9. Современное визуальное программирование: Google Blockly - http://blogerator.org/page/sovremennoe-vizualnoe-programmirovanie-google-blockly-vpl - 24.11.2018.

10. Среда программирования Blockly - http://blockly.ru/manual/beginning.html - 25.11.2018.

List of references

1. Robotics in education - https://nsportal.ru/npo-spo/obrazovanie-i-pedagogika/library/2017/06/20/robototehnika-v-obrazovanii - 23.11.2018.

2. Y. Yurevich, And, Fundamentals of Robotics, pp. 42-45.

3. Tarapot V. In, Samylkina N. N. Robotics in school, Ed. “Laboratory of Knowledge”, Moscow, 2017. P. 4-10.

4. Innovations in the practice of education - https://cyberleninka.ru/article/v/obrazovatelnaya-robototehnika-kak-innovatsionnaya-tehnologiya-realizatsii-politehnicheskoy-napravlennosti-obucheniya-fizike-v – 23.11.2018.

5. Shadronov D. S., Krylov N. V. Robotics in modern education // Young Scientist. - 2018. - №19.- p. 241-243. - URL: https://moluch.ru/archive/205/50145/ - 23.11.2018.

6. Shlyamin E. A. Robotics in the modern school, 2016. - URL: http://www.openclass.ru/node/511263

7. Features of the study of robotics in school - http://robot.uni-altai.ru/metodichka/publikacii/osobennosti-izucheniya-robototehniki-v-shkole - 24.11.2018.

8. Educational designers for robotics for children - https://robo-sapiens.ru/obzoryi/obrazovatelnyie-konstruktoryi-po-robototehnike-dlya-detey/ - 24.11.2018.

9. Modern visual programming: Google Blockly - http://blogerator.org/page/sovremennoe-vizualnoe-programmirovanie-google-blockly-vpl–24.11.2018.

10. The programming environment Blockly - http://blockly.ru/manual/beginning.html – 25.11.2018.

Секция 5. «Инновационные образовательные технологии»

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ОРГАНИЗАЦИИ И УПРАВЛЕНИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТЬЮ

Григоренко Виктория Игоревна[1]
vixa@gmail.com

Татаренко Валерия Андреевна[1]
vtatarenko572@gmail.com

Багдасарян Лусине Шагеновна[1]
канд.филос.наук
bagdasaryan_l@mail.ru

[1] Северо-Кавказский федеральный университет, Ставрополь, 355009, Россия

Аннотация

В данной статье рассматривается вопрос использования инноваций в сфере образования. На сегодняшний день основной целью процесса внедрения инноваций в образование можно считать полное изменение аспектов системы, которые стали традиционными благодаря использованию в течение многих лет. Автор рассматривает основные инновационные технологии и их влияние на эффективность управления образовательной организацией, сделан вывод о целесообразности введения инновационных технологий в образовательный процесс.

Abstract

The article discusses the use of innovation in education. Today the main goal of the process of innovation in education can be considered as a complete change of aspects of the system, which have become traditional through the use for many years. The author examines the basic innovative technologies and their impact on the productivity of management of educational organization, the conclusion efficiency of introduction of innovative technologies in the educational process is done.

Ключевые слова: педагогическая технология, учебный процесс, инновация, образовательная организация, инновационная образовательная технология, информационно-коммуникационные технологии.

Keywords: pedagogical technology, educational process, innovation, educational organization, innovative educational technology, information and communication technologies.

Современный этап развития мировых процессов характеризуется увеличивающейся значимостью применения инноваций во всех сферах жизнедеятельности общества. Применение новых технологий позволяет достигать значимых результатов и во многом повышать эффективность деятельности субъектов, поэтому инновационная направленность деятельности определяет успешность функционирования, конкурентоспособность и перспективы развития всех участников мирового сообщества.

Инновации в образовании – это, прежде всего, процедура обновления и изменения всех концепций образовательного процесса полностью. Данная концепция включает в себя множество разнообразных аспектов: содержание учебной программы, метода и методики изложения информации ученикам, а также различные способы, которые помогут обучать и воспитывать [4, с.84].

Настоящая социально-экономическая ситуация в стране требует модернизации системы образования с целью её максимального приспособления к реалиям общественной жизни. Важнейшим средством обновления и модернизации образования являются инновационные технологии повышения эффективности управления образовательными организациями. При правильно организованном взаимодействии управляющих и управляемых систем можно достичь оптимизации образовательного процесса, повысить уровень образования.

Инновационные процессы в образовании направлены на устранение множества проблем, существующих в детских садах, школах, лицеях, гимназиях, колледжах и высших учебных заведениях. В первую очередь внимание Министерства образования РФ было уделено совершенствованию технических средств обучения. Это позволяет повышать эффективность информационного обмена между учащимися и их педагогом. Инновационные информационные технологии, появившиеся в учебных заведениях, позволили создать новую образовательную среду для реформирования и совершенствования образовательного процесса [5].

Рассмотрим ключевые понятия данной проблематики. Педагогическая технология – это продуманная во всех деталях модель совместной педагогической деятельности по проектированию, организации и проведению учебного процесса с безусловным обеспечением комфортных условий для учащихся и учителя [2, с.85]. Инновация – новообразование в педагогической технологии и практике; превращение отдельных инициатив и новаций в механизм развития образования, что предполагает качественно новые концепции содержания и форм образования [1, с.170]. Именно овладение специальными технологиями управления поможет реализовать инновационные преобразования, так как

последние значительно отличаются от учебно-воспитательных преобразований и требуют особого подхода.

В статье Н.В. Роньжовой [6, с.513] приводятся следующие показатели эффективности управления образовательной организацией:

- дифференцированный подход к сотрудникам;
- умение привлечь педагогов к профессиональному самосовершенствованию;
- организация активных форм профессионального развития педагогов;
- возможность стимулирования и мотивирования профессионального роста педагогов.

Привлечение педагогов к овладению информационно-коммуникационными технологиями (ИКТ) как нельзя лучше может отразить их стремление к профессиональному самосовершенствованию и качественно упростить ведение предмета, приблизить цель мотивирования к познавательной активности. Здесь важно управляющей стороне обеспечить комфортное для педагогов знакомство с ИКТ и их преимуществами, а также необходимо сосредоточить должное внимание на технической оснащенности классных кабинетов [6, с.514].

Информационно-аналитическое обеспечение учебных процессов позволит педагогом следить за индивидуальным развитием учащихся, грамотно принимать меры по направлению его в правильном русле. А это, в свою очередь, отразится и на управлении образовательной организацией, поскольку качественное развитие личности каждого учащегося – гарант стремления педагога к профессиональному росту и самосовершенствованию. В данном аспекте управляющему будет актуально работать с каждым педагогом в отдельности, дифференцированно подходить к сотрудникам.

Воспитательные технологии, нацеленные на разностороннее развитие детей, предусматривают такое же разностороннее развитие и педагогов. Управляющая сторона в таком вопросе должна уделять особое внимание мотивации педагогов в организации культурных, спортивных, интеллектуальных мероприятий, включению в них максимального количества учащихся. Отсюда вытекает и соответствующее обучение учителей, и стимулирование [7, с.75].

Что касается таких технологий, как дидактические, психологопедагогические, личностно-ориентированные, дело обстоит подобным образом: при включении их в образовательный процесс возможно неоспоримое улучшение управления организациями. Все вышеперечисленные инновационные технологии предусматривают и возможность мотивирования и стимулирования профессионального роста педагогов, и организацию активных форм их профессионального развития, и дифференцированный подход к сотрудникам.

Инновации, которые внедряются в нашей стране, реализуют важный социальный заказ. Образовательные программы необходимо направлять не только на получение информации и новых навыков, но и на воспитание в учащихся чувства патриотизма, гордости за свою страну. От системы образования напрямую зависит, будут ли они чувствовать себя полноценными личностями, нужными своей стране. Одно из последних нововведений, которое коснулось школ и ВУЗов – это проведение единого государственного экзамена в

онлайн-режиме, а экзаменационные работы отправляются благодаря предварительному сканированию. Реорганизация системы образования способна разрешить многие проблемы в будущем. Она же, в свою очередь, возможна только благодаря современным инновациям в образовании и достижениям техники.

Инновационные технологии обучения, которые отражают выбор будущей профессии учащегося, формируют в последующем профессиональные качества специалиста, являются своеобразной базой, по которой учащиеся отрабатывают профессиональные навыки в условиях, приближенных к реальным. Одной из главных задач, поставленных перед современной образовательной организацией, является поиск, создание, внедрение образовательных инноваций, которые направлены на удовлетворение общественно-государственного заказа и потребностей участников образовательного процесса [5].

Инновации, которые коснулись современного образования, привели к повышению здоровой конкуренции между педагогическими работниками. У каждого педагога теперь есть свое электронное либо бумажное портфолио, в котором указаны все его профессиональные достижения. Именно по такому «портфелю результатов» эксперты оценивают эффективность и результативность его работы, принимают решение о присвоении своим коллегам определенной квалификационной категории. Благодаря активному внедрению в образовательные учреждения инновационных информационных технологий, появилась возможность полноценного дистанционного обучения детей, имеющих серьезные проблемы со здоровьем. В рамках специального государственного проекта «Доступная среда» для таких школьников создаются комфортные условия для развития, получения новых знаний, приобретения навыков, успешной адаптации к современным социальным условиям. Особое внимание уделяется и внедрению профильной системы на старшей ступени обучения. Это дает возможность учащимся выбирать те направления, которые им интересны, потребуются в большей степени при последующем обучении за пределами школы[3, С.49].

Таким образом, применение инновационных технологий в образовании является одной из технологий повышения уровня управления образовательными организациями. Внедрение таких технологий, как информационно-коммуникационные, личностно-ориентированные, дидактические и другие названные выше, в умелых руках не только позволит развивать образовательную организацию, опираясь на требования современности, но и достигать качественного уровня образования и подготовленности учащихся, их мотивации к учебной деятельности и дальнейшему самосовершенствованию. Проблемное обучение, профильная школа, современные компьютерные технологии, формирование патриотизма и другие – направления, которые стали возможны благодаря инновационным процессам, происходящим в последнее время в российском образовании.

Список используемой литературы

[1] Гнатышина, Е. В. Теоретические аспекты формирования информационной культуры педагога профессионального обучения: монография/ Е.В. Гнатышина. – Челябинск: Изд-во Челяб. гос. пед. ун-та, 2007. – 170 с.

[2] Демцура С.С., Рябчук П.Г., Гордеева Д.С. Ценовая политика государства и вузов на рынке образовательных услуг // Азимут научных исследований: экономика и управление. – 2017. – Т. 6. – № 2 (19). – С. 84-88.

[3] Демцура С.С., Рябчук П.Г., Гордеева Д.С. Проблемы и задачи опережающего управления в сфере реализации образовательных услуг // Азимут научных исследований: педагогика и психология. – 2017. – Т. 6. – № 2 (19). – С. 47-51.

[4] Крюкова А.А. Разработка инновационной системы рейтинговой оценки студентов учебных заведений с использованием механизмов геймификации / А.А. Крюкова, М.С. Зарецкая, К.П. Казаков // Труды Северо-Кавказского филиала московского технического университета связи и информатики. – 2015. – №2. – С. 84–85

[5] Майоров А.А. Инновационное управление образовательными учреждениями. Интернет-доступ: https://cyberleninka.ru/article/n/innovatsionnoe-upravlenie-obrazovatelnymiuchrezhdeniem.

[6] Роньжова Н. В. Эффективное управление образовательной организацией. Сущность понятия «Эффективное управление». Критерии оценки эффективности управления образовательной организацией // Молодой ученый. – 2016. – №23. – С. 513-515.

[7] Сыромятникова Е.Л., Плужникова И.А. К вопросу о процессе выработки стратегии развития образовательной организации // В мире науки и инноваций: сборник статей по материалам международной научнопрактической конференции. В 2-х частях. Краснодар: Издательство: Общество с ограниченной ответственностью «Научное партнерство «Апекс». – 2017. – С. 75-78.

List of references

[1] Gnatyshina, E. V. Theoretical aspects of formation of information culture of the teacher of professional training: monograph/ E. V. Gnatyshina. – Chelyabinsk: publishing house Chelyabinsk. GOS. PED. UN-TA, 2007. – 170 p.

[2] Demura S. S., Ryabchuk P. G., Gordeev D. S. Pricing policy of the state and universities in the market of educational services // Azimuth of scientific research: Economics and management. – 2017. – Vol.6. – № 2 (19). – P. 84-88.

[3] Demura S. S., Ryabchuk P. G., Gordeev D. S. Problems and challenges of advanced control in the sphere of realization of educational services // Azimuth of research: pedagogy and psychology. – 2017. – Vol.6. – № 2 (19). – P. 47-51.

[4] Kryukova A. A. Development of an innovative rating system of students of educational institutions using the mechanisms of gamification / A. A. Kryukova, M. S. Zaretsky,

K. P. Kazakov // Proceedings of the North-Caucasian branch of Moscow technical University of communications and Informatics. – 2015. – №2. – Pp. 84-85.

[5] May innovative management of educational institutions. Internet access: https://cyberleninka.ru/article/n/innovatsionnoe-upravlenie-obrazovatelnymiuchrezhdeniem.

[6] Ronjgova N. V. Effective management of the educational organization. The essence of the concept of «Effective management». Criteria for evaluating the effectiveness of management of educational organization / / Young scientist. – 2016. – №23. – P. 513-515.

[7] Syromyatnikova E. L., Pluzhnikova I. A. Process of development of educational organization strategy // In the world of science and innovation: collection of articles on the materials of the international scientific conference. In 2 parts. Krasnodar: Publisher: limited liability Company «scientific partnership «Apex». – 2017. – P. 75-78.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ СОЦИОЛОГИЧЕСКОГО ИССЛЕДОВАНИЯ

Козуб Алеся Юрьевна[1]
lesiakozub@mail.ru

Яковенко Юлия Андреевна[1]
iuliajakovencko@yandex.ru

Багдасарян Лусине Шагеновна[1]
канд.филос.наук
bagdasaryan_l@mail.ru

[1] Северо-Кавказский федеральный университет, Ставрополь, 355009, Россия

Аннотация

Для изучения конкретных социальных феноменов и социальной реальности как сложного многомерного явления требуется применение специальных методов исследования. Рассматривается роль информационных технологий для реализации информационных процессов на различных стадиях социологического исследования. Большое значение для организации социологического исследования и анализа социологической информации имеют консолидированные информационные ресурсы, благодаря которым исследователи получают совокупность данных об объекте, который они изучают в соответствии с целями и задачами исследования. Для создания консолидированного информационного ресурса решаются следующие задачи: обработка литературных источников и выбор методов и средств; проектирование консолидированного информационного ресурса; реализация. Особое место в решении данных задач занимает применение современных информационных технологий, в том числе сети Интернет.

Abstract

Study of specific social phenomena and social reality as a complex multidimensional phenomenon requires the use of special research methods. In the article the role of information technology for the implementation of information processes at various stages of sociological research is considered. Consolidated information resources, which help researchers receive a set of data about the object that they study in accordance with the goals and objectives of the study, are very efficient for the organization of sociological research and analysis of sociological information. To create a consolidated information resource, the following tasks are solved: the study of literary sources and the choice of methods and means; the design of a consolidated information resource; implementation. The special role in solving these problems plays the use of modern information technologies, including the Internet.

Ключевые слова: информационные технологии, социология, социологическое исследование, этапы социологического исследования, консолидированные информациоздфнные ресурсы, статистические пакеты.

Keywords: information technologies, sociology, sociological research, stages of sociological research, consolidated information resources, statistical packages.

Актуальность исследования информационных технологий в социологии обусловлена спецификой социальной реальности, которая всегда представляется как сложный, многогранный и многозначительный феномен, интегрирует многомерность общества с многомерностью внутреннего мира отдельного человека. Социологи, изучая социальную реальность, сталкиваются с необходимостью выбора адекватных подходов и методов, способных охватить все аспекты изучаемых социальных явлений, учитывая их целостность и взаимозависимость. Как известно, решение этой задачи осуществлялось путем разработки различных теоретических подходов, которые составили основу современной социологии. На эмпирическом уровне поиски «лучших» методов познания многомерной социальной реальности привели к размежеванию количественной и качественной методологии. Результатом стало то, что на сегодняшний день нет единого видения того, каким образом можно осуществить именно «многомерный» анализ, который бы позволил совместить исследования объективных социальных закономерностей с особенностями их субъективных проявлений. К сожалению, в последнее время идея многомерности чаще всего применяется только в контексте методов количественного анализа, хотя ее эвристический потенциал значительно шире.

Первичная социологическая информация представляет собой данные, собранные социологом в результате проведения социологического исследования с целью изучения конкретного социального феномена, для решения актуальной в данный момент проблемы. Такие данные получают в процессе анкетирования, интервьюирования, наблюдение или иным способом в зависимости от выбранной исследователем методологии.

Вторичная информация – это данные, собранные ранее для целей, отличных от решаемой в данный момент проблемы. Вторичная социологическая информация является основой развития так называемого вторичного анализа, который становится все более востребованным средством получения социологического знания. Его нарастающая популярность обусловлена прежде всего тем, что благодаря применению вторичных данных исследователь имеет возможность избежать трудностей и материальных затрат, связанных со сбором первичной социологической информации. Кроме того, информационная ценность исходных данных возрастает при повторном применении (в других исследовательских контекстах и в сочетании с данными других эмпирических измерений), а корректно проведенный синтез первичных данных собственного исследования с анализом вторичной информации дает возможность выйти на более высокий уровень обобщений и выводов, получить нетривиальные теоретические результаты.

О.М. Хмельницкая, З.Н. Нурлигенова обращают внимание на то, что в России использование Интернета как технологии для проведения современных исследований значительно ограничивается из-за особенностей развития научного сообщества. Приоритетными остаются «классические» методы, хотя, как отмечает автор, в связи с быстрым темпом развития информационных и коммуникативных технологий модифицируются уже существующие методы и возникают новые [4].

Ю.Ю. Петрунин считает, что для социологов важно четко понимать смысл событий, которые произошли в области новых коммуникативных технологий, их возможные последствия и использования в социологических исследованиях. Однако автор также указывает на то, что исследования, которые проводятся в этой области, сталкиваются со сложностями, которые связаны с действиями нескольких факторов. Это принципиальная новизна содержания изучаемых процессов, объективные трудности изучения информационных технологий в работе социолога, недостаточная развитость общественных наук в целом, повязанная с методологическим кризисом, слабое распространение новых коммуникативных средств в РФ [2].

О.В. Махныткина указывает на то, что общество становится сетевым, соответственно становятся необходимы сетевые методы сбора социологической информации. Если социальная структура превращается в сеть гетерогенных звеньев, то онлайн-исследования наиболее подходят для сбора информации о сетевых сообщества и для анализа современного сетевого общества в целом. К наиболее распространенным инновационным методикам, позволяющим изучать пользователей сети Интернет, можно отнести навигационную статистику, онлайн-опросы, e-mail-анкетирование, электронные фокус-группы, экспертные опросы, контент-анализ [1].

Интернет занимает особое место в российском пространстве, поскольку наблюдается или его полное игнорирование как феномена при изучении социальных процессов, или его использование ограничивается только проведением социальных опросов. В то же время интернет-пространство может быть «помощником» при использовании некоторых методов исследования (например, социальных опросов, e-mail- или онлайн-интервью). Например, использование электронной онлайн-интервью позволяет избежать многих проблем, с которыми может столкнуться исследователь, обращающийся к интервью в качестве основного метода исследования: затруднение, связанные с охватом достаточно большого географического региона или с доступом к информации, например, людей с ограниченными возможностями [3].

Несмотря на это, исследователи прогнозируют дальнейшее развитие и распространение социологических исследований в Интернете. Постепенно будет совершенствоваться инструментарий исследований и программные средства для их проведения. Для анализа количественных данных существует большое количество различных специализированных программ – статистических пакетов, каждый из которых обладает рядом достоинств и недостатков. Для реализации различных задач можно использовать разные статистические пакеты:

1. Интегрированные методоориентированные пакеты общего назначения. Такие пакеты ещё можно назвать универсальными, т.к они не ориентированы на какую-то конкретную предметную область. К этой группе пакетов можно отнести SPSS, STATA, STATISTIKA и другие.
2. Специализированные методоориентированные пакеты. Как правило, эти пакеты содержат методы 1-2 разделов статистики, применяемые в какой-либо предметной области. К специализированным пакетам статистической обработки данных можно отнести отечественные программы STADIA, Олимп, SAS, BMDP.
3. Предметно- (или проблемно-) ориентированные пакеты. Эти пакеты предназначены для решения вопросов, связанных с конкретной предметной областью. К ним можно отнести такие пакеты, как BioStat, MESOSAUR, DATASCOPE.

Рассмотрим применение информационных технологий на разных стадиях социологического исследования. Перед созданием консолидированного информационного ресурса для проведения социологических исследований необходимо построить «дерево целей». «Дерево целей» позволяет свести сложный процесс создания консолидированного информационного ресурса (КИР) до простых составляющих с помощью конкретных и последовательных действий. Главной целью, как видно из «дерева целей», является создание консолидированного информационного ресурса. Этой цели можно достичь только после выполнения следующих задач:

- обработка литературных источников и выбор методов и средств;
- проектирование консолидированного информационного ресурса;
- реализация.

В соответствии с поставленными задачами, прежде всего обработки литературных источников, необходимо изучить методы и этапы проведения социологического исследования, что позволит определить потребность в информационных технологиях. Также

необходимо проанализировать преимущества и недостатки возможностей информационных технологий, чтобы выявить целесообразность создания консолидированного информационного ресурса.

На втором этапе необходимо смоделировать систему с помощью диаграмм. Для этого необходимо определить основные требования к ресурсу, который проектируется, а также роль, которую он будет выполнять.

На третье этапе – реализации – необходимо описать процесс и графически представить процессы (технологический и механизмы логического вывода и получения данных и т.п.) накопления консолидированных данных. Также можно разместить консолидированный информационный ресурс в форме сайта на коммерческих или бесплатных серверных площадках (хостингах).

Следующий шаг системного анализа - проектирование диаграмм потоков данных, в которых описано и детализировано процессы создания консолидированного информационного ресурса.

Чтобы смоделировать консолидированный информационный ресурс для проведения социологических исследования необходимо исследовать и спроектировать три основных процесса:

1) проведение социологического исследования;
2) создание КИР для проведения социологического исследования;
3) использование КИР для проведения социологического исследования.

Для проведения социологических исследований исследователю необходимо знать информацию о тематике исследования, согласно которому он будет создавать все необходимые элементы для сбора информации. В процессе социологического исследования респондент получает форму для опроса (электронный вариант) и заполняет все необходимые поля (соответствует). Результатом будет вся собранная информация, которая будет подлежать анализу.

Первоначально будет проведена подготовка инструментария исследования, под которым следует понимать анкеты, бланки интервью, письма наблюдения и т.д. в зависимости от задач и метода исследования. В общем результатом будет форма для опроса, с помощью которой будут собирать данные. Респонденты давать ответы на вопросы, которые будут вноситься в специализированные программные средства. Так будет создано хранилище данных «Ответы». Благодаря этому вся собранная информации размещена в одном месте, что позволит ее анализировать и создавать отчеты в соответствии с тематикой исследования.

Следующим шагом будет построение контекстной диаграммы процесса создания консолидированного информационного ресурса для проведения социологического исследования. Для создания КИР для проведения социологических исследований исследователю необходимо разработать главные требования для КИР, поскольку именно от этого зависит информация о техническом задании, которое должен получить разработчик. В соответствии с требованиями разработчик создает шаблон интернет-формы ресурса, которую исследователь наполнить данными, которые необходимы для проведения исследования, то есть сбор информации.

Разрабатывая консолидированный информационный ресурс для проведения социологических исследований, необходимо учесть как общепринятые принципы (модульность, простоту поддержки в течение жизненного цикла), так и специфические требования по условиям его эксплуатации, возможность использования в сети Интернет. Необходимо разработать подсистемы сбора и хранения информации: обозначить принципы реализации благодаря использованию Веб-интерфейса, хранения информации в распределенной базе данных, раздельное хранение структур анкет и данных, содержащихся в них, и использование http-протокола для обмена данными в сети. Подсистемы сбора и хранения должны обеспечивать выполнение следующих задач: генерирование заданной исследователем структуры анкеты и хранение в хранилище данных; генерирование на основе созданной структуры графического интерфейса пользователя для передачи введенных через формы данных пользователя информации в центральное хранилище данных; прием и хранение информации в центральном хранилище данных; передачи введенных через формы пользовательской информации в хранилище данных; прием и хранение информации в центральном хранилище данных.

Таким образом, использование информационных технологий для проведения социологических исследований является лучшим средством, которое поможет исследователям собирать социологическую информацию, создавать анкеты или бланки интервью, также их распространять среди респондентов, например, в сети Интернет. Далее осуществляется загрузка собранных данных (ответов респондентов) в пакеты для статистической обработки данных (SAS, SPSS, BMDP и другие). Информационные технологии предназначены для обеспечения необходимого уровня информативности и качества данных, которые собраны при опросе респондентов, преобразованы в единый формат, в котором они могут быть загружены в хранилище данных или аналитическую систему. Благодаря консолидации социологической информации исследователи получают совокупность данных об объекте, который они изучают в соответствии с целями и задачами, которые поставил перед собой исследователь. Работа с этими данными помогает исследователям выявить основные характеристики, различия, тенденции развития и т.д. социальных процессов и сообществ, оформляется в отчетах, выводах и рекомендациях.

Список используемой литературы

[1] Махныткина О.В. Оптимизация траектории развития слабоформализованного объекта с иерархической структурой // Известия Алтайского государственного университета. – 2013. – №1 –1(77). – С. 116-120.

[2] Петрунин Ю.Ю. Информационные технологии анализа данных/ Ю.Ю.Петрунин. – М.:КДУ, 2017. – 288с.

[3] Шилкина Н.Е. Стратегии социальной адаптации современной студенческой молодежи в городском социальном пространстве (по материалам социологического исследования в г. Барнауле) // Среднерусский вестник общественных наук. – 2013. – № 1. – С. 76-80.

[4] Хмельницкая О.М., Нурлигенова З.Н. Развитие интернет-технологий как средства производства сетевых коммуникаций // Молодой ученый. – 2015. – №9. – С. 1000-1005.

List of references

[1] Mohnatkina O. V. Optimization of the trajectory of development of poorly formalized objects with a hierarchical structure // Izvestiya of Altai State University Journal. – 2013. – №1 – 1 (77). – P. 116-120. (In Russian)

[2] Petrunin Y. Y. Information technology for data analysis/ Yuri Petrunin. – Moscow: KDU, 2017. – 288 p. (In Russian)

[3] Shilkina N. E. Strategies of social adaptation of modern student youth in the urban social space (on the materials of sociological research in the city of Barnaul) // Central Russian Journal of Social Sciences. – 2013. – № 1. – P. 76-80. (In Russian)

[4] Khmelnitskaya O. M., Nurlyaminova Z. N. The development of the online technologies as means of production, network communications // Young Scientist. – 2015. – №9. – P. 1000-1005. (In Russian)

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА УРОКАХ МАТЕМАТИКИ ПРИ ЗАКРЕПЛЕНИИ УЧЕБНОГО МАТЕРИАЛА

Петрович М.П.[1]

marina.petrovich.2015@mail.ru

Зверева Л.Г.[1]

кандидат экономических наук

bdeh@mail.ru

[1]Ставропольский государственный педагогический институт, город Ставрополь, 355029, Россия

Аннотация

Сейчас школьники зачастую больше времени проводят в поиске нужной информации в глобальной сети, в сетевых сообществах, а не в традиционных учебниках. Мозг ребёнка, настроенный на получение знаний в форме развлекательных программ по телевидению, гораздо легче воспринимает предложенную учителем информацию с помощью ИКТ. Следовательно, учителю необходимо владеть не только современными методиками, но и новыми образовательными технологиями, чтобы общаться на одном языке с ребёнком и непрерывно развивающимися ИКТ [3]. Использование информационных технологий в школе становится не редкостью. Несмотря на то, что почти в каждом классе есть компьютер и проектор, многие учителя все же придерживаются традиционной формы урока. В данной статье рассматривается использование различных компьютерных технологий при закреплении материала, при повторении, а также при отработке знаний, умений и навыков. Рассмотрим примеры применение компьютерной

программ «Живая геометрия», Advanced grapher, а также использование универсальных информационных технологий, в частности презентации. Основной задачей педагога в процессе использования ИТ, сводится к поддержанию и направлению процесса развития личности учащихся, их творческого поиска, организации совместной работы.

Abstract

Now students often spend more time in search of the necessary information in the global network, in network communities, and not in traditional textbooks. The child's brain, which is set up to receive knowledge in the form of entertainment programs on television, is much easier to perceive the information offered by the teacher with the help of ICT. Therefore, the teacher needs to know not only modern techniques, but also new educational technologies to communicate in the same language with the child and continuously developing ICT [3]. The use of information technology in school is not uncommon. Despite the fact that almost every class has a computer and a projector, many teachers still adhere to the traditional form of the lesson. This article discusses the use of various computer technologies in the consolidation of the material, the repetition, as well as the development of knowledge and skills. Let us consider examples of the use of computer programs "Live geometry", Advanced grapher, as well as the use of universal information technologies, in particular the presentation. The main task of the teacher in the process of using it is reduced to the maintenance and direction of the process of personal development of students, their creative search, organization of joint work.

Ключевые слова: презентация, программы, математика, эффективность, Advanced grapher, функции, графики, информационные технологии.

Keywords: presentation, programs, mathematics, efficiency, Advanced grapher, functions, graphics, information technologies.

В современном обществе информационные технологии проникли в каждую отрасль, образование не стало исключением. Выпускник школы должен уметь адаптироваться в быстроизменяющихся условиях жизни. Применение компьютерных информационных технологий в обучении — одна из наиболее актуальных направлений развития

образовательного процесса [2]. При использовании на уроке информационных технологий информация становится более наглядной, и усвоить ее можно гораздо быстрее. Совмещая традиционную форму урока с ИТ, обучение можно сделать занимательным и интересным.
Информационные технологии можно разделить на следующие категории:

- Универсальные - текстовый редактор, табличный процессор, компьютерные презентации;
- Специальные - электронные учебники, энциклопедии, тренажеры, системы компьютерной алгебры;
- Интернет - виртуальные лаборатории, дистанционное обучение, виртуальные экскурсии [6].

Сейчас существует масса программ, которые помогают расширить границы урока и выйти за пределы «просто» презентации. Презентация – это не только меняющиеся слайды, на которых написана информация, которую школьники могут переписать к себе в тетрадь, но и возможность использовать ее в качестве шаблона для игры, используя гиперссылки. Например, для закрепления пройденного материала на уроке можно провести викторину в форме «Своя игра» (рисунок 1), шаблон к этой игре находится в свободном доступе в интернете. Ведь увеличение умственной нагрузки на уроках математики уменьшает интерес учеников к предмету, поэтому необходимо использовать дополнительные ресурсы для поддержания интереса на протяжении всего урока [4].

Рисунок 1. Шаблон презентации «Своя игра»

Использование такой презентации на уроке закрепления, полученных знаний способствует улучшению зрительного восприятия. На таком уроке школьнику необходимо вспомнить теоретические и практические знания для того, чтобы успешно ответить на вопрос. Можно сказать, что урок, на котором используется такая презентация, является частично поисковым.

Для того, чтобы разнообразить виды учебной деятельности учащихся при закреплении материала можно использовать обучающиеся программы, на которых ученики самостоятельно закрепляют изученную тему [1]. Так, при изучении темы: «Графики тригонометрических функций» преобразования графиков тригонометрических функций

учащиеся могут осуществить с помощью программы Advanced grapher (рисунок 2). С помощью данной программы можно проследить всю динамику последовательных действий с функциями *sinx, cosx, tgx* и т.д, построение которых вызывает постоянные затруднения. Использование такой программы способствует выработки навыка построения функции, запоминанию как выглядит график тригонометрических функции, так как при многократном построении запоминается зрительно вид графика [5]. Урок с использованием Advanced grapher будет более эффективен, нежели урок по данной теме в традиционной форме, т.к. ученики закрепляют знания в процессе самостоятельной творческой работы, знания необходимы им для получения конкретного, видимого на экране компьютера, результата. Педагог, выступая в роли посредника, наставника, создает ситуацию активного поиска и практической деятельности.

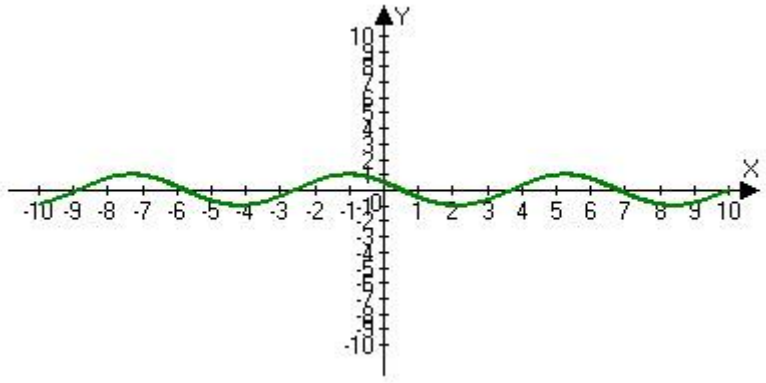

Рисунок 2. График функции, построенной в программе Advanced grapher

Вряд ли найдется много учеников, которые скажут, что их любимым предметом в школе является геометрия. Это достаточно сложная и трудная дисциплина, для понимания которой нужно приложить немало усилий. Применение программы «Живая Геометрия» позволит серьезно подтянуть уровень знаний. С помощью мультипликации можно «оживить задачи». Использование данной программы позволяет сделать процесс обучения интересным и наглядным, развивает творческую деятельность учащихся, их абстрактное, логическое и инженерное мышление[8].

«Живая геометрия» - это набор инструментов, который предоставляет все необходимые средства для построения чертежей и их исследований. Она дает возможность «открывать» и проверять геометрические факты. Программа позволяет "оживлять" чертежи, плавно изменяя положение исходных точек. Например, при построении окружности программа автоматические покажет уравнение окружности, вычислит площадь радиус, в программе можно выполнять построения сложных чертежей (рисунок 3).

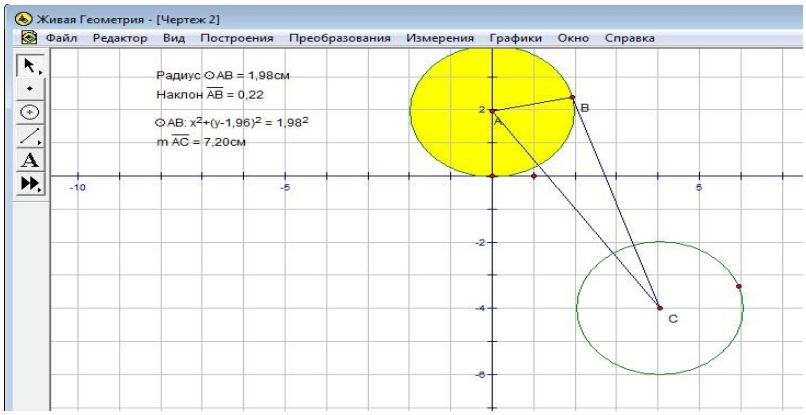

Рисунок 3. Использование программы «Живая геометрия» при построении чертежей

Таким образом, рассмотрев лишь малую часть программ, которые можно использовать на уроках математики. Можно сказать, что каждая программа станет отличным дополнением к традиционному уроку, разбавив рутинные вычисления в тетради. Использование ИТ является эффективным методом обучения и таким методическим приёмом, который активизирует мысль школьников, стимулирует их к самостоятельному приобретению знаний [7].

Список используемой литературы

[1] Оленев А.А., Тынчеров К.Т., Селиванова М.В., Петрович М.П. Решение задач теории чисел в СКА MAXIMA // Материалы 45-й Международной научно-технической конференции молодых ученых, аспирантов и студентов: в 2-х т. / отв. ред. В.Ш. Мухаметшин. – Уфа: Изд-во УГНТУ, 2018. – Т. 1. – 470 с.

[2] Ушакова В. А. Использование информационных технологий на уроках математики // Молодой ученый. – 2016. – №8. – 1053-1055 с.

[3] Стекленева С. Ю. Значение использования информационно-коммуникационных технологий в обучении географии [Текст] // Педагогическое мастерство: материалы Междунар. науч. конф. (г. Москва, апрель 2012 г.). – М.: Буки-Веди, 2012. –.180-182 с.

[4] Зверева Л.Г., Кумратова Ж.Р. Роль мониторинга вузов в принятии управленческих решений // Экономика устойчивого развития. 2015. № 2 (22) – 103-108 с.

[5] Погодина И.А. Формирование информационно-коммуникационной компетенции учащихся в условиях общеобразовательной школы //автореферат диссертации на соискание ученой степени кандидата педагогических наук // Северо-Осетинский государственный университет им. К.Л. Хетагурова. Владикавказ, 2011

[6] Гришин, В.Н. Информационные технологии в профессиональной деятельности: Учебник / В.Н. Гришин, Е.Е. Панфилова. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

[7] Киселев, Г.М. Информационные технологии в педагогическом образовании: Учебник / Г.М. Киселев, Р.В. Бочкова. - М.: Дашков и К, 2013. - 308 с.

[8] Николаева Е. Н. Информационные образовательные технологии на уроках математики // Научно-методический электронный журнал «Концепт». – 2014. – Т. 16. – С. 36–40

List of references

[1] Olenev A.A., Tyncherov K.T., Selivanova M.V., Petrovich M.P. Solving the problems of number theory in SKA MAXIMA // Proceedings of the 45th International Scientific and Technical Conference of Young Scientists, Postgraduates and Students: in 2 volumes / resp. ed. V.Sh. Mukhametshin. - Ufa: Publishing house UGNTU, 2018. - T. 1. - 470 p.
[2] Ushakova V. A. Use of information technologies at mathematics lessons // Young scientist. - 2016. - №8. - 1053-1055 s.
[3] S. Stekleneva. The value of using information and communication technologies in teaching geography [Text] // Pedagogical Mastery: Proceedings of the Intern. scientific conf. (Moscow, April 2012). - M .: Buki-Vedi, 2012. –180-182 p.
[4] Zvereva L.G., Kumratova J.R. The role of university monitoring in making management decisions // Economics of Sustainable Development. 2015. № 2 (22) - 103-108 p.
[5] Pogodina I.A. Formation of information and communication competence of students in a secondary school // dissertation abstract for the degree of candidate of pedagogical sciences // North Ossetian State University. K.L. Khetagurov. Vladikavkaz, 2011
[6] Grishin, V.N. Information technology in professional activities: Textbook / V.N. Grishin, E.E. Panfilov. - M .: ID FORUM, SIC INFRA-M, 2013. - 416 c.
[7] Kiselev, G.M. Information technologies in pedagogical education: Textbook / G.M. Kiselev, R.V. Bochkova. - M .: Dashkov and K, 2013. - 308 c.
[8] Nikolayeva Ye. N. Informational educational technologies at the lessons of mathematics // Scientific-methodical electronic journal "Concept". - 2014. - V. 16. - P. 36–40

ПРИМЕНЕНИЕ ИГРОВЫХ МЕТОДОВ ОБУЧЕНИЯ ДЛЯ ЗАКРЕПЛЕНИЯ ТЕОРЕТИЧЕСКОГО МАТЕРИАЛА ПО МАТЕМАТИЧЕСКИМ ДИСЦИПЛИНАМ

Сеитбекова Л.Д.[1]
lialiseitbekova@gmail.com.

Нугманов Д.Т.[1]
daniyar31604@gmail.com

Кручинин Д.В.[1]
Кандидат физико-математических наук, научный сотрудник, доцент
kdv@keva.tusur.ru

[1] Томский государственный университет систем управления и радиоэлектроники (ТУСУР), Томск, 634050, Российская Федерация

Аннотация

Традиционные методы преподавания, когда ведется пассивное преподнесение теоретического материала, неэффективны, ввиду отсутствия участия обучающегося в образовательном процессе. Электронное обучение активно применяется во многих образовательных учреждениях, но только система Moodle способна реализовывать сложные задания по высшей математике. В связи с чем необходимо изучить и использовать средства разработки заданий системы Moodle, для реализации «Своей игры» в рамках дисциплины «Математический анализ». В данной статье рассмотрены типы вопросов системы Moodle, такие как: краткий ответ, верно\неверно, на соответствие, множественный выбор. Составлено тестовое главное окно игры, описаны ее правила и попытки прохождения командой задания с удачным и неудачным исходами. Реализована игра «Новогодний Квиз», включающая в себя следующие темы: квадратные уравнения, неравенства, построение графиков, матрицы, производные, пределы. Произведена апробация

данной методики на студентах первого курса специальности «Экономическая безопасность». Студенты, на которых произведена апробация, показали большую активность и лучше сдали коллоквиум по сравнению со остальными первокурсниками. Использование игровых методов в математических дисциплинах более эффективно чем пассивное преподнесения теоретического материала.

Abstract

Traditional teaching methods, when passive presentation of theoretical material is carried out, are ineffective due to the lack of participation of the student in the educational process. E-learning is actively used in many educational institutions, but only the Moodle system is able to implement complex tasks in higher mathematics. Because of that, it is necessary to study and use the tools for the development of tasks of the Moodle system, to implement «Your game» within the discipline «Mathematical analysis». This article discusses the types of Moodle system questions, such as: short answer, true\false, matching, multiple choice. Made the test main window of the game, described rules and attempts of passing of a task by team with successful and unsuccessful outcomes. Implemented game «Christmas Quiz», which includes the following topics: square equations, inequalities, plotting, matrices, derivatives, limits. The approbation of this technique on students of the first course of the specialty «Economic security» is made. The use of game methods is a good solution to replace the passive presentation of theoretical material in mathematical disciplines. Students, in which the algorithm is tested, showed greater activity and better passed the Colloquium compared to the rest of the freshmen.

Ключевые слова: игра, система обучения, теоретический материал, математические дисциплины, Moodle, STACK.

Keywords: game, online-learning, mathematical disciplines, theoretical material, STACK, Moodle.

1 Введение

Традиционные методы преподавания, когда ведется пассивное преподнесение теоретического материала, неэффективны, ввиду отсутствия участия обучающегося в процессе освоения

материала. Человек может учиться, не замечая процесса обучения, поэтому интерес студента - это лучший помощник преподавателю в его успешной работе. Неудивительно, что игровые методы обучения являются одним из вспомогательных средств в освоении изучаемых предметов.

В качестве игры необходимо реализовать процесс изучения теоретического материала по математическим дисциплинам. Одними из самых популярных можно выделить следующие игры: «Что? Где? Когда?» [1], «Брейн-ринг» [2], «Своя игра» [3]. Так как первые две игры рассчитаны на малое количество вопросов, то за основу разработки выбрана российская телевизионная игра-викторина «Своя игра», в ней изначально представлено разделение вопросов по категориям и бальная оценка за каждый вопрос. Существует компьютерная версия «Своей игры» [4], но она не располагает возможностью создания викторин с математическими заданиями.

Электронное обучение в современном мире, активно входит учебную программу каждого развивающегося образовательного учреждения. Поэтому возможна реализация «Своей игры» на базе существует систем управления обучением, например, таких как: iSpring Online [5], Blackboard Learn [6], Schoology [7], Teachbase [8] и других. Blackboard Learn и iSpring Online не берутся во внимание, так как при всем своем функционале являются платными. В Schoology и Teachbase отсутствует возможность оценки курсов и создания собственного домена. Как видно, не каждая из них подходит для создания и оценивания заданий.

Moodle (Modular Object-Oriented Dynamic Learning Environment) [9] - модульная объектно-ориентированная динамическая обучающая система. Наряду с тем, что Moodle по функциональным возможностям сопоставима с выше приведёнными аналогами, она обладает совокупностью параметров, выделяющих ее из остальных:

- является системой с открытым исходным кодом, что позволяет интегрировать ее с информационными системами и сервисами, уже существующими в университете;
- обладает плагином Stack [10], средством для создания сложных заданий по математическим дисциплинам, способных, помимо выдачи бальной оценки, на формирование подробного отзыва, на ответ студента;
- является бесплатной и свободно распространяемой.

2 Постановка задачи

Изучить и использовать средства разработки заданий системы Moodle, для применения и реализации «Своей игры» для изучения теоретического материала по математическим дисциплинам.

3 Решение задачи

Для решения поставленной задачи необходимо выделить следующие подзадачи:

- определить и адаптировать правила игры;
- рассмотреть главные особенности типов вопросов в системе Moodle;

– применить возможности вопросов Moodle для реализации игры.

4 Правила игры

В отличии от оригинала разрабатываемая игра имеет ряд отличий:

– вместо денежного значения каждый из вопросов будет оценен определенным количеством баллов, в зависимости от сложности;
– вместо игроков будут соревноваться команды, количество и состав которых зависит от числа студентов группы и определяется преподавателем;
– для справедливого оценивания и равноправного участия в игре каждого из студентов, вводится условие, благодаря которому человек набравший определенное количество баллов выходит из игры и получает свою заслуженную оценку.
– борьбу продолжают оставшиеся члены команды;
– команда, все члены которой первыми наберут нужные баллы, является победителем.
– виды категорий и количество вопросов в них, зависят от проходимой темы и определяются преподавателем.

5 Типы вопросов в Moodle

Для разработки заданий по теории из перечня располагаемых системой Moodle вопросов, необходимо рассмотреть четыре наиболее подходящих [11]:

– краткий ответ - позволяет вводить в качестве ответа одно или несколько слов; ответы оцениваются путем сравнения с разными образцами ответов, в которых могут использоваться подстановочные знаки см (рис. 1);
– верно\неверно - простая форма вопроса «множественный выбор», предполагающая только два варианта ответа: «верно» или «неверно» см (рис. 2);
– множественный выбор - позволяет выбирать один или несколько правильных ответов из заданного списка см (рис. 3).
– на соответствие - ответ на каждый из нескольких вопросов должен быть выбран из списка возможных см (рис. 4);

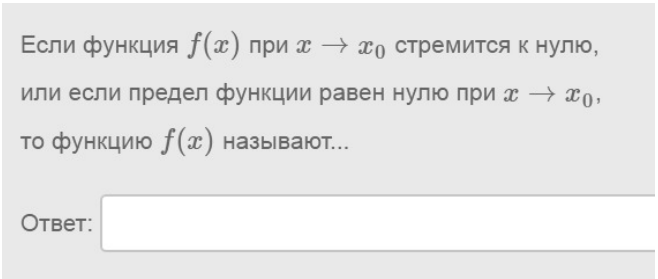

Рисунок 1. Тип вопроса «Краткий ответ».

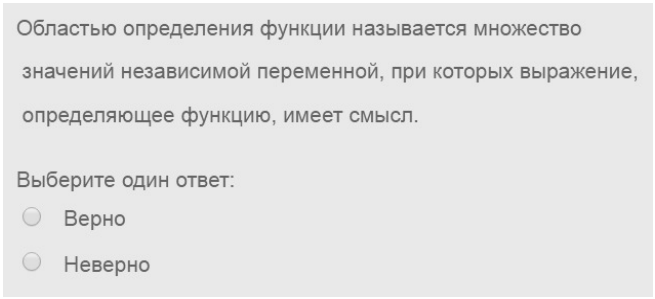

Рисунок 2. Тип вопроса «Верно\Неверно».

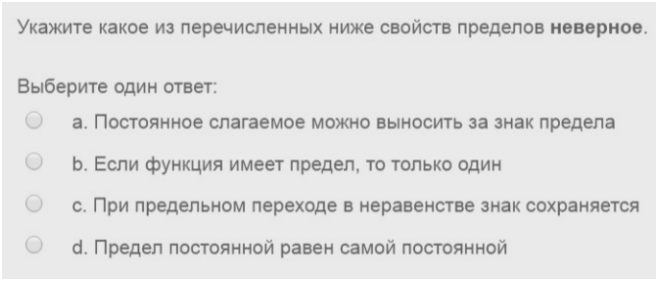

Рисунок 3. Тип вопроса «Множественный выбор».

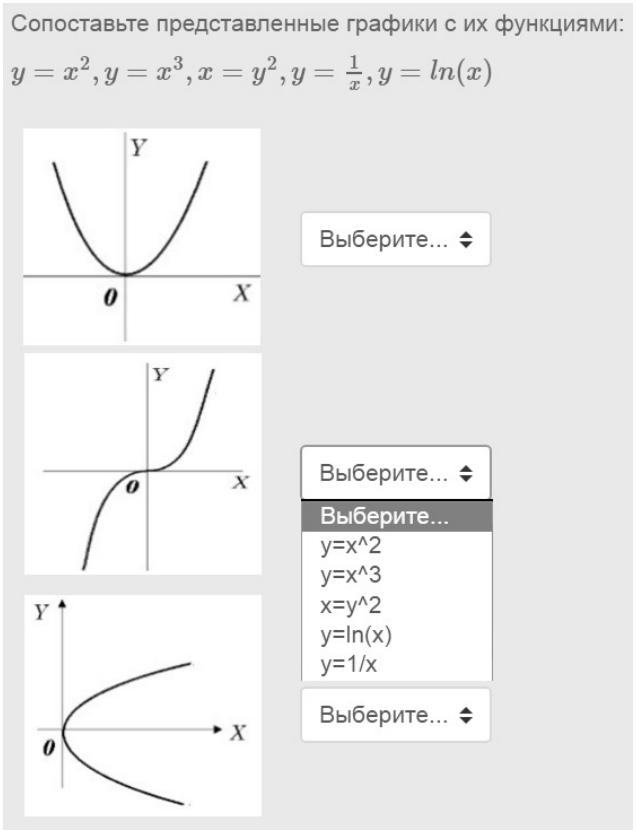

Рисунок 4. Тип вопроса «На соответствие».

Рисунок 5. Главное поле игры.

6 Реализация игры

Игра представляет совокупность всех четырех приведенных выше типов вопросов. Главное поле игры включает в себя названия разделов и сами вопросы с указанием баллового значения каждого из них см (рис 5.). Каждое из заданий принадлежит только к одному из типов вопросов.

После выбора категории и номера вопроса, открывается окно, которое состоит из четырех основных частей см (рис. 6):

- текст задания;
- номер вопроса, его балловая значимость, количество попыток, определяемое количеством команд в игре;
- «навигация по тесту» - таблица, объединяющая все вопросы вместе;
- поле проверки введенного или выбранного ответа.

Во время игры, если команда, которой принадлежит право ответа, ошибается, очередь на выполнение задания переходит к следующей.

При удачной попытке кнопка с номером вопроса в «Навигации по тесту» наполовину закрашивается темным цветом и к ней добавляется белая галочка, это означает, что задание выполнено верно, и команда получит свой заслуженный балл см (рис. 7).

Если ни одна из команд не ответила верно на задание, то его кнопка в «Навигации по тесту» наполовину закрашивается темным цветом, это означает, что вернуться к данному вопросу уже нельзя см (рис. 8) [12].

После того как будут пройдены все вопросы, объявлена команда победителей, игра считается завершенной.

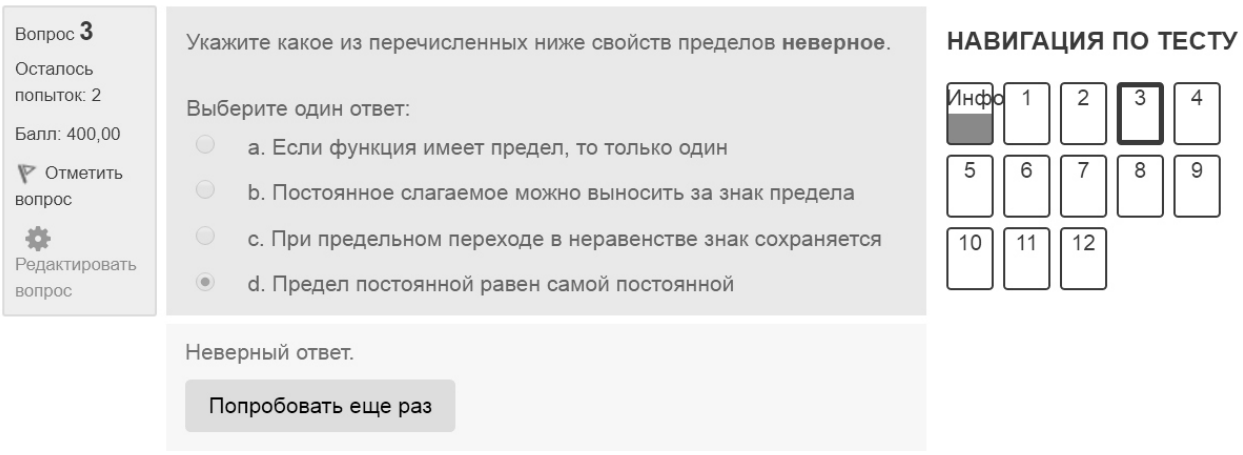

Рисунок 6. Неверный ответ, с последующей новой попыткой.

Рисунок 7. Правильный ответ на задание.

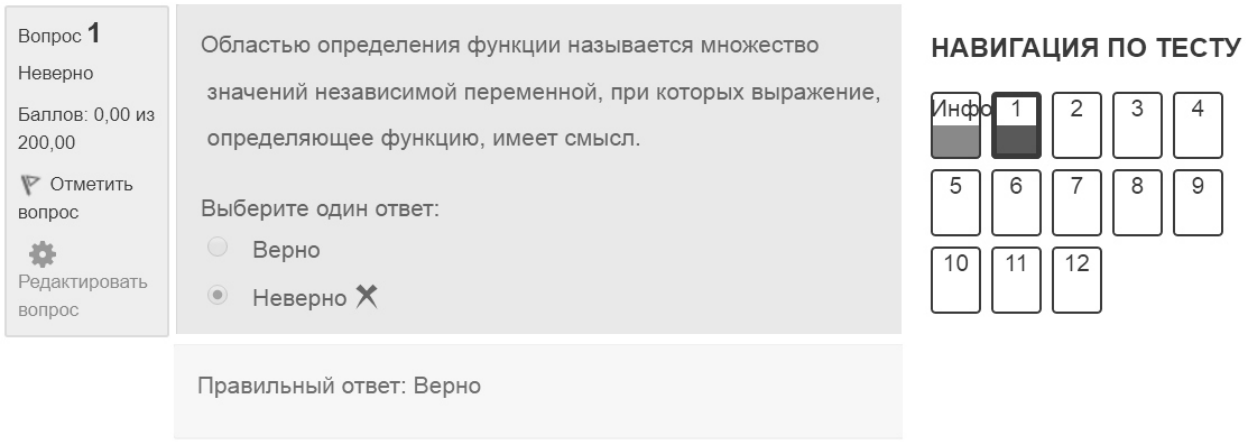

Рисунок 8. Неверный ответ, без права на новую попытку.

7 Результаты работы

Рассмотрены типы вопросов системы Moodle, составлено тестовое главное окно игры, описаны ее правила и попытки прохождения командой задания с удачным и неудачным исходами. Реализована игра «Новогодний Квиз», включающая в себя следующие темы: квадратные уравнения, неравенства, построение графиков, матрицы, производные, пределы. Произведена апробация данной методики на студентах первого курса специальности «Экономическая безопасность».

8 Обсуждение

Студенты, на которых произведена апробация, показали большую активность и лучше сдали коллоквиум по сравнению со остальными первокурсниками.

9 Заключение

Использование игровых методов обучения для реализации заданий в системе Moodle показало свою эффективность в повышении уровня усвоения теоретического материала по математическим дисциплинам.

Список используемой литературы

[1] Игра «Что? Где? Когда?» [Электронный ресурс]. – /Режим доступа: http://chgk.tvigra.ru/ (дата обращения 08.09.2017).

[2] Игра «Брэйн-ринг» [Электронный ресурс]. – /Режим доступа: http://brain.tvigra.ru/reglament/ (дата обращения 08.09.2017).

[3] Игра «Своя игра» [Электронный ресурс]. – /Режим доступа: http://www.ntv.ru/peredacha/svoya_igra/about/146/ (дата обращения 10.09.2017).

[4] Компьютерная версия «Своей игры» [Электронный ресурс]. – /Режим доступа: http://vladimirkhil.com/si/game (дата обращения 15.09.2017).

[5] iSpring Online [Электронный ресурс]. – /Режим доступа: https://www.ispring.ru (дата обращения 15.09.2017).

[6] Blackboard Learn [Электронный ресурс]. – /Режим доступа: https://help.blackboard.com (дата обращения 14.09.2017).

[7] Schoology [Электронный ресурс]. – /Режим доступа: https://www.schoology.com/ (дата обращения 08.09.2017).

[8] Teachbase [Электронный ресурс]. – /Режим доступа: http://teachbase.ru/ (дата обращения 11.09.2017).

[9] Moodle [Электронный ресурс]. – /Режим доступа: https://moodle.org/ (дата обращения 3.09.2017).

[10] Moodle plugins directory – STACK [Электронный ресурс]. – /Режим доступа: https://moodle.org /plugins/qtypestack (дата обращения: 07.09.2017).

[11] Дополнительное образование факультета безопасности ТУСУР [Электронный ресурс]. – /Режим доступа: https://do.fb.tusur.ru (дата обращения: 05.09.2017).
[12] Образовательный портал факультета безопасности ТУСУР [Электронный ресурс]. – /Режим доступа: https://edu.fb.tusur.ru (дата обращения: 05.09.2017).

List of references

[1] Игра «Что? Где? Когда?» – / Available at: http://chgk.tvigra.ru/ (accessed 08.09.2017). (In Russian).
[2] Игра «Брэйн-ринг» – / Available at: http://brain.tvigra.ru/reglament/ (accessed 08.09.2017).
[3] Игра «Своя игра» – / Available at: http://www.ntv.ru/peredacha/svoya_igra/about/146/ (accessed 10.09.2017).
[4] Компьютерная версия «Своей игры» – /Available at: http://vladimirkhil.com/si/game (accessed 15.09.2017).
[5] iSpring Online – /Available at: https://www.ispring.ru (accessed 15.09.2017).
[6] Blackboard Learn [Электронный ресурс]. – / Available at: https://help.blackboard.com (accessed 14.09.2017).
[7] Schoology – / Available at: https://www.schoology.com/ (accessed 08.09.2017).
[8] Teachbase – / Available at: http://teachbase.ru/ (accessed 11.09.2017).
[9] Moodle – / Available at: https://moodle.org/ (accessed 3.09.2017).
[10] Moodle plugins directory – STACK – / Available at: https://moodle.org /plugins/qtypestack (accessed 07.09.2017).
[11] Дополнительное образование факультета безопасности ТУСУР – / Available at: https://do.fb.tusur.ru (accessed 05.09.2017).
[12] Образовательный портал факультета безопасности ТУСУР – / Available at: https://edu.fb.tusur.ru (accessed 05.09.2017).

ИСПОЛЬЗОВАНИЕ СКА MAXIMA НА УРОКАХ АЛГЕБРЫ ПРИ ПОДГОТОВКЕ К ЕГЭ

Петрович М.П.[1]
marina.petrovich.2015@mail.ru

Оленев А.А.[1]
кандидат технических наук, доцент
olenevalexandr@gmail.com

[1] Ставропольский государственный педагогический институт, город Ставрополь, 355029, Россия

Аннотация

С экзаменом по математике может справиться каждый ученик при правильной подготовке. Безусловно, без натаскивания на варианты ЕГЭ не обойтись, но его нужно сочетать с фундаментальной подготовкой и использованием дополнительных ресурсов, которые способствуют не только закреплению полученных знаний, но и углублению [8]. Наряду с совершенствованием традиционных технологий, ИКТ становятся важнейшей составляющей совершенствования учебного процесса. Среди программных средств, которые получили широкое распространение в образовании, следует отметить системы компьютерной алгебры (СКА). Использование СКА на уроках алгебры в школе способствуют повышению интенсивности учебного процесса, исключают рутинные вычисления при решении на бумаге. В статье рассматривается использование одного из пакетов системы компьютерной алгебры Maxima для подготовке к ЕГЭ в школе на уроках алгебры. На основе пакета Maxima разберем типовые задачи ЕГЭ, которые можно реализовать с помощью встроенных функций.

Abstract

With the exam in mathematics can handle every student with proper preparation. Of course, without coaching on the exam options can not do, but it must be combined with fundamental training and the use of additional resources that contribute not only to consolidate the knowledge gained, but also to deepen [8]. Along with the improvement of traditional technologies, ICT are becoming an important component of improving the educational process. Among the software tools that are widely used in education, it should be noted computer algebra systems (CSA). The use of SKA in algebra lessons at school contribute to the intensity of the educational process, exclude routine calculations when solving on paper. The article discusses the use of one of the packages of the computer algebra system Maxima to prepare for the exam at school in algebra lessons. Based on the Maxima package, we will analyze typical use tasks that can be implemented with the help of built-in functions.

Ключевые слова: Алгебра, система компьютерной алгебры, тригонометрические функции, графики, критические точки, ЕГЭ, экстремум, функции.

Keywords: Algebra, computer algebra system, trigonometric functions, graphs, critical points, use, extremum, functions.

Современное общество ставит перед школой новые задачи, выпускник 21 века должен уметь быстро адаптироваться в изменяющихся условиях жизни. Современное развитие компьютерной техники и интенсивное развитие нового направления - компьютерной алгебры - привели к тому, что широкое распространение и спрос получили комплексы программ, которые называются системами компьютерной алгебры [5]. Использование систем компьютерной алгебры (СКА) дает возможность результативно усваивать и закреплять знания, получаемые школьниками при изучении общих и специальных математических дисциплин. Начинать активно применять СКА лучше со школы, это связано с рядом причин. Первая: у обучающихся в школе легче вызвать интерес к решению и проверки трудных для него задач. Вторая: для дальнейшего обучения останутся навыки ориентирования в сложном мире математики. Третья: расширяется кругозор и навыки использования информационных технологий [6].

Применение СКА в образовании поможет обучающимся избавиться от большого количества рутинных вычислений и высвобождает их время для обдумывания алгоритмов решения задач, более обоснованной постановки их решения, многовариантного подхода и представления результатов в наиболее наглядной форме [3]. Время, которое позволяет сэкономить применение СКА, можно направить для более глубокого изучения

математической или физической сущности решаемых задач и их решения различными методами. Иначе говоря, СКА не лишают учащихся серьезных математических навыков, а, напротив, способствуют их расширению и углублению.

В математической подготовке будущих учителей можно активно применять систему компьютерной алгебры Maxima. Данный выбор обусловлен рядом причин, особо весомой из них является следующая: данный математический пакет является свободно распространяемым программным продуктом, а общим вычислительным возможностям (решению основных задач школьного уровня) не уступает таким коммерческим аналогам, как СКА Maple и Mathematica. Наличие свободной лицензии является весьма актуальным в современных условиях, и позволяет свободно устанавливать данный продукт и в школе, и вузе без лишних затрат.

В этой статье будет рассмотрены возможности применения СКА Maxima при решении типовых заданий ЕГЭ, которые вызывают у школьников определенные трудности. Задания взяты из учебно-методических материалов по математике «Тренировочные тестовые задания по алгебре и началам анализа» для учащихся 10-х и 11-х классов [4].

Задание 1. Вычислить $2\sin 15° \cdot \cos 15°$

Для вычисления данного выражения при решении на бумаге необходимо было бы вспомнить формулы двойного угла, а для вычисления такого тригонометрического выражения в СКА Maxima достаточно ввести функцию trigreduce. Функция trigreduce выполняет свертку всех произведений тригонометрических и гиперболических функций в комбинации соответствующих функций от сумм. Функция работает не до конца, так что повторный вызов может изменить выражение. При вызове функции в формате trigreduce(expr, x) преобразования осуществляются относительно функций x.

```
(%i26)  2*sin(x)*cos(x);
(%o26)  2*cos(x)*sin(x)
(%i27)  trigreduce(%);
(%o27)  sin(2*x)
(%i28)  sin(2*π);
```

Ответ:

```
(%o28)  0
```

Использование СКА Maxima позволяет повысить интенсивность урока, СКА увеличивает количество решенных заданий и тем самым дает возможность не только углубить знания, полученные на уроке, но и делать самопроверку уже решенных заданий [7].

Задание 2. Упростить выражение $\frac{\tan\left(\frac{\pi}{4}+\alpha\right)-\tan\left(\frac{\pi}{4}-\alpha\right)}{1+\tan\left(\frac{\pi}{4}+\alpha\right)\tan\left(\frac{\pi}{4}-\alpha\right)}$ и найти его значение, если $\alpha = \pi$

```
(%i44)  trigsimp((tan((pi/4)+a)-tan((pi/4)a))/(1+tan((pi/4)+a)*tan((pi/4)-a)));
```

Для выполнения такого преобразования используем функцию СКА Maxima trigsimp. Данная функция выполняет упрощение. Функция trigsimp упрощает тригонометрические и гиперболические выражения, применяя к ним правила основного тригонометрического тождества и гиперболические тригонометрические тождества [2].

(%o44) (cos((pi-4*a)/4)*sin((pi+4*a)/4)-sin((pi-4*a)/4)*cos((pi+4*a)/4))/(sin((pi-4*a)/4)*sin((pi+4*a)/4)+cos((pi-4*a)/4)*cos((pi+4*a)/4))

(%i45) trigrat(%);

Использование функции trigrat (expr) приводит заданное тригонометрическое выражение expr к канонической упрощённой форме [9]. Полученный результат рассматривается как рациональное, содержащее функции sin(x), cos(x), tan(x), аргументы, которых являются линейные формы некоторых переменных и π/n, где (n - целое).

(%o45) sin(2*a)/cos(2*a)

Согласно условию задачи для выполнения преобразования необходимо выполнить подстановку $\alpha = \pi$:

(%i25) sin(2*π)/cos(2*π);

Ответ:

(%o25) 0

Задание3. Решить уравнение

$$\cos\frac{2\pi x}{3} = 1 + (x-3)^2$$

Уравнения и системы уравнений решаются в Maxima, используя функцию solve. Интерфейс wxMaxima позволяет упростить процедуру использования функции solve: пользователю необходимо лишь нажать в меню программы кнопку «Решить», после чего появится дополнительное окно «Решить», в котором необходимо конкретизировать вид уравнения, имя переменной, относительно которой нужно решить уравнение (рис.1)

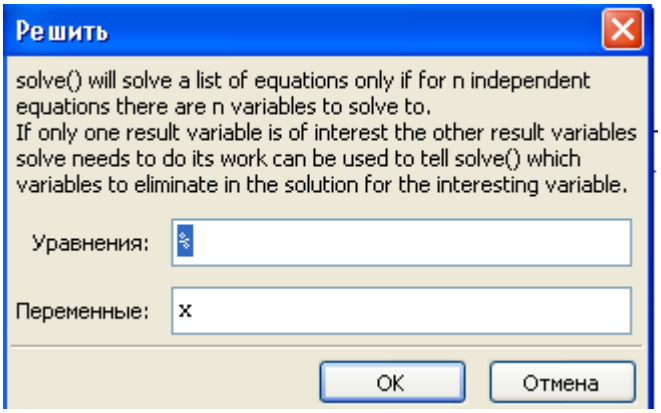

Рисунок 1. Диалоговое окно «Решить»

(%i8) solve([cos ((2*π*x)/3)=1+(x-3)^2],[x]);

(%o8) [x=3-sqrt(cos((2*%pi*x)/3)-1),x=sqrt(cos((2*%pi*x)/3)-1)+3]

В полученные корни уравнения $x = 3 - \sqrt{\cos\left(\frac{2\pi x}{3}\right) - 1}, x = 3 + \sqrt{\cos\left(\frac{2\pi x}{3}\right) - 1}$ подставим значение *x=0* и получим численное решение уравнений.

(%i7) n=3-sqrt(cos((2*%pi*x)/3)-1), x=0;

(%o7) n=3

(%i8) n=sqrt(cos((2*%pi*x)/3)-1)+3,x=0;

(%o8) n=3

Задание 4. Постройте график функции $y = -2\sin(\frac{\pi}{6} - x)$ на промежутке $[-\pi; 3\pi]$.

График функции y=f(x) на отрезке [a, b] в СКА Maxima можно построить, используя функции plot2d(f(x), [x,a,b], опции) или plot2d(f(x), [x,a,b], [y,c,d], опции). Для построения графика можно использовать большое количество дополнительных опций: вывод заголовка функции и подписи к осям, устанавливать цену деления по осям *Ox* и *Oy*, с которой будут наноситься метки на оси, веет координатных осей и прочее. Если изменять свойства графика не нужно, то опции можно не задавать. Если параметр [y,c,d] не задан, то высота графика выбирается по умолчанию [1].

```
(%i12)  plot2d([-2*sin((π/6)-x)], [x,-π,3*π], [y,-π,3*π],
   [plot_format, xmaxima])$
```

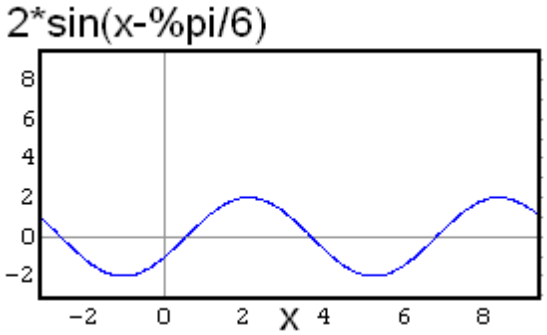

Рисунок 2. График функции $y = -2\sin(\frac{\pi}{6} - x)$

Задание 5. Указать точки экстремумов функции $f(x) = \frac{x^2+8}{(\sqrt{x+1})^2}$

Для нахождения точек экстремума в Maxima выполняется следующий алгоритм действий:

1. Вычислить производную функции, использовав функцию СКА Maxima - diff, которая записывается как diff(выражение, переменная1, порядок производной для переменной1 [,переменная2, порядок производной для переменной2,…]), где выражение - это функция, производную которой необходимо найти, второй аргумент является переменной, по которой нужно брать производную, третий (необязательный) - порядок производной, если порядок не указан, то по умолчанию устанавливается первый.

2. Решить уравнение, приравнять производную к нулю, используя уже знакомую нам функции СКА Maxima solve. Решив уравнение, находим критические точки.

3. Вычислить производную второго порядка d2f(x).

4. Чтобы найти значение второй производной в критических точках, необходимо использовать функцию СКА Maxima - map (функция, выражение1,выражение2,...) – данная функция применяется к последовательности выражений.

Другие функции, используемые при нахождении экстремума функции: define аналогичны оператору определения функции :=.

```
(%i14)  f(x):=(x^2+8)/((sqrt(x+1))^2);
(%o14)  f(x):=(x^2+8)/sqrt(x+1)^2
```

```
(%i15)  define(df(x),diff(f(x),x));
(%o15)  df(x):=(2*x)/(x+1)-(x^2+8)/(x+1)^2
(%i16)  solve(df(x)=0,x);
(%o16)  [x=-4,x=2]
(%i17)  define(d2f(x),diff(df(x),x));
(%o17)  d2f(x):=2/(x+1)-(4*x)/(x+1)^2+(2*(x^2+8))/(x+1)^3
(%i18)  map(d2f,%o16);
(%o18)  [2/(x+1)-(4*x)/(x+1)^2+(2*(x^2+8))/(x+1)^3=-2/3,2/(x+1)-
(4*x)/(x+1)^2+(2*(x^2+8))/(x+1)^3=2/3]
```

Итак, получаем, что у исследуемой функции два экстремума - точка x = -4 – точка максимума, x = 2 – точка минимума.

Таким образом, были рассмотрены некоторые возможности применения СКА Maxima в процессе подготовки к ЕГЭ на примере решения отдельных типовых заданий по математике. Использование систем компьютерной алгебры на уроках способствуют более глубокому прорабатыванию материала [10]. У школьников появляется возможность проверить свои результаты, не прибегая к объемным вычислениям с использованием черновиков. Сочетая традиционную форму подготовки с применением компьютерных систем, мы получаем образование, которое идет в ногу с изменяющимися в мире запросами к школьникам.

Список используемой литературы

[1] Чичкарев Е.А. Компьютерная математика с Maxima Руководство для школьников и студентов // Москва: ALT Linux, 2009. - 233 с

[2] Стахин Н.А. Основы работы с системой аналитических (символьных) вычислений maxima // Учебное пособие. – Москва: 2008. — 86 с.

[3] Оленев А.А., Тынчеров К.Т., Селиванова М.В., Петрович М.П. Решение задач теории чисел в СКА MAXIMA // Материалы 45-й Международной научно-технической конференции молодых ученых, аспирантов и студентов: в 2-х т. / отв. ред. В.Ш. Мухаметшин. – Уфа: Изд-во УГНТУ, 2018. – Т. 1. – 470 с.

[4] Орлова Е.А., Севрюков П.Ф., Сидельникова В.И., Смоляков А.Н. Тренировочные тестовые задания по алгебре и началам анализа для учащихся 10-х и 11-х классов // Учебное пособие. Ставрополь, – М.: Илекса, 2011. – 160 с.

[5] Оленев А.А., Малиатаки В.В., Тынчеров К.Т., Селиванова М.В. Система компьютерной алгебры и элементарная теория чисел // Современные технологии в нефтегазовом деле – 2018: сборник трудов международной научно-технической конференции: в 2-х томах. 2018. – 293-300 с.

[6] Филиппова Н. В. Применение систем компьютерной математики и компьютерных технологий при изучении дисциплин высшей математики как один из видов педагогических технологий // Молодой ученый. — 2009. — №7. — С. 254-259.

[7] Виноградов И.М. Элементарная теория чисел / Математическая энциклопедия. М.: Советская энциклопедия, 1985. – 996 с.
[8] Зайцева Ж.И. Методика преподавания высшей математики с применением новых информационных технологий (в техническом вузе): дис. ... канд. пед. наук.: 13.00.02, 13.00.08; Елабуга, 2005. – 140 с
[9] Малиатаки В.В., Медведева Л.М., Оленев А.А. Совершенствование математической подготовки учителя в вузе на основе использования СКА Maple // Актуальные вопросы инженерного образования – 2015: Сборник научных трудов международной научно-методической конференции (Октябрьский, 27 ноября 2015 г.). Екатеринбург: Универсальная Типография «Альфа Принт», 2016. – С. 129-135.
[10] Халидова О.Х., Оленев А.А. Применение СКА Maple на примере изучения основ «Теории чисел» // Международный студенческий научный вестник. – 2018. – № 6.;

List of references

[1] Chichkarev E.A. Computer Mathematics with Maxima Guide for schoolchildren and students // Moscow: ALT Linux, 2009. - 233 p.
[2] N. Stakhin Basics of working with the system of analytical (symbolic) calculations maxima // Study Guide. - Moscow: 2008. - 86 p.
[3] Olenev A.A., Tyncherov K.T., Selivanova M.V., Petrovich M.P. Solving the problems of number theory in SKA MAXIMA // Proceedings of the 45th International Scientific and Technical Conference of Young Scientists, Postgraduates and Students: in 2 volumes / resp. ed. V.Sh. Mukhametshin. - Ufa: Publishing house UGNTU, 2018. - T. 1. - 470 p.
[4] Orlova E.A., Sevryukov P.F., Sidelnikova V.I., Smolyakov A.N. Training tests on algebra and the beginnings of analysis for students in 10th and 11th grades // Study Guide. Stavropol, - Moscow: Ileksa, 2011. - 160 p.
[5] Olenev A.A., Maliataki V.V., Tyncherov K.T., Selivanova M.V. Computer algebra system and elementary number theory // Modern technologies in the oil and gas business - 2018: collection of works of the international scientific and technical conference: in 2 volumes. 2018. - 293-300 s.
[6] N. Filippova. Application of Computer Mathematics Systems and Computer Technologies in the Study of Higher Mathematics Subjects as One of the Types of Pedagogical Technologies // Young Scientist. - 2009. - №7. - p. 254-259.
[7] Vinogradov I.M. Elementary Number Theory / Mathematical Encyclopedia. M .: Soviet Encyclopedia, 1985. - 996 p.
[8] Zaitseva Zh.I. Methods of teaching higher mathematics using new information technologies (in a technical college): dis. ... Cand. ped. PhD .: 13.00.02, 13.00.08; Yelabuga, 2005. - 140 seconds

[9] Maliataki V.V., Medvedeva L.M., Olenev A.A. Improving the mathematical training of teachers in higher education through the use of SKA Maple // Actual issues of engineering education - 2015: Collection of scientific papers of the international scientific-methodical conference (October, November 27, 2015). Yekaterinburg: Alpha Print Universal Printing House, 2016. - P. 129-135.

[10] Khalidova O.Kh., Olenev A.A. The use of SKA Maple on the example of learning the basics of "Theory of Numbers" // International Student Scientific Bulletin. - 2018. - № 6.;

ОПЕРАЦИИ С ПОЛИНОМАМИ В СИСТЕМЕ КОМПЬЮТЕРНОЙ АЛГЕБРЫ MAPLE ДЛЯ УЧАЩИХСЯ СРЕДНЕЙ ШКОЛЫ

Халидова О.Х.
Ставропольский государственный педагогический институт,

г. Ставрополь, 355000, Российская Федерация
oxana795@yandex.ru

Оленев А.А.
Ставропольский государственный педагогический институт,

г. Ставрополь, 355000, Российская Федерация
кандидат технических наук, доцент
olenevalexandr@gmail.com

Аннотация

В данной работе рассматривается задача применения программного пакета Maple (система компьютерной алгебры) при разборе полиномов различных степеней. Важным моментом, на котором акцентируется внимание в данной статье, является применение различных функций для многочленов. Так как с появлением СКА меняются подходы и методы изложения материала, становится возможным преподносить учебный материал на более высоком уровне. Занятия проходят в более интересном и качественном формате, привлекают большее внимание учащихся. Программу Maple возможно использовать на разных уровнях обучения, таких как: начальное, среднее и даже высшее образование. Главное суметь правильно выбрать метод применения системы компьютерной алгебры и уровень сложности заданий. Использование такого программного пакета позволяет значительно увеличить интенсивность урока, весьма обогатить содержание предмета. Использование СМК Maple предполагает

развитие таких навыков у обучающихся, как формирование системы фундаментальных знаний, которые позволяют самостоятельно ориентироваться в быстротекущем потоке информации. Система компьютерной алгебры позволяет осуществлять самоконтроль посредством указания на ошибки учащегося. Следовательно, правильно подобранные методы обучения в сочетании с информационными технологиями позволяют достичь необходимого качественного уровня образованности обучающихся.

Abstract

In this paper, we consider the problem of using the Maple software package (computer algebra system) in the analysis of polynomials of various degrees. An important point, which focuses attention in this article, is the use of various functions for polynomials. Since with the advent of SKA, approaches and methods of presenting the material are changing, it becomes possible to present the training material at a higher level. Classes are held in a more interesting and high-quality format, attracting more attention of students. The Maple program can be used at different levels of education, such as primary, secondary and even higher education. The main thing is to be able to choose the right method of applying the computer algebra system and the level of difficulty of the tasks. The use of such a software package can significantly increase the intensity of the lesson, significantly enrich the content of the subject. The use of Maple QMS implies the development of such skills among students as the formation of a system of fundamental knowledge that allows them to independently navigate the rapid flow of information. The computer algebra system allows self-checking by pointing out student errors. Consequently, properly chosen teaching methods in combination with information technologies make it possible to achieve the required quality level of education of students.

Ключевые слова: система компьютерной алгебры, Maple, информатизация, обучение, полином, коэффициент, множители, степень и корни полинома.

Keywords: computer algebra system, Maple, informatization, learning, polynomial, coefficient, factors, degree and roots of a polynomial.

Так как за последнее десятилетие произошли серьезные изменения в плане усовершенствования информационных технологий, следовательно, образование также нуждается в информатизации. Усвоение и постоянное обновление компьютерных технологий становится необходимостью [6].

В процессе информатизации важное значение имеет правильно сделанный выбор наиболее эффективного программного обеспечения. В настоящее время существует огромное количество специальных программных средств математической направленности. Среди них выделяется система компьютерной алгебры (СКА) Maple, которая так же легко находит свое применение в системе среднего образования [7]. А целесообразность использования СКА на уроках совсем не вызывает сомнений. Главным вопросом становится выбор наиболее эффективного способа применения данной системы[11]. Примером может служить изучение полиномов, так как на их основе строятся решения многих математических задач школьного курса.

Полином – алгебраическое выражение, которое представляет собой конечную сумму одночленов, то есть чисел, переменных и их неотрицательных степеней.

Использование полиномов в школьной практике достаточно обширно. Полиномиальные уравнения являются центральным объектом изучения в школьной программе.

Основное достоинство полиномов определяется тем, что с помощью них возможно представление многих зависимостей, требующих только умения выполнять арифметические операции. Полиномы играют важную роль в изучении алгебраической геометрии, объектом которой являются множества решений систем многочленов.

Такие операции, как упрощение, разложение на множители, разложение по степеням, вычисление корней, оценка полинома легко реализовать при помощи системы компьютерной алгебры Maple.

Для того, чтобы выделить коэффициенты полинома применяется следующая команда[10]:

coeff(p,x) – определение коэффициента при *x* полинома *p.*

Существуют различные вариации данной команды [9]:

coeff(p.x.n) – коэффициент для члена со степенью *n*полинома*p.*

coeff(p.x) – возвращает полином, объединяя коэффициенты при степенях данной переменной.

coeff(p.x^n) – возвращает коэффициенты x^n полинома*p.*

Пример 1. Определить коэффициенты в полиноме$p = 78x^7 + 6x^4 + 2x^3 - 88x$ при переменной, используя СКА Maple:

$$> p := 78\cdot x^7 + 6\cdot x^4 + 2\cdot x^3 - 88\cdot x;$$
$$p := 78x^7 + 6x^4 + 2x^3 - 88x$$
$$> coeff(p, x, 3);$$
$$2$$
$$> coeffs(p);$$
$$78, 6, 2, -88$$

Рисунок 1. Определение коэффициентов в полиноме.

Степень полинома можно оценить с помощью таких команд:

degree(p.x) –команда, которая возвращает старшую степень полинома.

ldegree(p.x) – команда, определяющую низшую степень многочлена.

Пример 2. Определить высшую и низшую степень многочлена $p = 78x^7 + 6x^4 + 2x^3 - 88x$, используя СКА Maple [3]:

$$> p := 78\cdot x^7 + 6\cdot x^4 + 2\cdot x^3 - 88\cdot x;$$
$$p := 78x^7 + 6x^4 + 2x^3 - 88x$$
$$> degree(\mathrm{p}, x);$$
$$7$$
$$> ldegree(\mathrm{p}, x);$$
$$1$$

Рисунок 2. Определение высшей и низшей степени в полиноме.

Так как, полином может иметь как отрицательные, так и положительные целые степени при неизвестном, то данные команды возвращают такие числа [2].

Для определения того, возможно ли разложение многочлена на несокращаемые множители используют команду [5]:

*Пример 3.*Разложить на множители данный полином: $x^3 - 1$.

$$> factor(\mathrm{x}^3 - 1);$$
$$(x-1)\left(x^2 + x + 1\right)$$

Рисунок 3. Разложение полинома на множители.

Разложить полином по степеням позволяет такая команда:*Evala(AFactor(p))*[9];

Пример 4. Разложить полином $x^3 + 6x - 1$ по степеням.

$$> evala(AFactor(\mathrm{x}^3 + 6x - 1));$$
$$(x-1)\left(x - RootOf\left(\_Z^2 + \_Z + 1\right)\right)\left(x + 1 + RootOf\left(\_Z^2 + \_Z + 1\right)\right)$$

Рисунок 4. Разложение полинома по степеням.

Вычислить действительные и комплексные корни полиномов возможно, используя команду *solve(p,x)*. Данная функция возвращает список корней данного полинома одной переменной.

Пример 5. Вычислить корни данного полинома $p = x^2 - 54x + 6$:

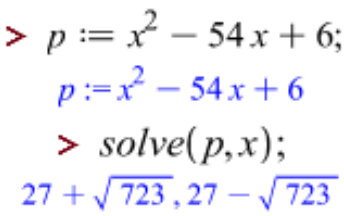

Рисунок 5. Вычисление корней полинома.

Пример 6. Найти корни многочленар $= \sqrt{2}x^3 - 3$:

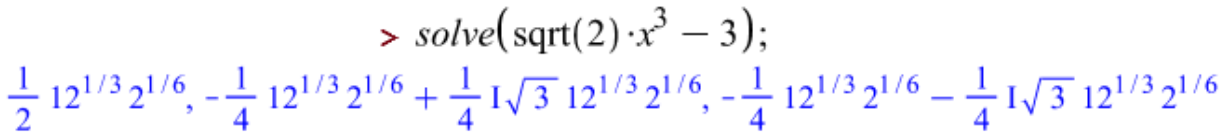

Рисунок 6. Корни многочлена из примера 6.

Пример 7. Найти решение данного уравнения $5x^3 - 8x^2 - 8x + 5 = 0$:

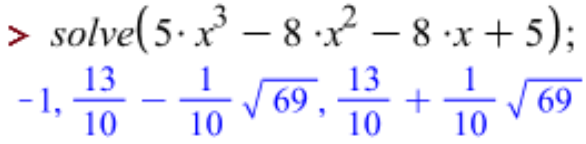

Рисунок 7. Решение уравнения из примера 7.

Для полиномов существуют еще такие функции [4]:

discrim(p, x) – отыскание дискриминанта полинома по данной переменной.

randpoly(x, eqns) – возвращение полинома, полученного случайным образом по данной переменной, где *eqns* – максимальная степень многочлена.

Результат команды *randpoly(x, eqns)* всегда случаен, следовательно, повторение практически не реально.

Пример 8. Получить случайным образом полином с максимальной степенью 8, найти дискриминант [1].

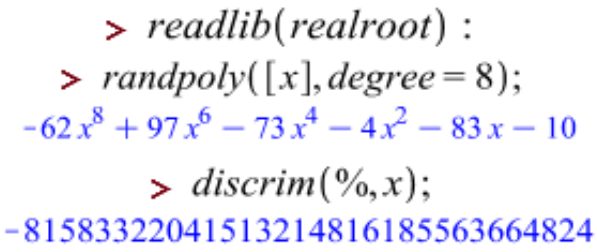

Рисунок 8. Решение 8 примера.

Важно обратить внимание на то, что для использования некоторых команд в Maple нужно вызывать их из стандартной библиотеки [8].

Образование выступает в роли системы, которая формирует необходимый уровень знаний, позволяющий быть самостоятельным в выборе необходимой информации. Образование в настоящее время предполагает также развитие критического, рационального

мышления учащихся, способных на реализацию творческих идей. На мой взгляд, система компьютерной алгебры Maple вполне справляется с задачей помощника при развитии таких умений у обучающихся.

Список используемой литературы:

[1] Алексеев, Е. Р. Решение задач вычислительной математики в пакетах Mathcad 12, MATLAB 7, Maple 9 [Текст] / Е. Р. Алексеев, О. В. Чеснокова. – М.: НТ Пресс, 2006. – 496 с.

[2] Васильев А. Н. Maple 8. Самоучитель, М.: Диалектика, Вильямс, 2003. – 352 с.

[3] Виноградов И.М. Элементарная теория чисел / Математическая энциклопедия. М.: Советская энциклопедия, 1985. – 996 с.

[4] Говорухин В.Н., Цибулин В.Г. Введение в Maple. Математический пакет для всех. Мир.1997. – 208 с.

[5] Дьяконов В.П. Maple 7. Учебный курс. СПб.: Питер, 2002. – 672 с.

[6] Зайцева Ж.И. Методика преподавания высшей математики с применением новых информационных технологий (в техническом вузе): дис. канд. пед. наук.: 13.00.02, 13.00.08; Елабуга, 2005. –140 с.

[7] Малиатаки В.В., Медведева Л.М., Оленев А.А. Совершенствование математической подготовки учителя в вузе на основе использования СКА Maple // Актуальные вопросы инженерного образования – 2015: Сборник научных трудов международной научно-методической конференции (Октябрьский, 27 ноября 2015 г.). Екатеринбург: Универсальная Типография «Альфа Принт», 2016. – С. 129-135.

[8] Оленев А.А., Малиатаки В.В. Моделирование логических элементов и простейших узлов ЭВМ в системе компьютерной математики Maple // Информатика в школе.2017. №8(131). С. 58-63.

[9] Оленев А.А., Малиатаки В.В., Тынчеров К.Т., Селиванова М.В. [Текст] Система компьютерной алгебры и элементарная теория чисел // Современные технологии в нефтегазовом деле –2018: сборник трудов международной научно-технической конференции: в 2-х томах. 2018. – С. 293-300.

[10] Прохоров Г., Леденев М, Колбеев В. Пакет символьных вычислений Maple. М: Компания Петит, – 1997. – 198 с.

[11] Халидова О.Х., Оленев А.А. Применение СКА Maple на примере изучения основ «Теории чисел» // Международный студенческий научный вестник. – 2018. – №6.; URL: http://eduherald.ru/ru/article/view?id=19243 (дата обращения: 27.11.2018).

List of references:

[1] Alekseev, E.R. Solving problems of computational mathematics in Mathcad 12 packages, MATLAB 7, Maple 9 [Text] / E. R. Alekseev, OV Chesnokova. – M.: NT Press, 2006. – 496 p.

[2] Vasilyev A.N. Maple 8. Tutorial, M.: Dialectics, Williams, 2003. – 352 p.
[3] Vinogradov I.M. Elementary Number Theory / Mathematical Encyclopedia. M .: Soviet Encyclopedia, 1985. –996 p.
[4] Govorukhin V.N., Tsybulin V.G. Introduction to Maple. A math package for everyone. Mir.1997. – 208 p.
[5] Dyakonov V.P. Maple 7. Training course. SPb.: Peter, 2002. – 672 p.
[6] ZaitsevaZh.I. Methods of teaching higher mathematics using new information technologies (in a technical college): dis. ... Cand. ped. Ph.D.: 13.00.02, 13.00.08; Yelabuga, 2005. – 140 p.
[7] Maliataki V.V., Medvedeva L.M., Olenev A.A. Improving the mathematical preparation of teachers in high school based on the use of SKA Maple // Actual issues of engineering education - 2015: Collection of scientific papers of the international scientific-methodical conference (October, November 27, 2015). Yekaterinburg: Alpha Print Universal Printing House, 2016. - P. 129-135.
[8] Olenev A.A., Maliataki V.V. Simulation of logical elements and simplest computer nodes in the system of computer mathematics Maple // Informatics at school.2017. No. 8 (131). Pp. 58-63.
[9] Olenev A.A., Maliataki V.V., Tyncherov K.T., Selivanova M.V. [Text] Computer algebra system and elementary number theory // Modern technologies in oil and gas business – 2018: collection of works of the international scientific and technical conference: in 2 volumes. 2018. – p. 293-300.
[10] Prokhorov G., Ledenev M., Kolbeev V. A package of symbolic Maple computations. M: PetitCompany, – 1997. – 198 p.
[11] Khalidova, O.Kh., Olenev, A.A. APPLICATION OF SKA MAPLE ON THE EXAMPLE OF STUDYINGTHE BASIS "THE THEORY OF NUMBERS" // International Student Scientific Journal. - 2018. - № 6.; URL: http://eduherald.ru/ru/article/view?id=19243 (appeal date: 11/27/2018).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПОДГОТОВКЕ К ОГЭ ПО ИНФОРМАТИКЕ

Лайпанова Д. М. [1]
dinara.laypanova@gmail.com

Шевченко Г. И. [2]
кандидат педагогических наук, доцент
shgaiv@yandex.ru

СКФУ, г. Ставрополь, 355029, Россия[1]
СКФУ, г. Ставрополь, 355029, Россия[2]

Аннотация

Использование информационных и коммуникативных технологий является необходимым в современном образовательном процессе. Они используются очень активно, как педагогами, так и обучающимися. В плане подготовки к ОГЭ информационные и коммуникационные технологии выступают одним из важнейших звеньев, существенно дополняя широкий спектр других образовательных технологий. Использование информационных и коммуникативных технологий универсально, оно уместно при организации самых разных форм образовательной деятельности. В статье рассматриваются виды и роль этих технологий при подготовке обучающихся к ОГЭ по информатике, уделяется внимание тем технологиям, которые мало рассматриваются при подготовке к государственному экзамену. Раскрываются особенности применения наиболее эффективных сайтов, программ и социальных сетей для подготовки к аттестации.

Abstract

The use of information and communication technologies is essential in the modern educational process. They are used very actively, both by teachers and students. In terms of preparing for the

OGE, information and communication technologies are one of the most important links, significantly complementing a wide range of other educational technologies. The use of information and communication technologies is universal, it is appropriate in the organization of various forms of educational activities. The article discusses the types and role of these technologies in preparing students for the OGE in computer science, focuses on those technologies that are little considered in preparing for the state exam. Discloses the features of the use of the most effective sites, programs and social networks to prepare for certification.

Ключевые слова: информационные и коммуникационные технологии (ИКТ), учащиеся, учитель, ОГЭ, государственный экзамен, преподаватель, информатика, подготовка, результат.

Keywords: information and communication technologies (ICT), students, teacher, OGE, state exam, teacher, computer science, training, result.

Одной из особенностей распределенного изучения возможностей применения средств информационных и коммуникативных технологий (ИКТ) в процессе освоения различных предметных областей, является осуществление учебной деятельности с использованием средств ИКТ в процессе освоения содержательных линий изучения конкретного общеобразовательного или учебного предмета. С помощью средств ИКТ осуществляется взаимодействие между преподавателем и обучаемым в современных открытых и дистанционных системах образования. Поэтому современный преподаватель должен не только иметь представление об ИКТ, но и активно использовать их в своей педагогической деятельности [2].

В настоящий момент, значительной проблемой в обучении школьников является подготовка и сдача экзаменов по окончанию 9-го класса. Результаты этих экзаменов принято считать успешностью педагогического труда, основой при комплектовании профильных классов в старшей школе, а также при поступлении в учреждения системы среднего профессионального образования [4,5]. Это говорит о том, что подготовку следует начинать заранее, с каждым обучающимся индивидуально, осуществлять ее системно, применяя различные организационные формы обучения: работа в парах, в группах и т. п.

В связи с этим учителю информатики предстоит решить ряд задач [1], а именно:

- подготовить обучающихся так, чтобы они смогли жить и трудиться в условиях информационного общества и продолжать образование в течение всей жизни;
- подготовить обучающихся к ОГЭ, основной целью которого является получение объективной оценки, отражающей качество подготовки выпускников основной школы

Традиционные методы для подготовки хорошо отработаны и привычны для обучающихся, но они не всегда подходят для дифференцированной и индивидуальной работы с каждым из них. Возникает вопрос: что делать в данной ситуации учителю, как решить проблему?

Для решения этой проблемы в настоящее время существуют различные виды информационных технологий, которые могут успешно использоваться при подготовке обучающихся как к основному государственному экзамену по информатике, так и по другим предметам. Примером таких технологий является:

- сайт Федерального института педагогических измерений «ФИПИ»;
- программа «Skype»;
- обучающая система Дмитрия Гущина «Решу ОГЭ»;
- сервис «YouTube»;
- социальная сеть «Вконтакте»;
- сайт «ЭкзаменRU» и др.

Использование их при подготовке к экзамену является наиболее удобным как для преподавателя, так и для обучающихся. Остановимся коротко на каждой технологии.

На сайте Федерального института педагогических измерений (ФИПИ) возможно провести онлайн тестирование обучающихся и сразу по полученным результатам провести анализ выполненных работ, также на сайте представлены демоверсии контрольно-измерительных материалов, также возможно задавать вопросы, на которые регулярно отвечают администраторы портала. (Рис. 1.)

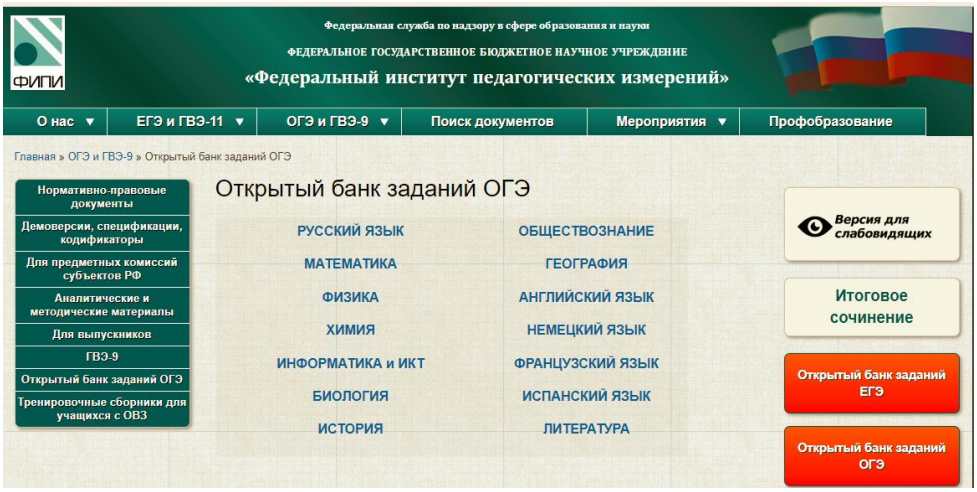

Рисунок 1. Сайт «Федеральный институт педагогических измерений»

С помощью программы «Skype» (Рис. 2.) преподаватель и обучающиеся могут осуществлять подготовку к ОГЭ, находясь вне образовательной организации. Это особенно актуально, если ученик отсутствует по причине болезни или же, когда образовательная организация находится на карантине.

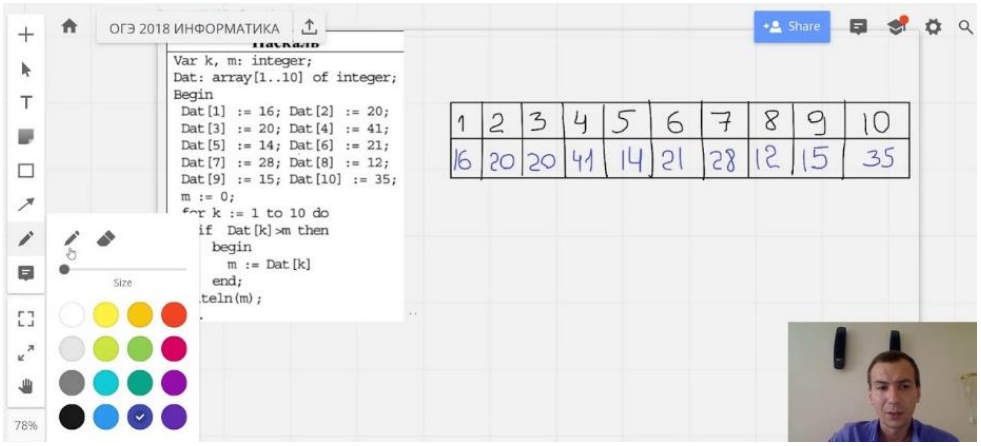

Рисунок 2. Программа « Skype».

Благодаря обучающей системе Дмитрия Гущина «Решу ОГЭ» ученик может самостоятельно осуществлять подготовку к ОГЭ, результаты которой учитель может увидеть после ее выполнения (Рис. 3).

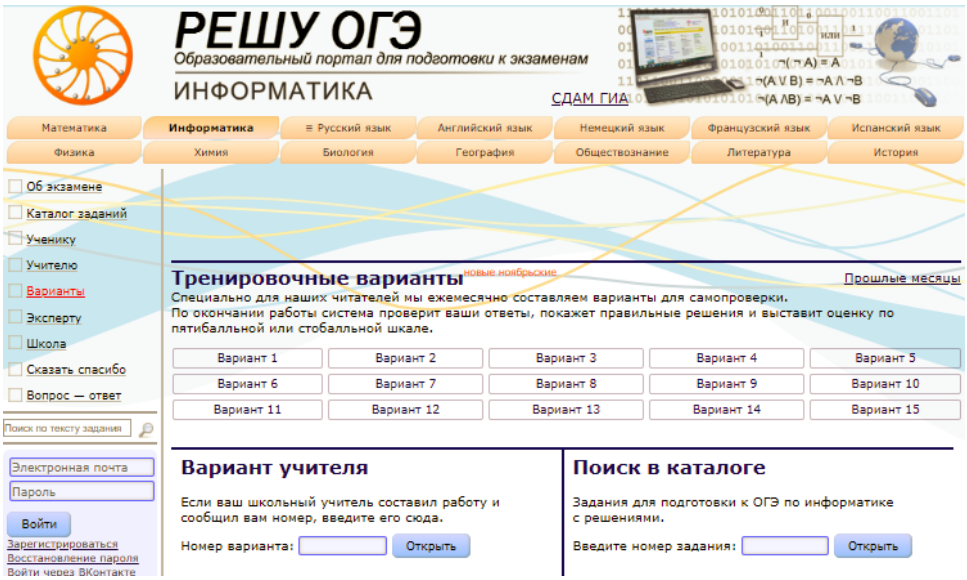

Рисунок 3. Сайт «Решу ОГЭ»

В сервисе «YouTube» можно найти множество различных видеоматериалов (видеоблогов Рис. 4.) с подробным разбором заданий ОГЭ по информатике.

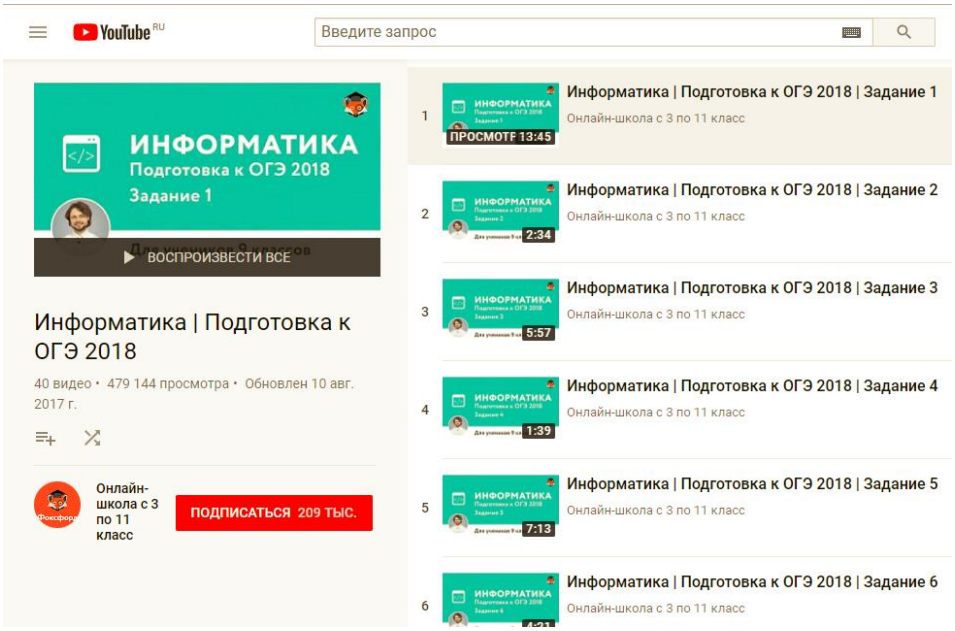

Рисунок 4. Сервис «YouTube».

При помощи социальной сети «Вконтакте» (Рис. 5.), есть множество групп по онлайн подготовке к итоговой аттестации также преподаватель может создать группу или беседу, в которой он и обучающиеся смогут обсуждать различные вопросы при подготовке к ОГЭ.

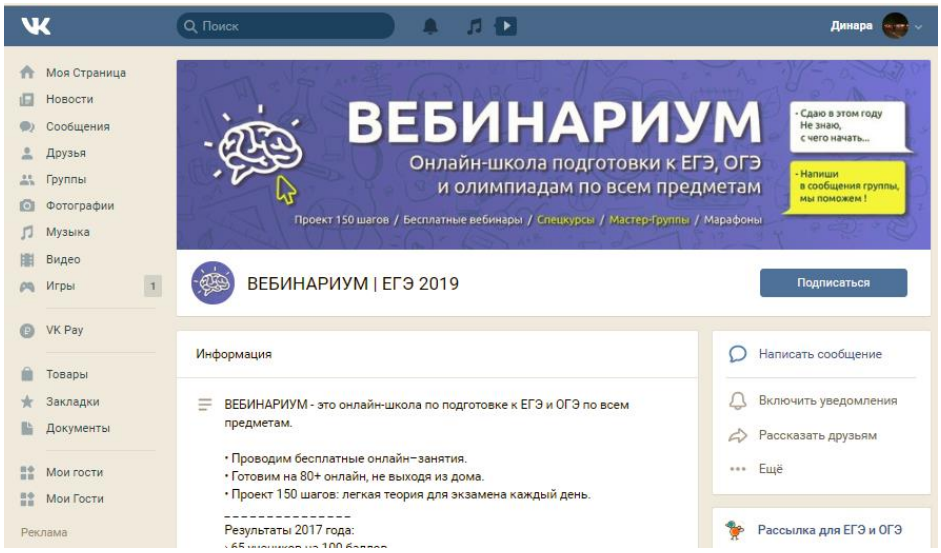

Рисунок 5. Социальная сеть «Вконтакте».

ЭкзаменRU – портал для выпускников и их родителей (Рис. 6). Здесь возможно найти информацию о государственных экзаменах, порешать бесплатные онлайн-тесты ОГЭ практически по всем предметам и ответы с решениями, узнать о системах обучения в разных странах, стипендиях и возможностях бюджетного обучения. Также размещены тесты для профориентации.

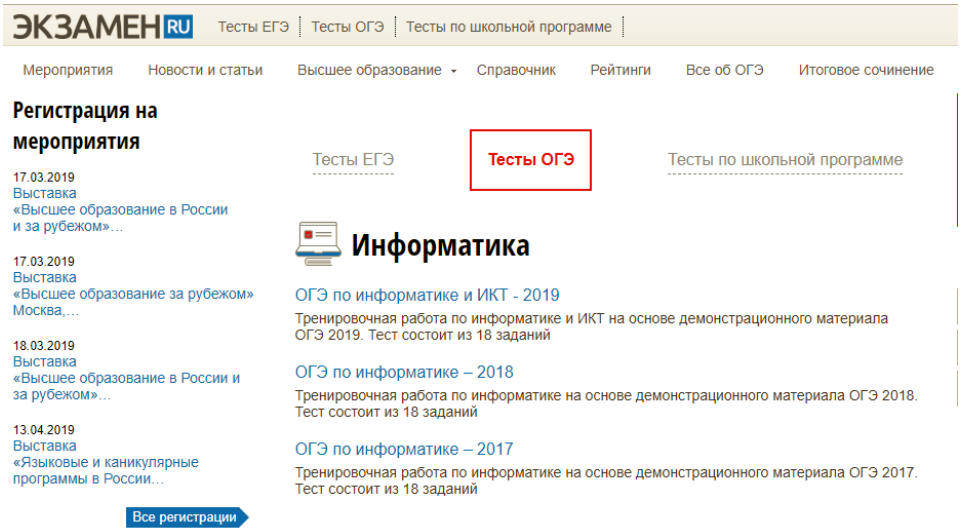

Рисунок 6. Сайт «ЭкзаменRu»

Материал хорошо усваивается обучающимися и может быть достойным рефлексивным фактором занятий при подготовке к ОГЭ. Подготовка обучающихся к итоговой аттестации в форме ОГЭ дает хороший результат лишь при системном подходе к данному вопросу. ИКТ являются неотъемлемым инструментом в достижении этой цели при правильном применении их в образовательном процессе.

Подобных программ, используемых при подготовке к ОГЭ с каждым днем, становится все больше. Обучающиеся теперь могут получать помощь преподавателя, не выходя из дома. Подобные виды ИКТ позволяют развивать у обучающихся мобильность, адаптивность, самостоятельность, повышать уровень их само образованности. Но для большего успеха обучающиеся должны быть готовы осваивать передовые способы деятельности, в том числе адекватные новым средствам ИКТ.

Обобщая вышесказанное можно утверждать, что ИКТ является неотъемлемой частью подготовки обучающихся к ОГЭ. Их использование возможно в разных формах и на разных стадиях образовательной деятельности. ИКТ дают возможность выстроить собственную траекторию обучения, сделать совместные занятия учителя и учеников более эффективными, добиться высоких образовательных результатов, и в конечном итоге успешно пройти ОГЭ.

Список используемой литературы

[1] Роберт И.В. Распределенное изучение информационных и коммуникационных технологий в общеобразовательных предметах // Информатика и образование. – 2001. – №5.

[2] Шевченко Г.И. Информационная культура преподавателя вуза в контексте его управленческой деятельности //Информатика и образование. 2011. № 8 (226). С. 83-85

[3] Поддубная Н. А., Куликова Т. А. Средства информационных и коммуникационных технологии в совершенствовании профессиональной подготовки будущего учителя-предметника Стандарты и мониторинг в образовании. – 2014. – №3. – 91-97 с.

[4] Шевченко Г.И., Куликова Т.А., Рыбакова А.А. Методика обучения и воспитания информатике. Учебное пособие. – Ставрополь: Изд-во СКФУ, 2017. – 172 с.

[5] Яковлев А.И. Информационные и коммуникационные технологии в образовании. 2009 [Электронный ресурс]. – Режим доступа: http://www.infsoft.itais.ru/index.php/ittech/71-konsult.

[6] Чернова Е.В., Боброва И.И., Мовчан И.Н., Трофимов Е.Г., Зеркина Н.Н., Чусавитина Г.Н. Обучение учителей по предотвращению отклонения поведения учащихся в ИКТ / В сборнике: Материалы конференции по информационным технологиям 2016. – 294-297 с.

[7] Шевченко Г.И. Основы Интернет-технологий. Учебно-методическое пособие (в помощь учителю предметнику) / – Ставрополь: Изд-во СГУ, 2006. – 246 с.

[8] Гохберг Г.С. Информационные технологии / Г.С. Гохберг, А.В. Зафиевский, А.А. Короткин. – М., 2004. – 208 с.

List of references

[1] Robert I.B. *Raspredelennoye izucheniye informatsionnykh i kommunikatsionnykh tekhnologiy v obshcheobrazovatel'nykh predmetakh* // Informatika i obrazovaniye. – 2001. – №5. (In Russian)

[2] Shevchenko G.I. *Informatsionnaya kul'tura prepodavatelya vuza v kontekste yego upravlencheskoy deyatel'nosti //Informatika i obrazovaniye*. 2011. № 8 (226). S. 83-85 (In Russian)

[3] Poddubnaya H. A., Kulikova T. A. *Sredstva informatsionnykh i kommunikatsion-nykh tekhnologii v sovershenstvovanii professional'noy podgotovki budushchego uchitelya-predmetnika Standarty i monitoring v obrazovanii*. – 2014. – №3. – 91-97 c. (In Russian)

[4] Shevchenko G.I., Kulikova T.A., Rybakova A.A. *Metodika obucheniya i vospitaniya informatike. Uchebnoye posobiye*. – Stavropol': Izd-vo CKFU, 2017. – 172 c. (In Russian)

[5] Yakovlev A.I. *Informatsionnyye i kommunikatsionnyye tekhnologii v obrazova-nii.* 2009 [Elektronnyy resurs]. – Rezhim dostupa: http://www.infsoft.itais.ru/index.php/ittech/71-konsult. (In Russian)

[6] Chernova E.B., Bobrova I.I., Movchan I.H., Trofimov E.G., Zerkina H.H., Chusavi-tina G.H. *Obucheniye uchiteley po predotvrashcheniyu otkloneniya povedeniya ucha-shchikhsya v IKT / B sbornike: Materialy konferentsii po informatsionnym tekh-nologiyam* 2016. – 294-297 c. (In Russian)

[7] Shevchenko G.I. *Osnovy Internet-tekhnologiy. Uchebno-metodicheskoye posobiye (v pomoshch' uchitelyu predmetniku)* / – Stavropol': Izd-vo CGU, 2006. – 246 c.

[8] Gokhberg G.C. *Informatsionnyye tekhnologii* / G.C. Gokhberg, A.B. Zafiyevskiy, A.A. Korotkin. – M., 2004. – 208 s. (In Russian)

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ В УЧЕБНОМ ПРОЦЕССЕ

Джанибекова К.Р.[1]
d.kamila.r24@gmail.com

Шевченко Г.И.[2]
доцент
shgaiv@yandex.ru

[1]Северо-Кавказский федеральный университет, Ставрополь, 355029, Россия

[2]Северо-Кавказский федеральный университет, Ставрополь, 355029, Россия

Аннотация

Актуальность выбранной темы исследования обусловлена тем, что информационные технологии являются одной из наиболее значимых частей концепции модернизации образования. В статье проанализированы возможности использования технологии компьютерного тестирования в учебном процессе, рассмотрены функциональные возможности программы MyTest и разработан компьютерный тест. Авторы приходят к выводу, что использование технологии компьютерного тестирования в учебной деятельности рано или поздно станет массовым, обыденным явлением, которое предоставит преподавателям и обучаемым новые возможности и преимущества.

Abstract

The relevance of the chosen research topic is due to the fact that information technologies are one of the most significant parts of the concept of the modernization of education. The article ana-

lyzes the possibility of using computer testing technology in the educational process, discusses the functionality of the program MyTest and developed a computer test. The authors conclude that the use of computer testing technology in learning activities will sooner or later become a mass, everyday phenomenon that will provide teachers and learners with new opportunities and benefits.

Ключевые слова: Информационные технологии, тест, компьютерное тестирование, контроль знаний, программа MyTest.

Keywords: Information technology, test, computer testing, knowledge control, MyTest program.

Использование в современной системе образования информационных и коммуникационных технологий открывает новые возможности в организации учебного процесса, способствует развитию творческих способностей обучающихся, позволяет педагогу гораздо эффективнее управлять процессом обучения, использовать различные способы представления учебной информации [1, 2].

Компьютер является и источником знаний, и наглядным пособием, и тренажером, и средством оценки и контроля. Чтобы обучающиеся смогли успешно освоить изучаемый материал, учителю необходимо следить за возникающими трудностями и своевременно предотвращать их. Для получения более объективной и полной картины об освоении изучаемого материала учитель может применить технологию компьютерного тестирования (ТКТ). Для обучающегося немаловажно то, что сразу после прохождения теста он получает объективный результат с указанием ошибок. Бесспорным достоинством тестирования является возможность выбора уровня сложности задания для конкретного ученика, а также возможность раскрепостить обучающихся при ответе на вопросы, так как при прохождении компьютерного тестирования (КТ), ученикам никто не делает замечание, никто не смеется над их неверным ответом. Тесты можно применять с различной целью: для проверки домашнего задания, усвоении нового материала, а также при закреплении пройденного. Еще одним значительным достоинством является то, что выставление оценок не зависит от личных отношений учителя к ученику и всегда объективно [3,5].

Использование КТ предоставляет прекрасную возможность для самостоятельной творческой и практической деятельности обучающихся, что содействует пониманию учениками учебного процесса, достижению больших результатов в общем развитии учеников различных уровней, формированию их познавательной активности. Плюсом такой формы контроля является возможность его применения не только на уроке, но и при дистанционном обучении или самостоятельной работе обучающихся, что, несомненно, развивает их творческую активность. Помимо выше сказанных плюсов КТ следует отметить, что использование теста в

процессе обучения способствует хорошему накапливанию оценок и снижает объём бумажной работы. Отметим также и недостатки КТ:

- вероятность выбора ответа наугад;
- проверка только результатов и невозможность проследить логику рассуждений учеников;
- замедление тестирования из-за технических сбоев;
- отсутствие обратной связи и наводящих вопросов, позволяющих «вытянуть» ученика.

При выборе КТ результативным считается разработка собственных тестов, при создании которых возможен самостоятельный выбор назначения и формы теста, прогнозирование результата [4].

Однако, нередко педагоги, разрабатывающие КТ, сталкиваются с трудностями, связанными с их созданием.

Одним из способов решения данной проблемы, может служить использование для разработки КТ различных программных средств, обладающих интуитивно понятным интерфейсом и широким спектром функциональных возможностей.

Подобных программных средств существует множество: MultiTester, UniTest System, RichTest, PikaTest, MyTest.

Среди всех этих программ, можно отметить свободно распространяемую программу MyTest, автором которой является А.С. Башлаков.

Рассмотрим возможности этой программы и этапы разработки теста в ней[7].

Программа содержит в себе следующие части-модули: редактор тестов, журнал тестирования и модуль тестирования.

С помощью Модуля Редактора тестов можно свободно добавлять и модифицировать варианты ответов и вопросы, также есть возможность изменять количество правильных ответов и число тестовых вопросов.

Модуль тестирования предусмотрен для выполнения теста.

Модуль Журнал тестирования дает возможность отправлять тесты благодаря компьютерной сети, а также результаты тестирования можно обрабатывать в виде таблицы и получать их централизованно. Преподаватель может изучить полученные результаты и сохранить их в документ.

Программа MyTest функционирует со следующими видами тестовых заданий: множественный выбор, одиночный выбор, установление соответствия, установление порядка следования, ручной ввод текста, ручной ввод чисел, выбор места на изображении, заполнение пропусков. Для всех заданий имеется возможность установления уровня сложности, объяснение точного решения и закрепление подсказки.

Благодаря всем возможностям этой программы можно разрабатывать самостоятельные, обучающие, диагностирующие тесты по информатике для всех обучающихся, а также для старшеклассников при подготовке к выпускным экзаменам.

Разработаем в программе MyTest тест для 7 класса по информатике на тему «Компьютер как универсальное устройство для работы с информацией».

Чтобы запустить программу MyTest для прохождения теста нужно нажать на кнопки «Тест → Начать». Дальше необходимо написать свои данные, чтобы учитель мог получить результат каждого ученика.

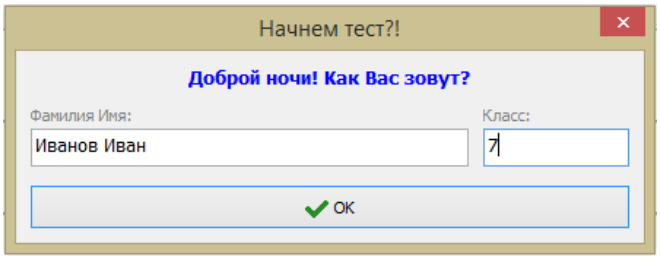

Рисунок 1- Ввод данных

В разработанном тесте содержатся разные формы тестовых заданий. В задании с выбором одного правильного ответа главный текст дан в виде утверждения. Ниже предоставляются варианты ответов, в которых все неверные, кроме 1-го верного.

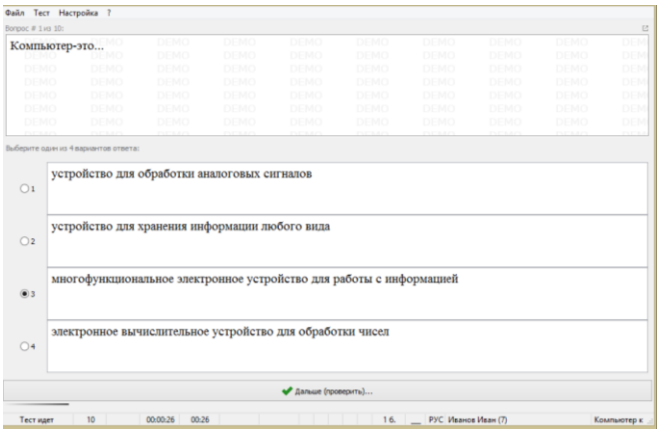

Рисунок 2- Пример тестового задания с выбором 1-го верного ответа

Задания, в которых содержится только один правильным ответ считается более легким, чем задания с несколькими верными ответами.

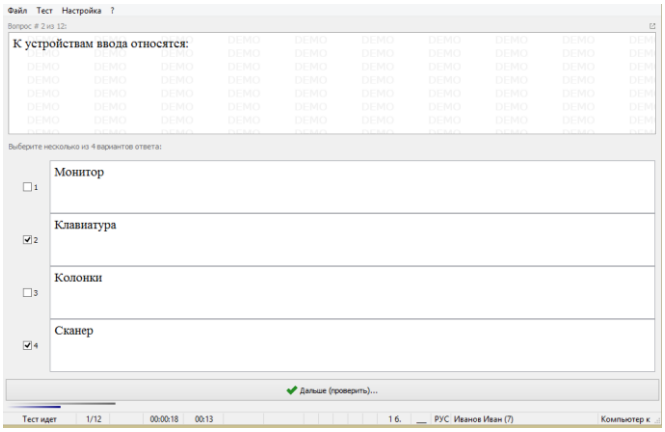

Рисунок 3-Пример тестового задания с выбором нескольких верных ответов

В тестовых заданиях на соответствие, обучающемуся предлагается установить соответствие между устройством компьютера и его свойством, представленных в двух колонках.

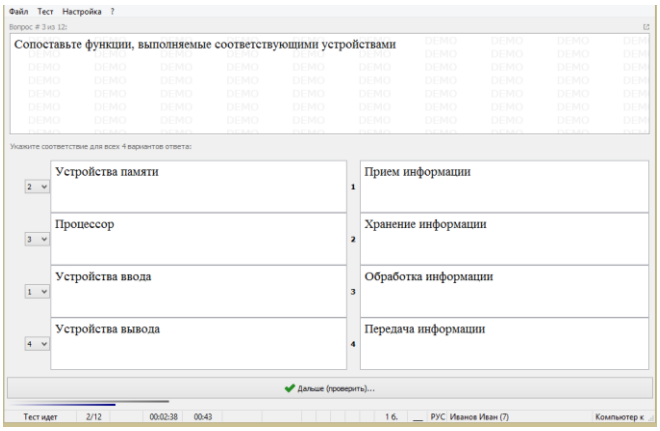

Рисунок 4- Пример тестового задания на установление соответствия

До проверки теста, у испытуемого есть возможность вернуться к заданиям, в которых он не уверен, и еще раз попытаться выбрать верный вариант. По окончанию тестирования ученик может ознакомиться с результатом, перейти в любое задание и сравнить его результат с полученным верным ответом.

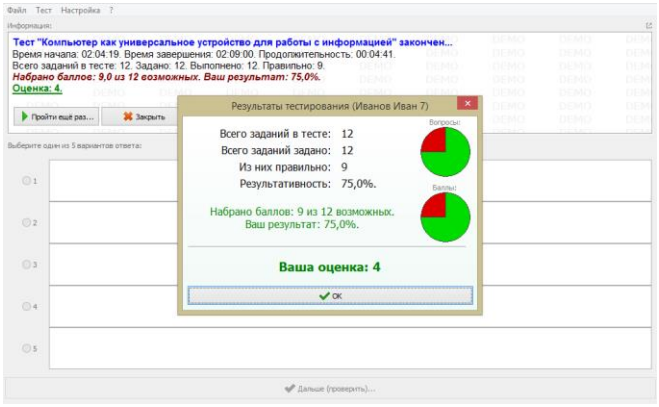

Рисунок 5-Результаты тестирования

Тест, разработанный в данной программе, обладает простым интерфейсом, для всех учеников единые требования при проведении тестовой аттестации и понятные толкования итогов, минимизация времени на проверку и диагностика достижений. Программа MyTest поможет с помощью тестирования выявить качество учебных достижений обучающихся [6].

В заключении необходимо отметить, что использование в учебном процессе ТКТ дает возможность за короткий промежуток времени закрепить изученный материал; провести анализ результатов тестирования; возвратиться к выполненному заданию и устранить неточности.

Такая форма контроля позволит ученику получить результат сразу после прохождения теста, а не через определенное время, когда уже отметка для него утрачивает свою актуальность. При верном выборе материала, тест можно применять как для обучения, так и для контроля. И существенным, является то, что обучающийся получает возможность обнаружить пробелы в своих знаниях и принять меры для их ликвидации. Поэтому использование ТКТ в образовательном процессе должно стать массовым, обыденным явлением, благодаря которому в современной школе можно будет решить множество проблем [8].

Список используемой литературы

[1] Джанибекова К.Р. Использование онлайн-сервисов для визуализации учебной информации// Студенческая наука для развития информационного общества: сборник материалов VI Всероссийской научно-технической конференции: в 2-х томах. Т.1. – Ставрополь: Изд-во СКФУ, 2017. – 323 с.

[2] Шевченко Г.И. **С**редства методического сопровождения учебной деятельности студентов в электронной информационно-образовательной среде //Мир науки, культуры, образования. 2015. № 3 (52). С. 195-197.

[3] Джанибекова К.Р. Применение технических средств мультимедиа в современном образовании // Студенческая наука для развития информационного общества: сборник материалов V Всероссийской научно-технической конференции: в 2-х томах. Т.1. – Ставрополь: Изд-во СКФУ, 2016. – 624 с.

[4] Звонников В.И. Современные средства оценивания результатов обучения: учебное пособие для студентов высших учебных заведений. М.: Издательский центр «Академия», 2012. 224 с.
[5] Дьячук П.П. Динамическое компьютерное тестирование. Педагогическая информатика, № 3, 2005, - с.3-9
[6] Сиврук А.И., Папко Т.П. Автоматизация подготовки тестовых заданий. Педагогическая информатика, № 2, 2003, - с.43-49
[7] Пачурин Г.В., Тюмина Н.С., Шевченко С.М. Анализ тестирования как средства контроля знаний обучающихся // Современные проблемы науки и образования. – 2017.
[8] Шевченко Г.И. Инновационность отечественного образования и новые проблемы педагогического менеджмента //Стандарты и мониторинг в образовании. 2012. № 6. С. 21-24.

List of references

[1] Dzhanibekova K.R. Ispol'zovaniye onlayn-servisov dlya vizualizatsii uchebnoy informatsii// Studencheskaya nauka dlya razvitiya informatsionnogo obshchestva: sbornik materialov VI Vserossiyskoy nauchno-tekhnicheskoy konferentsii: v 2-kh tomakh. T.1. – Stavropol': Izd-vo CKFU, 2017. – 323 c.
[2] Shevchenko G.I. Sredstva metodicheskogo soprovozhdeniya uchebnoy deyatel'nosti studentov v elektronnoy informatsionno-obrazovatel'noy srede //Mir nauki, kul'tury, obrazovaniya. 2015. № 3 (52). S. 195-197.
[3] Dzhanibekova K.R. Primeneniye tekhnicheskikh sredstv mul'timedia v sovremennom obrazovanii // Studencheskaya nauka dlya razvitiya informatsionnogo obshchestva: sbornik materialov V Vserossiyskoy nauchno-tekhnicheskoy konferentsii: v 2-kh tomakh. T.1. – Stavropol': Izd-vo CKFU, 2016. – 624 c.
[4] Zvonnikov B.I. Sovremennyye sredstva otsenivaniya rezul'tatov obucheniya: uchebnoye posobiye dlya studentov vysshikh uchebnykh zavedeniy. M.: Izdatel'skiy tsentr «Akademiya», 2012. 224 c.
[5] D'yachuk P.P. Dinamicheskoye komp'yuternoye testirovaniye. Pedagogicheskaya informatika, № 3, 2005, - s.3-9
[6] Sivruk A.I., Papko T.P. Avtomatizatsiya podgotovki testovykh zadaniy. Pedagogicheskaya informatika, № 2, 2003, - c.43-49
[7] Pachurin G.B., Tyumina N.C., Shevchenko C.M. Analiz testirovaniya kak sredstva kontrolya znaniy obuchayushchikhsya // Sovremennyye problemy nauki i obrazovaniya. – 2017.
[8] Shevchenko G.I. Innovatsionnost' otechestvennogo obrazovaniya i novyye problemy pedagogicheskogo menedzhmenta //Standarty i monitoring v obrazovanii. 2012. № 6. S. 21-24.

ЭЛЕКТИВНЫЕ КУРСЫ, КАК СПОСОБ ПРОФИЛЬНО-ДИФФЕРЕНЦИРОВАННОГО ОБУЧЕНИЯ ИНФОРМАТИКЕ

Шевелева М.С.

bluzmarina@yandex.ru

Руководитель – кандидат пед. наук, доцент Г.И. Шевченко

shgaiv@yandex.ru

[1] Северо-Кавказский Федеральный Университет, г. Ставрополь 355000 Россия

Аннотация

В статье обращается внимание на то, что элективные курсы обеспечивают углубленное изучение предмета, повышают качество знаний, заинтересованность обучающихся и ориентированность на подготовку к профессиональному образованию. Инновационные процессы в современной школе актуализируют проблему совершенствования методики обучения информатике, направленную на личностное развитие ребенка. Наиболее эффективно эти процессы протекают при использовании элективных курсов, как способа дифференциации учебного содержания информатики, определяющего содержание программы, образовательные потребности, индивидуальные способности и возможности обучающегося. Использование элективных курсов, способствует созданию такой модели обучения, которая образовательную деятельность ученика не замыкает на учебной деятельности, включая синтез, все виды и формы социальной и культурной деятельности, превращает в образовательный опыт разносторонний индивидуальный опыт, получаемый в школе и в социуме.

Abstract

The article draws attention to the fact that elective courses provide in-depth study of the subject, improve the quality of knowledge, interest of students and focus on training for vocational education. Innovative processes in modern school actualize the problem of improving methods of teaching computer science, aimed at the personal development of the child. These processes are most effective when using elective courses as a way to differentiate the educational content of Informatics, which determines the content of the program, educational needs, individual abilities and capabilities of the student. The use of elective courses, contributes to the creation of a model of learning that educational activities of the student is not confined to educational activities, including synthesis, all types and forms of social and cultural activities, turns into an educational experience versatile individual experience obtained in school and in society.

Ключевые слова: элективные курсы; профильное обучение; дифференциация, информатика, информационные технологии.

Keywords: elective courses; vocational training; differentiation, informatics, information technologies.

Современное общество, стратегическим ресурсом которого является интеллектуальное развитие его членов, предъявляет к ним новые образовательные требования, направленные не на усвоение определенной суммы знаний, а на формирование познавательных и созидательных способностей. В связи с этим на старшей ступени общеобразовательной школы к обучению подходят дифференцированно. Поскольку дифференциация обучения – важная задача современной школы, направленная на осознание, исследование и принятие жизненных ценностей, смыслов, позволяющих ориентироваться в нравственных нормах и правилах, выработку своей жизненной позиции по отношению к миру, окружающим людям, самому себе и своему будущему.

В настоящее время принято различать:

- уровневую дифференциацию, которая учитывает современные результаты и достижения методической науки, и основывается на планировании результатов обучения, т.е. явном выделении уровня обязательной подготовки и формирования на этой основе более высоких уровней овладения материалом;
- профильную дифференциацию – это дифференциация по содержанию, предполагающая обучение разных групп школьников по программам,

отличающимися глубиной и визуализацией изложения материала, объемом сведений и т.д.

Одним из предметов, в которых дифференциация обучения реализуется наиболее естественным образом, является информатика. Однако истинная дифференциация школьного предмета «Информатика» связана не с методическими различиями в изложении одного и того материала, как в базовом курсе, а с действительными различиями в содержании дифференцированных курсов, способствующих ориентации обучающихся на будущую профессию и выбор профиля дальнейшего обучения.

Дифференциация учебного содержания, в частности, введение обязательных курсов по выбору обучающихся, стало основным изменением, которое смогло бы создать условия для ориентации на индивидуальные потребности школьника. Каждый из этих курсов освещает намеченные, но совершенно не проработанные в общем курсе вопросы, необходимые каждому ученику. Они учитывают гибкость, интересы и способности обучающихся в соответствии с их намерениями в отношении направлений продолжения образования и выбора жизненного пути; способствуют не только выработке умений и закреплению уже имеющихся навыков, но и формированию устойчивого интереса обучающихся к процессу и содержанию деятельности.

Дифференциации учебного содержания информатики позволяет по сути создавать уникальную информационно-образовательную среду, которая соответствует требованиям образовательных стандартов нового поколения. При этом обучение строится на принципах, благодаря которым достигается понимание и признание личности ученика. Принципы, реализуемые в информационных технологиях, основаны на знаниях и умениях обучающегося основной школы, которые были сформированы при изучении обязательного общеобразовательного предмета «Информатика».

Цели и задачи профильно-дифференцированных курсов информатики способствуют учету интересов каждого из обучающихся; учитывают направленность допрофессиональной подготовки; способствуют формированию основ научного мировоззрения и развитию мышления; готовят обучающихся к практическому труду и продолжению образования.

По содержанию выделяют фундаментальные и прикладные профильно-дифференцированные курсы. Для фундаментальных курсов ведущей функцией является формирование научного мировоззрения, а для прикладных – подготовка к практической деятельности.

Сегодня компьютерная графика становится такой областью в курсе информатики, которая охватывает все формы и виды представления изображений. Умение работать с компьютерной графикой становится важной частью информационной грамотности обучающегося, ведь в его распоряжении не только изображения на экране монитора, но и большое количество изображений полученных с помощью цифровых фотоаппаратов, Web-камер, сканеров.

Мотивацией к изучению становится возможность приобретения умений и навыков работы в графических редакторах, обработки изображений. Знания, умения, навыки, способы деятельности, сформированные у школьников при его изучении, будут востребованы не

только в выбранной ими последующей профессиональной деятельности, но уже и в школе. К этому относятся и углубление профессиональной ориентации обучающихся, и удовлетворение их интересов в областях знаний, которые не имеют непосредственного отношения к профилю класса, в котором обучается школьник.

Используя информационные технологии, учитель имеет возможность широко применить методы активного, дифференцированного обучения.

Для организации углубленного изучения средств графической обработки информации нами был разработан элективный курс, за основу которого была взята коллекция изображений на основе спутниковых данных дистанционного зондирования Земли для учреждений общего и среднего профессионального образования Российской Федерации. Коллекция спутниковых снимков Земли широко используется для изучения базовых, элективных и профильных курсов и организации внеурочной деятельности. Размещенные в коллекции спутниковые данные и результаты их тематических обработок демонстрируют глобальные, региональные и локальные явления и объекты природного и антропогенного характера.

Разработанный элективный курс отличает широта и востребованность его образовательных результатов. Поскольку сбор данных остается трудоемкой операцией, а Интернет развивается очень быстро, обновление данных в реальном времени имеет все основания стать популярным решением в проекте GIS.

Планируемые образовательные результаты, после изучения элективного курса, должны отвечать следующим требованиям:

1. Обучающиеся должны знать:

– основы применения и использования компьютерной графики;

– особенности, достоинства и недостатки растровой и векторной графики;

– способы получения спутниковых снимков;

– способы хранения растровых и векторных изображений;

– способы хранения изображений файлов в специальных форматах спутниковых снимков;

– методы сжатия графических данных;

– проблемы преобразования форматов графических файлов;

– назначение и функции различных программ для отображения спутниковой информации и цифровых карт.

2. В результате освоения практической части элективного курса, обучающиеся должны уметь:

– монтировать цифровые карты, снимки, фотографии;

– создавать многослойные документы;

– получать данные на основе цифровых карт и спутниковых снимков;

– использовать методики расчетов в практических работах элективного курса.

В отличие от существующих разработок, элективный курс имеет выраженную практическую направленность, является расширением и углублением имеющихся знаний по

компьютерной графике. Апробация разработанного курса осуществлялась в МБОУ лицее №35 г. Ставрополя в профильном 10 «В» классе с углубленным изучением математики и информатики. Навыки, полученные при выполнении практических работ общего назначения, использовались практически на каждом уроке, во время проведения практической части.

Опыт профильно-дифференцированного обучения информатике показал, что дифференциация обеспечивает свободу личности обучаемого, в выборе предметов и углубления в изучении отдельных тем, способствует подготовке будущего выпускника к высококвалифицированной социальной и профессиональной деятельности в современных условиях. Решение проблемы дифференциации содержания обучения во многом сопутствует развитию системы образования и переходу ее на качественно новый уровень.

Список используемой литературы

[1] Белонова Г.Р. / Учитель Башкортостана [Текст] / Белонова Г.Р. // – Предпрофильная подготовка учащихся основной школы. – 2006. – №2.-с. 83–87.

[2] Блужин С.Б. Элективный курс «Спутниковые снимки Земли» как метапредмет. Инновации в общем и профессиональном образовании: опыт, проблемы, перспективы: материалы 55-й научно-методической конференции преподавателей и студентов Ставропольского университета «Университетская наука региону», СГУ, Ставрополь, 2010

[3] Егорова А. М. Профильное обучение и элективные курсы в средней школе [Текст] // Теория и практика образования в современном мире: материалы Междунар. науч. конф. (г. Санкт-Петербург, февраль 2012 г.). – СПб.: Реноме, 2012 – С. 173-179. – URL https://moluch.ru/conf/ped/archive/21/1617/ (дата обращения: 25.11.2018).

[4] Кассанс Т. КНИГА Над Землей: ошеломляющие спутниковые снимки Земли. Магма . 2005 г.

[5] Могилев А.В., Пак Н.И., Хеннер Е.К./ Информатика [Текст] / Могилев А.В., Пак Н.И., Хеннер Е.К – М: Академия, 2003. -809.

[6] Шевелева М.С. Роль элективных курсов в профильном обучении. Развитие современного образования: от теории к практике Материалы V Международной научно-практической конференции. Редкол.: О.Н. Широков [и др.].. 2018 Издательство: Общество с ограниченной ответственностью "Центр научного сотрудничества "Интерактив плюс" (Чебоксары).

[7] Шевелева М.С. Элективные курсы в системе профильного обучения информатике и ИКТ. Студенческая наука для развития информационного общества: сборник материалов VII Всероссийской научно-технической конференции. – Ставрополь. Издательство СКФУ, 2018 г. – 544 с.

[8] Шевченко Г.И., Куликова Т.А., Рыбакова А.А. Методика обучения и воспитания информатики: Учебное пособие [Текст] / Шевченко Г.И., Куликова Т.А., Рыбакова А.А.. – Ставрополь: Изд-во СКФУ, 2017. – 172 с.

[9] Шевченко. Г.И. Построение школьного курса информатики, ориентированного на технические приложения при дифференцированном обучении. Автореферат диссертации на соискание ученой степени кандидата педагогических наук / Московский государственный открытый педагогический университет. Москва, 1997.

List of references

[1] Belanova G. R. / Teacher of Bashkortostan[Text] / G. R. Belanova // – Preprofile preparation of pupils of the primary school. - 2006. - №2.- p. 83-87.

[2] Bluzhin S. B. Elective course "Satellite images of the Earth" as MetaFrame. Innovations in General and professional education: experience, problems, prospects: materials of the 55th scientific-methodical conference of teachers and students of Stavropol University "University science in the region", SSU, Stavropol, 2010

[3] Egorova M. Profile training and elective courses in high school [Text] / / Theory and practice of education in the modern world: materials international. scientific. Conf. (St. Petersburg, February 2012). – SPb.: Renome, 2012-P. 173-179. URL https://moluch.ru/conf/ped/archive/21/1617/ (accessed: 25.11.2018).

[4] Cassens So the BOOK is Above the Earth: stunning satellite images of Earth. Magma. 2005.

[5] Mogilev V. A., Pak N. And. Henner E. K./ Computer Science [Text] / Mogilev V. A., Pak N. And. Henner E. K. – M: Academy, 2003. -809.

[6] Pobedonostseva, M. G. system of elective courses in Informatics at the senior level of secondary school [Text] / / Informatics and education. - 2008. - № 10. - p. 25-28.

[7] Sheveleva M. S. the role of elective courses in profile training. Development of modern education: from theory to practice Materials of the V International scientific-practical conference. Redkol.: O. N. Shirokov [et al.].. 2018 Publisher: limited liability Company "center for scientific cooperation "Interactive plus" (Cheboksary).

[8] Sheveleva M. S. Elective courses in the system of specialized training in Informatics and ICT. Student science for the development of information society: collection of materials VII all-Russian scientific and technical conference. – Stavropol. Publisher SKFU, 2018 – 544 with

[9] Shevchenko G.I., Kulikova T.A., Rybakova A.A. Metodika obucheniya i vospitaniya informatiki: Uchebnoye posobiye [Tekst] / Shevchenko G.I., Kulikova T.A., Rybakova A.A.. – Stavropol': Izd-vo SKFU, 2017. – 172 s.

[10] Shevchenko. G. I. Building a school course in computer science, focused on technical applications in differentiated education. Thesis abstract for the degree of candidate of pedagogical Sciences / Moscow state open pedagogical University. Moscow, 1997.

Научное издание

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Сборник материалов IX Всероссийской
научно-технической конференции
(г. Ставрополь, 19–21 декабря 2018 года)
Часть 2

Материалы изложены в авторской редакции
на CD-диске в формате PDF