Российский фонд фундаментальных исследований (РФФИ) Южный Федеральный университет Сочинский государственный университет

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И КОМПЬЮТЕРНЫХ СЕТЕЙ

Материалы
12-й Международной научной конференции
(SIN 2019)
(12-15 сентября 2019 г., Сочи, Россия)

Сочи - РИЦ ФГБОУ ВО «СГУ» - 2019

УДК 51
ББК 22.12
Б40

Печатается по решению Ученого совета
инженерно-экологического факультета
Сочинского государственного университета
(протокол № 1 от 09.09.2019 года)

Ответственные редакторы:
кандидат физико-математических наук, доцент
Сочинского государственного университета
А.Р. Симонян
кандидат технических наук, доцент,
Сочинского государственного университета
Ю.И. Дрейзис
кандидат технических наук, доцент
Южного Федерального университета
М.В. Аникеев
доктор технических наук, профессор
Южного Федерального университета
Л.К. Бабенко
доктор технических наук, профессор Аксарайского университета Турции
Atilla Elci

Б40 Безопасность информации и компьютерных сетей (SIN 2019): материалы 12-й Междунар. науч. конф. 12-15 сентября 2019 г., Сочи, Россия. − Сочи: РИЦ ФГБОУ ВО «СГУ», 2019 – 94 с. (яз.: рус., англ.)

ISBN 978-5-88702-636-7

Мероприятие проводилось при финансовой поддержке Российского фонда фундаментальных исследований и Администрации Краснодарского края, проект № 19-47-231001.

Представлены результаты научных исследований молодых ученых, подготовленные в рамках 12-й Международной научной конференции по безопасности информации и компьютерных сетей (SIN 2019)

Предназначены для студентов, магистрантов, аспирантов, преподавателей, ученых, занимающихся исследо-ваниями в различных областях защиты информации, информационной безопасности и безопасности компьютер-ных сетей.

ISBN 978-5-88702-636-7

УДК 51
ББК 22.12

Научное издание

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И КОМПЬЮТЕРНЫХ СЕТЕЙ (SIN 2019)

Материалы
12-й Международной научной конференции (**SIN 2019**), 12-15 сентября 2019 г., Сочи, Россия

В авторской редакции

Подписано в печать 09.07.2019.
Формат 29,7 × 42/4. Бумага офсетная.
Печать трафаретная. Гарнитура Times New Roman.
Уч.-изд. л. 2,0. Усл. печ. л. 2,3.
Тираж 50 экз.
354003, г. Сочи, ул. Пластунская, 94. Тел. 268-25-73.
Отпечатано с готового оригинал-макета в типографии РИЦ ФГБОУ ВО «СГУ».
354003, г. Сочи, ул. Пластунская, 94.

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ К СБОРНИКУ ТРУДОВ КОНФЕРЕНЦИИ

Юрий Дрейзис, Арсен Симонян
кафедра информационных технологий
кафедра прикладной математики и информатики
Сочинский государственный университет, Сочи
Yurid206@yandex.ru, oppm@mail.ru

Быстрый рост глобальной сети Интернет и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Новые технологические возможности облегчают распространение информации, повышают эффек-тивность производственных процессов, способствуют расширению деловых от-ношений.

Однако несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса.

В настоящее время информацию следует рассматривать как важнейший стратегический ресурс, как товар, поэтому при наиболее общем подходе к вопро-сам защищенности информационных процессов можно сказать, что нанесение ущерба информации относится к материальным затратам либо напрямую, либо опосредованно. Здесь может идти речь о раскрытии секретов не только сферы государственных интересов, систем военного ведомства, но и уникальных про-мышленных технологий, о потере рынков сбыта в силу утраты конкурентоспо-собности, сохранности конфиденциальных данных потребителя, нарушении бан-ковской тайны и т.д.

Другим аспектом служит представление информации как важнейшего субъекта систем принятия решений или субъекта управления. И с этой точки зрения, особенно в системах реального времени, таких как производственные технологические системы, обеспечение транспортных перевозок и движения, искажение или утрата информации может привести к катастрофическим последствиям не только в объектах управления, но и представлять угрозу человеческим жизням.

Современное понимание процессов обработки информации требует рассматривать информацию как важнейшую часть информационных технологий, и обеспечение безопасности информации является специфическим аспектом этих технологий. Поскольку эта сфера научно-практической деятельности в настоя-щее время развивается наиболее динамично, возможные решения в области обеспечения безопасности не должны быть частными или узконаправленными, как

обучающие методики, учебные курсы или программно-технические изделия. Требуются механизмы новаторских решений, позволяющие адекватно реагировать на вызовы информационной безопасности, уметь предвидеть новые угрозы и уметь им противостоять.

Широта охвата сферы информатизации показывает, что для разных категорий субъектов характер решаемых задач по обеспечению информационной безопасности может существенно различаться.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития ИТ.

В прошедшие годы общими тенденциями стали: непрерывные, иногда суще-ственные, изменения в спектре интернет-угроз; увеличение количества и разно-видностей вредоносных программ и их усложнение; варьирование тактики и рас-ширение арсенала используемых технологий и инструментов кибератак и инци-дентов информационной безопасности.

За последние годы заметно возросло число угроз, направленных на мобильные платформы. Подтверждением тому, что мобильным устройствам все больше внимания уделяют как специалисты по безопасности, так и киберпреступники, стал резкий рост числа уязвимостей, обнаруженных в мобильных операционных системах.

Появление большого количества новых мобильных платформ в сочетании с пониженным уровнем внимания к вопросам безопасности и нехваткой средств защиты мобильных устройств позволяет предположить, что киберпреступники начнут атаковать мобильные устройства путем заражения их бот-сетями.

Одновременно социальные сети стали использоваться злоумышленниками как платформы для распространения атак, а блогосфера — как привлекательная мишень для кибератак.

Популярность социальных сетей продолжает расти, и создатели вредоносных программ все чаще стали использовать «социальную тактику».

Интернет сегодня — это технология, кардинально меняющая весь уклад нашей жизни: темпы научно-технического прогресса, характер работы, способы общения. Эффективное применение информационных технологий является общепризнанным стратегическим фактором роста конкурентоспособности компании. Многие предприятия в мире переходят к использованию широких возможностей Интернета и электронного бизнеса, неотъемлемый элемент которого — электронные транзакции (по Интернету и другим публичным сетям).

Электронная коммерция, продажа информации в режиме on-line и многие другие услуги становятся основными видами деятельности для многих компа-

ний, а их корпоративные информационные системы (КИС) — главным инструментом управления бизнесом и, фактически, важнейшим средством производства.

Важным фактором, влияющим на развитие КИС предприятия, является поддержание массовых и разнообразных связей предприятия через Интернет с одновременным обеспечением безопасности этих коммуникаций. Поэтому решение проблем информационной безопасности, связанных с широким распростране-нием Internet, Intranet и Extranet — одна из самых актуальных задач, стоящих пе-ред разработчиками и поставщиками информационных технологий.

Задача обеспечения информационной безопасности КИС традиционно решается построением системы информационной безопасности (СИБ), определяю-щим требованием к которой является сохранение вложенных в построение КИС инвестиций. Иначе говоря, СИБ должна функционировать абсолютно прозрачно для уже существующих в КИС приложений и быть полностью совместимой с ис-пользуемыми в КИС сетевыми технологиями.

Создаваемая СИБ предприятия должна учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к любым элементам КИС.

Применение информационных технологий (ИТ) требует повышенного внимания к вопросам информационной безопасности. Разрушение информацион-ного ресурса, его временная недоступность или несанкционированное использо-вание могут нанести компании значительный материальный ущерб. Без должной степени защиты информации внедрение ИТ может оказаться экономически не-выгодным в результате значительных потерь конфиденциальных данных, храня-щихся и обрабатываемых в компьютерных сетях.

Реализация решений, обеспечивающих безопасность информационных ресурсов, существенно повышает эффективность всего процесса информатизации в организации, обеспечивая целостность, подлинность и конфиденциальность до-рогостоящей деловой информации, циркулирующей в локальных и глобальной информационных средах.

Исходя из сказанного, следует принимать во внимание два важнейших заме-чания:

• в зависимости от сферы деятельности, назначения информационных систем и используемых информационных технологий задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

• информационную безопасность следует рассматривать как интегрированный показатель и обобщенное понятие, которое не может быть сведено только лишь к защите от неправомерного доступа или обеспечению компьютерной безопасности.

12-й Международная научная конференции по безопасности информации и

компьютерных сетей (SIN 2019) проходила с 12 по 15 сентября 2019 г. в г. Сочи под эгидой Российского Фонда фундаментальных исследований.

Результаты представленных исследований направлены на анализ методов противодействия сбору информации с сайтов и обхода такого противодействия, системам передачи конфиденциальной информации по принципу технологии VLC, системам анализа и верификации индикаторов компрометации (IoC), про-блемам безопасности работы современных роботов, анализ и обнаружения ки-бер-физических угроз и неинформационного воздействия на системы группового управления роботами, реализации криптографических протоколов на основе ди-намического анализа информации с помощью различных протоколов и инстру-ментов, интеллектуальным системам защиты информации, технологиям глубо-кой проверки пакетов для распознавания и блокировки трафиков сетей, исследо-ваниям алгоритмов анализа шифров и многим другим проблемам информацион-ной безопасности и безопасности компьютерных сетей.

Результаты студенческих научных исследований в различных областях за-щиты информации и компьютерных сетей были представлены на 12-й Междуна-родной научной конференции по безопасности информации и компьютерных се-тей (SIN 2019) при финансовой поддержке Российского фонда фундаментальных исследований и Администрации Краснодарского края, проект № 19-47-231001.

Международная конференция была направлена также на популяризацию, продвижение и поощрение инновационной деятельности среди студентов, имею-щих инновационные разработки и идеи в области информационной безопасно-сти, защиты информации и компьютерных сетей, а также на помощь в разработке и реализации собственных нововведений студентов.

Участие в Международной научной конференции (SIN 2019) позволили во-влечь студентов в научно-исследовательскую деятельность в области информа-ционной безопасности, защиты информации, безопасности компьютерных сетей.

Проведение конференции также способствовало развитию научно-техниче-ского направления, реализуемого вузами и научными организациями в области информационной безопасности.

PREFACE TO THE WORK OF THE CONFERENCE

Yuriy Dreizis, Arsen Simonian
Department of Information Technology
Department of Applied Mathematics and Computer Science
Sochi State University, Sochi
Yurid206@yandex.ru, oppm@mail.ru

The rapid growth of the global Internet and the rapid development of information technologies have led to the creation of an information environment that affects all spheres of human activity. New technological capabilities facilitate the dissemination of information, increase the efficiency of production processes and contribute to the expansion of business relations.

However, despite the intensive development of computer tools and information technologies, the vulnerability of modern information systems and computer networks unfortunately does not decrease. Therefore, information security issues attract the attention of both computer system and network professionals and numerous users, including e-business companies.

At present, information should be considered as a critical strategic resource, as a commodity, so with the most general approach to the security of information processes, it can be said that damaging information refers to material costs either directly or indi-rectly. This may include the disclosure of secrets not only in the sphere of state interests, military systems, but also in unique industrial technologies, the loss of markets due to the loss of competitiveness, the preservation of confidential consumer data, the viola-tion of bank secrecy, etc.

Another aspect is the presentation of information as an essential subject of decision-making systems or a subject of management. From this perspective, especially in real-time systems such as manufacturing technology systems, transport and traffic, dis-tortion or loss of information can have catastrophic consequences not only in manage-ment facilities but also as a threat to human lives.

Today's understanding of information processing processes requires that information be seen as an essential part of information technology, and ensuring information security is a specific aspect of these technologies. Since this area of scientific and practical activity is currently developing most dynamically, possible security solutions should not be private or highly focused, such as training techniques, training courses or software and technology products. Innovative solutions are needed to respond ade-quately to the challenges of information security, to anticipate and confront new threats.

The breadth of the scope of informatization shows that for different categories of subjects, the nature of the information security tasks to be solved may differ significantly.

Modern methods of processing, transmitting and storing information have contrib-uted to threats related to the possibility of loss, distortion and disclosure of data ad-dressed to or owned by end users. Therefore, ensuring information security of computer systems and networks is one of the leading directions of IT development.

Over the years, common trends have been: continuous, sometimes significant, changes in the spectrum of Internet threats; increasing the number and complexity of malware; varying tactics and expanding the range of technologies and tools used for cyber-attacks and information security incidents.

Threats to mobile platforms have increased markedly in recent years. The fact that mobile devices are increasingly being paid attention by both security professionals and cyber criminals was confirmed by the sharp increase in the number of vulnerabilities found in mobile operating systems.

The emergence of a large number of new mobile platforms, with a reduced focus on security and a lack of mobile security tools, suggested that cyber criminals would attack mobile devices by infecting their botnets.

At the same time, social networks began to be used by attackers as platforms for spreading attacks, and the blogosphere as an attractive target for cyber-attacks.

The popularity of social media continues to grow, and malware creators have in-creasingly used «social tactics».

The Internet today is a technology that fundamentally changes the entire way of our lives: the pace of scientific and technological progress, the nature of work, the ways of communication. Effective application of information technologies is a recognized strategic factor of the company's competitiveness growth. Many businesses around the world are moving to take advantage of the Internet and e-business, an integral part of which is electronic transactions (over the Internet and other public networks).

E-commerce, on-line sales and many other services are becoming the main activ-ities of many companies, and their corporate information systems (CIS) are the main tool for business management and, in fact, the most important means of production.

An important factor affecting the development of the CIS of the enterprise is the maintenance of mass and diverse communications of the enterprise via the Internet while ensuring the security of these communications. Therefore, solving information security problems related to the wide distribution of Internet, Intranet and Extranet is one of the most pressing tasks facing developers and suppliers of information technol-ogy.

The task of ensuring information security of CIS has traditionally been solved by the construction of an information security system (IRB), the defining requirement of which is the preservation of investments invested in the construction of CIS. In other words, the IRB should be completely transparent to existing applications in the CIS and be fully compatible with the network technologies used in the CIS.

The enterprise's IRB should take into account the emergence of new technologies and services, as well as meet the general requirements today for any elements of the

CIS.

The use of information technology (IT) requires increased attention to information security issues. The destruction of an information resource, its temporary un-availabil-ity or unauthorized use can cause significant material damage to the company. Without a proper degree of information protection, IT implementation can be economically un-economical as a result of significant losses of sensitive data stored and processed in computer networks.

The implementation of solutions that ensure the security of information resources significantly improves the efficiency of the entire informatization process in the organ-ization, ensuring the integrity, authenticity and consistency of expensive business in-formation circulating in local and global information environments.

On that basis, two important points should be taken into account:

• Depending on the field of activity, the purpose of information systems and the information technologies used, the tasks of ensuring information security for different categories of entities may differ significantly;

• Information security should be considered as an integrated indicator and a generic concept that cannot be reduced merely to protection against illegal access or com-puter security.

The 12th International Scientific Conference on Security of Information and Com-puter Networks (SIN 2019) was held from September 12 to September 15, 2019 in Sochi under the auspices of the Russian Foundation for Fundamental Research.

The materials of the conference present student, master and postgraduate works of representatives of universities and scientific centers of different regions of Russia, as well as works from foreign countries.

The results of the presented studies are aimed at analysis of methods of counteracting the collection of information from sites and circumventing such interaction, systems of transmitting confidential information on the principle of VLC technology, systems of analysis and verification of compromise indicators (IoC), problems of safety of modern robots operation, analysis and detection of cyber-physical threats and non-informational impact on systems of group control of robots, Implementing cryptographic protocols based on dynamic analysis of information using various protocols and tools, Intelligent information protection systems, deep packet inspection technologies to recognize and block network traffic, Research into encryption analysis algorithms and many other problems of information security and computer network security.

The results of student scientific research in various fields of information protection and computer networks were presented at the 12th International Scientific Conference on Information Security and Computer Networks (SIN 2019) with the financial support of the Russian Foundation for Fundamental Research and the Administration of Kras-nodar Territory, Project No. 19-47-231001.

The international conference was directed also to promoting, advance and encour-

agement of innovative activity among the students, graduate students and young scien-tists having innovative developments and the ideas in the field of information security, information security and computer networks, and also to the aid in development and realization of own innovations of students and young scientists.

Participation in the International Scientific Conference (SIN 2019) allowed to involve students in research activities in the field of information security, information protection, and security of computer networks.

The conference also contributed to the development of scientific and technical di-rection implemented by universities and scientific organizations in the field of infor-mation security

THE USING OF PREDICTIVE ANALYTICS METHODS IN THE TASK OF SECURITY ANALYSIS OF SMART-CARDS WITH SOFTWARE AND HARDWARE COMPLEX

Alexander Ananyev
Department of Information Technology Security,
South Federal University, Taganrog, Russian Federation
a.ananev@outlook.com
Oleg Makarevich
Department of Information Technology Security
South Federal University, Taganrog, Russia
mak@tsure.ru
Dmitry Bespalov
Department of Computer Engineering,
South Federal University, Taganrog, Russia
bda82@mail.ru

ABSTRACT

This paper presents the results of the study of the developed method to optimize the process of analyzing the security of modern microprocessor plastic cards using predictive Analytics. In the course of the study, a method was developed to reliably determine the beginning of the desired phase of the algorithm inside the plastic card for further application of the power attack. The developed algorithm can significantly reduce the overhead costs of experimental studies and more accurately apply the effects on the power supply chains by detecting the phases of the algorithms with timely preparation of further actions on the part of the equipment. Tests were carried out based on the developed software and hardware complex of research of protection of microprocessor plastic cards and the available measuring equipment. The use of this method has improved the temporal accuracy of the effects by 15%, reducing the number of iterations of the study.

KEYWORDS

Microprocessor plastic card, Hardware and software system, Predictive analytics, Signal, Algorithm, Method, Research.

1 INTRODUCTION

Currently, there is an acute problem of studying the security of microprocessor systems, individual chips and plastic cards in particular from the destructive effects of the environment and from targeted attacks of intruders. Microprocessor-based cards are often attacked at various levels for the purpose of destruction, unauthorized withdrawal of funds and obtaining personal data of the owner. Such attacks are often reproduced

both on the software and on the physical (hardware) level. At the same time, the effects performed at the hardware level, that is, at the level of electrical signals, are the most dangerous, since they imply direct and unlimited access to the resources of the device.

Most of these attacks are made at the power circuits, can identify the algorithms that are currently running inside the microprocessor core, and may purposefully cause crashes, and interferes with the operation of these algorithms, such as the generation of «null» passwords, wipe information from the internal memory or overwriting of files with encryption keys and passwords.

2 NEED AND PURPOSE OF WORK

This work is relevant, as it allows conducting comprehensive studies of the security of microprocessor elements and plastic cards [1], to determine their degree of protection against various threats, as well as to build other comprehensive research methods in this area.

The aim of this work is to create a universal method to solve the following problems:

- determination of the beginning of the characteristic phases in the algorithms inside the microprocessor core by changes in the power consumption signals in the power supply circuits (power profile);
- primary classification profile of the signal in the neighborhood of the predicted phrases to increase the likelihood of the recognition performed by the algorithm inside the microprocessor in the conditions of a priori uncertainty;
- optimization of the research process of the microprocessor or plastic card in terms of accuracy in the time of application of various effects/

3 THEORETICAL INTRODUCTION

It is known that the most effective methods of carrying out attacks on microprocessor devices and plastic cards are simple attacks on energy consumption and differential attacks on energy consumption [2]. Such attacks are carried out by the researcher mainly by means of visual analysis of the dependence of the power consumption of the device on time. Specific phases of algorithms and their stages (phrases) are formed by the power profile, which depends on the type of operations performed by the microprocessor and their duration. At the same time, various microprocessors and plastic cards can have some variability in the form of signals in the power supply chain, which complicates the use of classical methods of signal analysis and increases the amount of work of the researcher. Often, tens and hundreds of simple launches of the analyzed algorithm and the selection of the place of the impact precede the moment of application of the analyzing influence.

The algorithms used by the authors to analyze the security of microprocessors and microprocessor plastic cards belong to the class of high-order differential power attacks

[3], and therefore require the use of special tools and instruments for their implementation.

In the course of the work previously performed by the authors, a hardware-software complex was formed, consisting of a specialized software shell in C# language, which allows to execute scripts in LUA language, which allow to work with an external hardware platform, intercept event triggers in the analyzed device, form impact templates and load them into a free-form digital signal generator and, finally, perform these actions with the subsequent interception of signal profiles using a digital oscilloscope.

However, even such a complex solution did not allow accurate detection of the beginning of certain phases and phrases in the power supply chains with high accuracy and in automatic mode, which led to the need for multiple repetition of experiments and direct selection of the moment of impact. Multiple repetitions of the effects on the power lead to wear of the investigated element and significantly increase the probability of its failure.

In this regard, the authors proposed to expand the functionality of the existing hardware and software solutions by introducing additional tools based on predictive Analytics.

4 DECISION OF TASKS

The proposed method of solving the problem is as follows:

- formation of a database of reference signals in the power supply circuit of the analyzed microprocessor device, in which certain phases are clearly traced (on, off, restart, inactivity, initialization, execution of the algorithm, saving the results in internal or external memory, data exchange on external ports of the device);
- allocation of characteristic phrases in the above phases (for example, the inclusion of internal devices after a restart, initialization of internal memory, interrupt processing, the beginning of the algorithm, algorithm cycles, etc.);
- selection and training of predictive Analytics model;
- selection and analysis of neural network model for predictive Analytics;
- neural network training according to the selected model;
- testing of neural network on reference data;
- processing of real data from the analyzed device;
- identification of training errors and correction of predictive Analytics model based on neural network.

To implement this method, a software package was developed in Python using the numpy, mtplotlib, scipy, Keras, Tensor Flow libraries [4]. As a neural network, a modified model of recurrent neural network was used - a network of long-term memory with the number of layers equal to four [5]. Here are the results of the experiments.

ACKNOWLEDGMENTS

The experiment was based on 150 million points with a representative sample of

900 points for each phase.

Three characteristic phrases (patterns) of algorithms were predicted. In the course of the experiments, it was possible to achieve a prediction error in the range of 2% - 6%, which allows us to attribute the proposed method to a class of methods with high reliability.

Processing of real data involves pre-cleaning and noise reduction according to a certain, in the course of experimental studies, noise model, which reduces the prediction error by 30% - 35%.

This paper presents the results of the development and experimental verification of the effectiveness of the method of predictive Analytics based on the neural network of long-term short-term memory in the analysis of the security of microprocessors and microprocessor plastic cards.

REFERENCES

[1] Babenko L.K., Bespalov D.A., Makarevich O.B. Modern intelligent plastic cards. - Moscow: Helios ARV, 2015. - 416 p.

[2] F.N.M Surname, Article Title, https://www.acm.org/publications/proceedings-template.

[3] Mangard S., Oswald E., Popp T. Power Analysis Attacks. Revealing the secrets of smart cards. Springer Science+Business Media, LLC. 2007. - 337 p.

[4] Charvet X., Pelletier H. Improving the DPA attack using wavelet transform. SAGEM DS. 2005. - 15 p.

[5] Chollet F. Deep learning with python. Manning Publications Co. 2018. - 373 p.

[6] Hochreiter S., Schmidhuber J. Long short-term memory. Neural computation 9 (8). 1997, - 33 p.

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СБОРУ ИНФОРМАЦИИ С САЙТОВ И ОБХОДА ТАКОГО ПРОТИВОДЕЙСТВИЯ

Анатолий Басюк
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
anatoly.basyuk@gmail.com
Евгений Абрамов
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия abramoves@sfedu.ru

АННОТАЦИЯ

В статье рассматриваются история и некоторые методы противодействия сбору информации с сайтов.

КЛЮЧЕВЫЕ СЛОВА
Crawler, scraping, captcha, reCAPTCHA, JavaScript.

1 ВВЕДЕНИЕ

Веб-сканеры, так же называемые пауками или роботами, являются инст-рументами, которые предоставляют возможность сканировать интернет страницы в автоматическом и систематическом режиме. Их целью является получение и анализ информации, которая публикуется в Интернете. Первоначаль но были разработаны сканеры поисковыми система для индексирования веб-страниц. Теперь же сканеры используются для проверки ссылок на веб-сайты, как краулеры для сбора контента или в качестве анализаторов сайтов, которые обрабатывают собранные данные для аналитических или архивных целей [1].

В то время как многие краулеры являются законными и помогают поль-зователям находить соответствующий контент в интернете, так же существуют краулеры которые разворачиваются для вредоносных целей. Например, киберпреступники выполняют крупномасштабные сканирования в социальных сетях для сбора информации о профиле пользователя, и которая в дальнейшем может быть продана онлайн-маркетологам или быть использована для целенаправленных атак.

В 2010 году Facebook подал в суд, на предпринимателя, который просканировал более 200 миллионов профилей и планировал создать собственную службу поиска, по данным которым он собрал.

В целом, проблема краулинга сайтов не ограничивается социальными сетями. Многие сайты, рекламирующие товары, услуги желают иметь защиту от конкурентов, которые используют сканеры для отслеживания их контента.

Многие веб-сайты напрямую запрещают несанкционированное очищение в их условиях пользования. К сожалению, такие условия просто игнорируются вредоносными краулерами.

Современные методы обнаружения полагаются на простое обнаружение краулера (например, изменённые строки user-agent, подозрительные referrers) и простые шаблоны трафика, чтобы отличать человеческий трафик от трафика краулера. К сожалению, лучшие реализации краулеров могут обходить данные методы обнаружения.

Многие сайты полагаются на CAPTCHA, чтобы предотвратить краулинг своего веб-контента. Но некоторые тесты CAPTCHA могут быть уязвимы для автоматических методов распознавания. Тем не менее, хорошо разработанные CAPTCHA предлагают разумный уровень защиты от автоматических атак. К сожалению, их чрезмерное использование приводит к проблеме удобства использования сайтом и значительно снижает удовлетворенность пользователей [2].

2 МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СБОРУ ИНФОРМАЦИИ

2.1 Блокирование IP-адресов

Блокирование IP-адресов – это конфигурация сетевых служб, так, чтобы запросы от хостов с определенными IP-адресами отклонялись.

Unix-подобные операционные системы обычно реализуют блокировку IP-адресов с использованием TCP-Wrappers.

Самый простой и наиболее распространённый способ определения попыток автоматического сбора информации с веб-сайтов – это анализ частоты запросов на сервер. Если запросы с определенного IP-адреса слишком частые или их слишком много – адрес блокируется [3].

2.2 Использование учетных записей и методов аутентификации

С помощью этого метода защиты доступ к данным может осуществляется только авторизированными пользователями. Это упрощает контроль над поведением пользователей и блокирует подозрительные учетные записи независимо от IP-адреса, с которого работает клиент.

2.3 Использование CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans A part) — это тип теста, используемый в вычислениях, чтобы опреде-лить, является ли пользователь человеком или нет.

Эта процедура идентификации пользователей получила множество кри-тических замечаний, особенно от людей с ограниченными возможностями, а также от людей, которые считают, что их повседневная жизнь замедляется искаженными словами, которые трудно прочесть. Среднестатистическому человеку требуется приблизительно 10 секунд, чтобы распознать типичную CAPTCHA.

reCAPTCHA – обновленная система, разработанная в университете Карнеги-Меллон для защиты от ботов и для помощи в оцифровке текстов книг.

Принцип ее работы заключается в том, что человеку предлагают ввести два слова вместо одного. Одно из этих слов уже известно системе и раннее было распознано. Второе слово еще не распознано и его нельзя распознать программой распознавания текста. Проверка этой капчи работает через то слово, которое было раннее распознано в системе. Причем второе слово, которое еще не распознано в системе даже вводить не обязательно. Система reCAPTCHA предоставляет клиентам изображения для распознавания и получает результаты, которые потом передает фирмам по оцифровке материалов.

2.4 Использование сложной JavaScript логики

Когда страница загружается в браузер, она становится объектом документа, чьи HTML-элементы или узлы элементов становятся доступны JavaScript коду. По мере загрузки JavaScript может создавать может создавать новые HTML-элементы и добавлять их в документ. Страница, на которой это происходит, называется страницей, созданной JavaScript. Новые элементы не будут присутствовать в исходном

коде страницы, но они будут присутствовать в коде, который загружается как документ HTML. Этот HTML-код можно получить с помощью DOM`s innerHTMLproperty, представляет собой код завершенной веб-страницы, отображаемый браузером после завершения работы JavaScript.

2.5 Частое обновление структуры страницы

Одним их наиболее эффективных способов защиты веб-сайтов от автоматического сбора информации является частое изменение их структуры. Это может применятся не только к изменению имен идентификаторов и классов HTML-элементов, но даже и всей иерархии сайта.

Это делает написание краулера сложным, но данный метод может перегрузить код сайта, а иногда и всю систему.

2.6 Ограничение частоты запросов и загружаемых данных

Это позволяет сделать краулер большего количества данных очень медленным и, следовательно, нецелесообразным. В тоже время ограничения долж-ны применятся с учетом потребностей обычного пользователя, чтобы этот метод не уменьшал общее удобство использования сайта.

2.7 Предоставление важных данных в виде изображений

Этот метод защиты контента делает автоматический сбор данных более сложным и в тоже время поддерживает визуальный доступ для обычных пользователей. Изображения часто заменяют, например, цены, адреса электронной почты и номера телефонов, но некоторые веб-сайты даже могут заменить случайные буквы в тексте. Хотя ничего не мешает отображать содержимое веб-сайта в графической форме (например, с использованием Flash или HTML5), но это может значительно снизить его индексируемость для поисковых систем.

СПИСОК ЛИТЕРАТУРЫ

[1] Protect your site against Web Scraping, https://blog.jscrambler.com/pro-tect-your-site-against-web-scraping/

[2] Protecting Users and Businesses from CRAWLers, https://www.sba-research.org/wp-content/uploads/publications/usenix12_pubcrawl.pdf

[3] IP address blocking https://en.wikipedia.org/wiki/IP_address_blocking

SYSTEM OF MANAGEMENT MSF THROUGH RPC REQUESTS

Vasiliy Kryuchkov
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
im@vkryuchkov.ru
Evgeny Abramov
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
abramoves@sfedu.ru

ABSTRACT

This work presents a software package that implements the ability to remotely network application and manage modules of the Metasploit Framework [1]. This software package is designed to test systems for detecting, preventing and eliminating the effects of computer attacks, antiviruses, and other means of protecting distributed computer network information against malware code on client personal electronic computers with Windows and Linux operating systems.

KEYWORDS

Metasploit, rpc, security analysis system, pentest, simulation of network attacks, automated exploiting, testing of information security tools

1 INTRODACTION

Over the past few decades, information technology has been increasingly entering our lives, and with this, the importance of information security is growing.

Information security breaches can be caused by many reasons:

- vulnerabilities in operating systems;
- vulnerabilities in installed applications;
- errors in setting security policy;
- incorrect configuration of protective equipment.

Due to the occurrence of such violations, attackers can make attacks on the automated system. Therefore, at each stage of the life cycle of automated systems, it is necessary to understand whether the system meets the required level of security.

Today, the Metasploit Framework is one of the best penetration testing tools.

Penetration testing consists of many separate checks. Manual verification takes a huge amount of time, and the automatic verification tools available today, such auto_pwn [2], are quite crude methods and are not very effective, as they are based on iterating through a large number of exploits.

2 SYSTEM ARCHITECTURE

Today, there are a huge number of software tools for a comprehensive assessment of the security of programs, computer networks, and their complexes. All these tools are created independently of each other and often do not have a common compatible software interface that would allow the comprehensive use of analysis tools, which necessitates a tool that should solve the problems of launching, monitoring and analyzing the results of analysis tools of software tools.

To implement the task, the system architecture displayed in Fig. 1 was chosen.

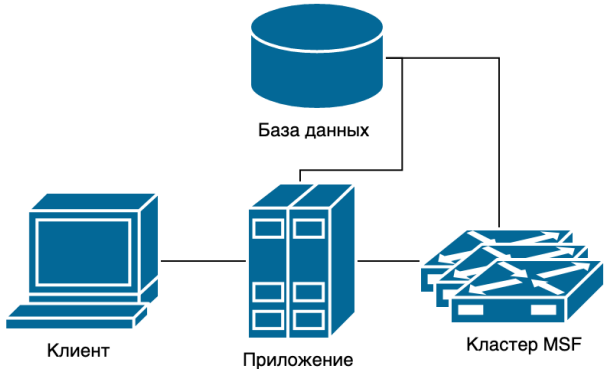

Figure 1: General system architecture

In this architecture, the client only interacts with the application, which is the Node.JS REST server [3]. In turn, the application deals with the task of managing the MSF cluster, as well as the distribution and management of tasks that come from the client. The application and the MSF cluster use the same physical database and each instance of the MSF or application has its own logical database. The interaction between all elements is through TCP / IP [4].

Docker containers are used to deploy the MSF cluster, target systems, and applications.

Docker is software for automating the deployment and management of applications in a virtualization environment at the operating system level [5]. Allows you to "pack" the application with all its surroundings and dependencies into a container that can be ported to any Linux system with groups support in the kernel, and provides a container management environment.

Kali Linux is used as the base system for the MSF container.

Kali Linux OS - an OS specially designed for penetration testing, includes a huge number of pre-installed programs and utilities for software and technical expertise, such as Aircrack-ng, Burp_suite, Hydra, John_the_Ripper, Metasploit, Nmap, Wireshark, Armitage and others [6].

3 CONCLUSION

As a result, a software package was developed that implements the remote network application and control of the Metasploit Framework modules and is designed to test

detection systems, prevent and eliminate the effects of computer attacks, anti-viruses, and other means of protecting distributed computer network information against malware code on client PCs with operating Windows, Linux family systems.

This project has ways of further development. For example, a rational addition to the existing complex would be the addition of the ability to run your own scripts, as well as their generation based on visual representation using visual programming languages. It is also possible to expand the drivers used, for example drivers for web scanners and sql injections.

REFERENCES

[1] Metasploit Basics [Electronic resource]. URL: https://metasploit.help.ra-pid 7.com/docs/metasploit-basics

[2] The New Metasploit Browser Autopwn: Strikes Faster and Smarter - Part 1 [Electronic resource]. URL: https://blog.rapid7.com/2015/07/15/the-new-metas-ploit - browser-autopwn-strikes-faster-and-smarter-part-1/

[3] About Node.js [Electronic resource]. URL: https://nodejs.org/en/about/

[4] TRANSMISSION CONTROL PROTOCOL [Electronic resource]. URL: https://tools.ietf.org/html/rfc793

[5] Docker overview [Electronic resource]. URL: https://docs.docker.com/en-gine/docker-overview/

[6] What is Kali Linux? [Electronic resource]. URL: https://docs.kali.org/in-troduction/what-is-kali-linux

РАЗРАБОТКА И ИССЛЕДОВАНИЕ АЛГОРИТМОВ АНАЛИЗА ШИФРА CLEFIA

Артур Куликов
Южный Федеральный Университет, Таганрог, Россия
refulgent_armor@mail.ru

АННОТАЦИЯ

В ходе выполнения работы разработана, реализована и опробована на практике программа шифрования и расшифрования данных с помощью алгоритма шифрования «Clefia», а также разработан и реализован алгоритм дифференциального анализа шести, девяти, двенадцати раундов шифрования с различными упрощениями и без них с помощью данного алгоритма.

В данной работе содержится подробное описание алгоритма нахождения правильных пар текстов по характеристике с целью последующего дифференциального криптоанализа алгоритма «Clefia». В результате применения данного ал-

горитма были получены правильные пары текстов для последующего криптоанализа. Проведена оценка сложности поиска пар для всех используемых характеристик для шифров с используемыми упрощениями и уменьшенным количеством раундов. Все результаты подробно описаны, объяснены на примерах с использованием таблиц, иллюстраций и схем.

КЛЮЧЕВЫЕ СЛОВА

Криптография, блочный шифр. дифференциальный анализ, шифр «CLEFIA»

1 ВВЕДЕНИЕ

«Clefia» – блочный симметричный алгоритм шифрования. Целью данной работы была разработка и реализация алгоритма для дифференциального криптоанализа алгоритма «Clefia».

2 РАЗРАБОТКА И ИССЛЕДОВАНИЕ

В ходе выполнения работы решались задачи по разработке и реализации алгоритма шифрования. После программной реализации алгоритма шифрования был проведён анализ быстродействия алгоритма шифрования, состоящий из замеров быстродействия шифрования блока данных и алгоритма выработки ключей, как по отдельности, так и вместе. Следующим этапом были проанализированы криптографические примитивы. Представляющие интерес в рамках дифференциального криптоанализа. С помощью метода Гаусса было установлено, что матрицы рассеивания обратны сами себе, что позволило в дальнейшем преобразовывать разницы необходимым нам образом для предсказания их поведения. Были проанализированы блоки замены и построены таблицы с возможными разностными входами и выходами с вероятностями таковых преобразований. Опираясь на эти таблицы, стало возможно выработать характеристику и оценить сложность поиска правильной пары, соответствующей такой характеристике.

После анализа криптографических примитивов было принято решение ослабить оригинальный шифр с целью нахождения максимального количества раундов, не устойчивых к дифференциальному криптоанализу. Также алгоритм ослаблялся частичным или полным отключением механизма переключения рассеивания (Diffusion Switching Mechanism – DSM). Частичное отключение подразумевало отключения разнообразия либо только матриц рассеивания, либо только таблиц замены, полное отключение подразумевает отключение разнообразий обеих криптографических примитивов.

Отключение разнообразие не подразумевает исключение блоков замены или матриц рассеивания, а лишь использование одинаковых, вместо чередующихся.

В результате анализу подвергались шесть и двенадцать раундов без разнообразия блоков замены и матриц рассеивания, двенадцать раундов только без раз-

нообразия матриц рассеивания. Следующим этапом механизм переключения рассеивания работал полноценно, но были проанализированы алгорит-мы размером лишь шесть и девять раундов.

Каждый из выбранных упрощённых алгоритмов был атакован успешно.

Однако больший интерес представлена сложность нахождения разности. Одной из целей анализа было проверить степень влияния механизма переключения рассеивания на устойчивость алгоритма против дифференциальных атак. В результате можно утверждать, что разнообразие матриц рассеивания играет большую роль, чем разнообразие блоков замены. Алгоритм с одинаковыми матрицами рассеивания легче поддаётся дифференциальному анализу. Максимальное количество раундов, которое получилось атаковать при функционирующем механизме переключения рассеивания равно девяти, в то время как без функционирования данного механизма получится атаковать более 12 раундов, что говорит о большом вкладе данного механизма в стойкость алгоритма шифрования «Clefia» к дифференциальному классу атак.

СПИСОК ЛИТЕРАТУРЫ

[1] Shirai T., The 128-bit Blockcipher CLEFIA (Extended Abstract) [Electronic resource]. – URL: https://www.iacr.org/archive/fse2007/45930182/45930182.pdf.

[2] Biham E., Differential Cryptanalysis of the Data Encryption Standard [Electronic resource]. – URL: http://www.cs.technion.ac.il/~biham/Reports/dif-ferential-cryptanalysis-of-the-data-encryption-standard-biham-shamir-authors-latex-version.pdf.

[3] Бабенко Л.К., Дифференциальный криптоанализ алгоритма ГОСТ 28147-89 [Текст] / Л.К. Бабенко, Е.А. Ищукова // Известия ЮФУ. Технические науки. – 2011. – №12 (125). – С. 120 – 130.

[4] Арифметика полей Галуа для кодирования информации кодами Рида-Соломона [Электронный ресурс]. – URL: https://habr.com/ru/post/212095/.

[5] Конечное поле GF(256) и немного магии [Электронный ресурс]. – URL: https://habr.com/ru/post/279197/.

[6] Ищукова Е.А., Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147-89 [Текст] /Е.А. Ищукова, И.А. Калмыков // Инженерный вестник Дона. – 2015. – №4. – 8 с.

[7] Biham E., Differential Cryptanalysis of the Full 16-round DES, Advances in Cryptology [Text] / E. Biham, A. Shamir // Crypto’92, Springer-Velgar. – 1998. – P. 487 – 496.

[8] Biham E., Differential Cryptanalysis of DES-like Cryptosystems, Exten-ded [Text] / E. Biham, A. Shamir // Crypto’90, Springer-Velgar. – 1998. – 105 p.

[9] Ищукова Е.А. Дифференциальный анализ шифра Кузнечик [Текст] / Е.А. Ищукова, Л.К. Бабенко, Е.А. Толоманенко // Известия ЮФУ. Технические науки. – Таганрог: Изд-во ЮФУ. – 2017. – № 5. – С. 25 – 37.

[10] Бабенко Л.К., Применение параллельных вычислений при решении задач защиты информации [Текст] / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров // Программные системы: теория и приложения. – 2013. – Т. 4 – № 3–1 (17). – С. 25 – 42.

[11] Шнайер Б., Прикладная криптография. Протоколы, алгоритмы и исходный код на С [Текст] / Б. Шнайер. – М.: Изд-во Вильямс. – 2017. – 1040 с.

[12] Компаниец В.С., Безопасность человеко-машинного взаимодействия [Текст] / В.С. Компаниец // Таганрог: ИКТИБ ЮФУ. – 2015. – 47 с.

TECHNOLOGY OF DEEP PACKET INSPECTION FOR RECOGNITION AND BLOCKING TRAFFIC OF THE TOR NETWORK

Vitaly Lapshichyov
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
lapshichyov@sfedu.ru
Oleg Makarevich
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
obmakarevich@sfedu.ru

ABSTRACT

On the Internet there are a large number of materials that are prohibited for distribution. This list includes extremist materials, documents containing state secrets, various photos and video materials for adults, information on the manufacture of explosives, weapons and drugs.

Often, a popular anonymizer, the Tor software package, is used to access such sites and anonymously post materials. The Tor server network allows users to achieve a high degree of anonymity on the Internet.

Both sites with such materials and the actions of Internet users who place these materials should be blocked in accordance with federal laws of the Russian Federation.

Currently, the technology of Deep Packet Inspection is used to identify prohibited materials and to restrict access to them. Since this technology requires significant resources for work and has some features in the mechanism for analyzing the transmitted data, there is a reasonable need for alternative methods of identifying and blocking users that will achieve high efficiency in countering criminals with minimal resources.

KEYWORDS

Cybersecurity, forensics, Tor Bundle, de-anonymization, TLS encryption, counterterrorism, Deep Packet Inspection, TLS certificate.

1 INTRODUCTION

In connection with the development of anonymous access technologies and hiding the activities of individual users on the Internet used by them to commit various types of crimes in the field of information technology, one of the central topics of research by scientists in this area is the study and analysis of the Tor Bundle for the subsequent deanonymization of such users and to legally block their access to data networks.

The Tor Bundle is interesting in that, in addition to the users of this network using a specially created list of proxy servers, it allows accessing the so-called Darknet network of the Tor network servers by using a software package that includes a browser and software proxy server for tunneling traffic to one of the network nodes.

Such opportunities for anonymizing of users are used for criminal purposes: for the sale of weapons, drugs and materials prohibited for free circulation in most countries of the world, for the disclosure of information constituting a state secret. In this regard, the Tor software package and its users attract the close attention of law enforcement agencies, including those who are fighting cybercrime.

Moreover, such opposition is aimed not only at identifying and establishing the identity of persons committing crimes using information technology, but also at suppressing such activities, if possible, at the earliest stages of its implementation.

2 DEEP PACKET INSPECTION

Currently, one of the effective and at the same time resource-intensive technology aimed at identifying and blocking connections to the Tor network is a Deep Packet Inspection.

The technology of Deep Packet Inspection (hereinafter - DPI) is based not only on the recognition and creation of a "black" list of IP addresses and ports of incoming and outgoing connections, but also on heuristic (behavioral) analysis of network traffic data transmission [1]. In-depth analysis involves the study of the upper layers of the OSI protocols, which is carried out both by the behavior patterns of certain applications, and by previously unknown signs that go beyond such patterns.

In their article [2], Swedish researchers from the University of Karlstad Philippe Winter and Stefan Lindskog discuss the basic principles of the Great China Firewall, a traffic analysis and blocking service within the PRC Golden Shield project, the main

principle of which is the use of DPI.

Tor network traffic is recognized by the set of ciphers offered to establish a secure connection during TLS-handshake. Along with another researcher of the protocols for connecting the Tor Bundle, Tim Wilde, they claim that it is unique and is used only by the software package, while being completely identical to the Firefox browser cipher suite version 3 [2-3]. Another Swedish researcher Anders Granerud from the Gjøvik University College in his study [4] of the anomalies of the TLS connection protocol indicates that the Tor complex offers 28 ciphers for traffic encryption, browsers: Opera - 27, Chrome - 11, Firefox - 33, Internet Explorer - 12. Thus, this feature is still not unique for unambiguous determination of the network traffic of Tor.

Nevertheless, an alternative method developed by the author for identifying Tor network traffic in data transmission networks [5] uses other principles that are related to the features of establishing a connection between the client software of the user and the Tor network server, namely, it is based on the characteristics of SSL / TLS certificates transmitted on the line "user-server of Tor network". These characteristics are currently identified in the analysis of the Tor network data.

Well-known signs of connecting to the Tor network and certificate parameters, which are described in the scientific literature, are mentioned as follows:

1. Connecting to the Tor network is done through ports 443, 9001.

2. The name of the server that issued the certificate, which the user of the Tor network receives during SSL / TLS-handshake, contains a set of letters and numbers and .net.

Moreover, one of the characteristics, according to the author, is unique - this is the size of the certificate. The study of certificates of various servers using packet analyzers (sniffers) allows to state at this stage that the third attribute of a certificate is its size, which is 450-590 bytes.

It is currently unknown whether in Deep Packet Inspection can be used to identify Tor network data using known certificate parameters.

The principle of identifying these characteristics in real time (on-line) is under development as part of the dissertation research “Development and research of methods for detecting and identifying the use of the Tor Bundle in data transmission networks”.

REFERENCES

[1] A brief overview of DPI technology - Deep Packet Inspection. Habr. The community of IT professionals, https://habr.com/en/post/111054/

[2] Philipp Winter, Stefan Lindskog (University Karlstad). How the Great Firewall of China is Blocking Tor. Materials of 12th Free and Open Communications on the Internet Conference. Bellevue, WA, USA: USENIX. The Advanced Computing Systems Association, 2012.

[3] Tim Wilde. Tor Bug 4185 Testing and Report. https://gist.github.com/twilde/da3c7a9af01d74cd7de7.

[4] Anders Olaus Granerud. Identifying TLS abnormalities in Tor, https://doc-player.net/49209918-Identifying-tls-abnormalities-in-tor-anders-olaus-granerud.tml

[5] Lapshichyov V. V. Using network analyzers (sniffers) to study the characteristics of the Tor network data, https://hub.lib.sfedu.ru/repository/material/ 801262066.

ALGORITHM FOR ANALYZING AND BLOCKING ACCESS TO THE TOR NETWORK

Vitaly Lapshichyov
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
lapshichyov@sfedu.ru
Oleg Makarevich
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
obmakarevich@sfedu.ru

ABSTRACT

To implement the legitimately blocking of access to the Internet using software that allows anonymous actions in data networks and on the pages of various sites, researchers are developing various principles for detecting user actions.

One of the most popular anonymizer among criminals is the Tor software package. The specified anonymizer uses a network of proxy servers and encryption to ensure maximum protection of the transmitted data.

Connecting to the Tor network is performed using SSL / TLS encryption, during which the server sends a certificate to the user to confirm that it belongs to the anonymous network.

During the study, certain features of the specified certificate were established that allow it to be identified in the network data stream.

To identify the certificates, an algorithm has been developed that can be used to create software for legitimately blocking access to users of the Tor software package.

KEYWORDS

Cybersecurity, forensics, Tor Bundle, de-anonymization, TLS encryption, counterterrorism, TLS certificate.

1 INTRODUCTION

In connection with the increase in the use of the Tor Bundle for realizing the anonymity of Internet users [1, p. 9], as well as with the increasing role of this complex in the process of committing crimes in the field of information technology, law enforcement and security services attach great importance to the early suppression of such activities and the identification of persons involved in the commission of such crimes.

To implement the second task, methods are used to analyze various parameters of using the Tor network (fingerprinting), and, with a variable degree of success, a MITM attack (man in the middle) to the output node of the Tor network can be used, during which a controlled node of the chain is created, the data to which are already unencrypted and can be analyzed or replaced [2, p. 258-261].

The first task mentioned above can be implemented in various ways, but the author sees the solution in restricting access to the Internet for users of the Tor Bundle and suggests that such a restriction be made on the segment between the user and the Tor network server.

This decision is based on the results of a study of the features of the Tor network certificates transmitted during the establishment of a TLS connection on the Tor network "user-server" line and the exchange of this certificate between the server and the user.

Features of Tor certificates were described by one of the Swedish researchers at the Gjøvik University College Anders Granerud, who pointed out signs that were abnormal compared to certificates of other applications: the contents of the name of the server issuing the certificate (contains a set of numbers and letters in the name and has the extension .net or .com, for example: www.jzhdfgkj79kjh98.net) and using port 443 [3].

During the experimental study of the Tor certificates by Wireshark and NetworkMiner analysis programs, the author came to the conclusion that there is a third feature of the Tor certificate - its size, and also supplemented the data on the Tor network ports [4].

2 ALGORITHM

Based on this data, an algorithm was developed (Fig. 1) for analyzing certificate data and restricting user access to the Internet, which is based on a sequential check of the presence of three features of the Tor certificate: connection port, name of the server issuing the certificate, and known size, where:

(1) Connection start

(2) SSL/TLS v1.2 handshake

(3) Connection port check

(4) Port {443, 9001, 8443, 22, 80, 8080, 9000, 20000, 20001, 20002} -> yes/no

(5) If “no” -> traffic skipping
(6) Connection establishing
(7) End of algorithm
(8) If “yes”-> TLS Certificate Details check
(9) Mask TLS Certificate: CN = www.[set of letters and digits].net -> yes/no
(10) If “no” -> traffic skipping
(11) Connection establishing
(12) End of algorithm
(13) If “yes” -> certificate size check
(14) 401 b ≤ certificate size ≤ 599 b -> yes/no
(15) If “no” -> traffic skipping
(16) Connection establishing
(17) End of algorithm
(18) If “yes” -> data network access blocking
(19) End of algorithm

REFERENCES

[1] Burtsev S. E. Reasons for the increase in the number of Russian users of the Tor anonymous network and the effect of PR campaigns on interest in hidden Internet services. ITportal, 2017. No. 4 (16). http://itportal.ru/science/tech/prichiny-rosta-chisla-rossiyskikh-p.

[2] Lazarenko A.V. (2016). Technology to de-anonymize Tor users. New information technologies in automated systems, 2016, 19.

[3] Anders Olaus Granerud. Identifying TLS abnormalities in Tor. https://doc-player.net/49209918-Identifying-tls-abnormalities-in-tor-anders-olaus-granerud. html

[4] Lapshichyov V.V. Using network analyzers (sniffers) to study the characteristics of the Tor network data, https://hub.lib.sfedu.ru/repository/material/ 801262066.

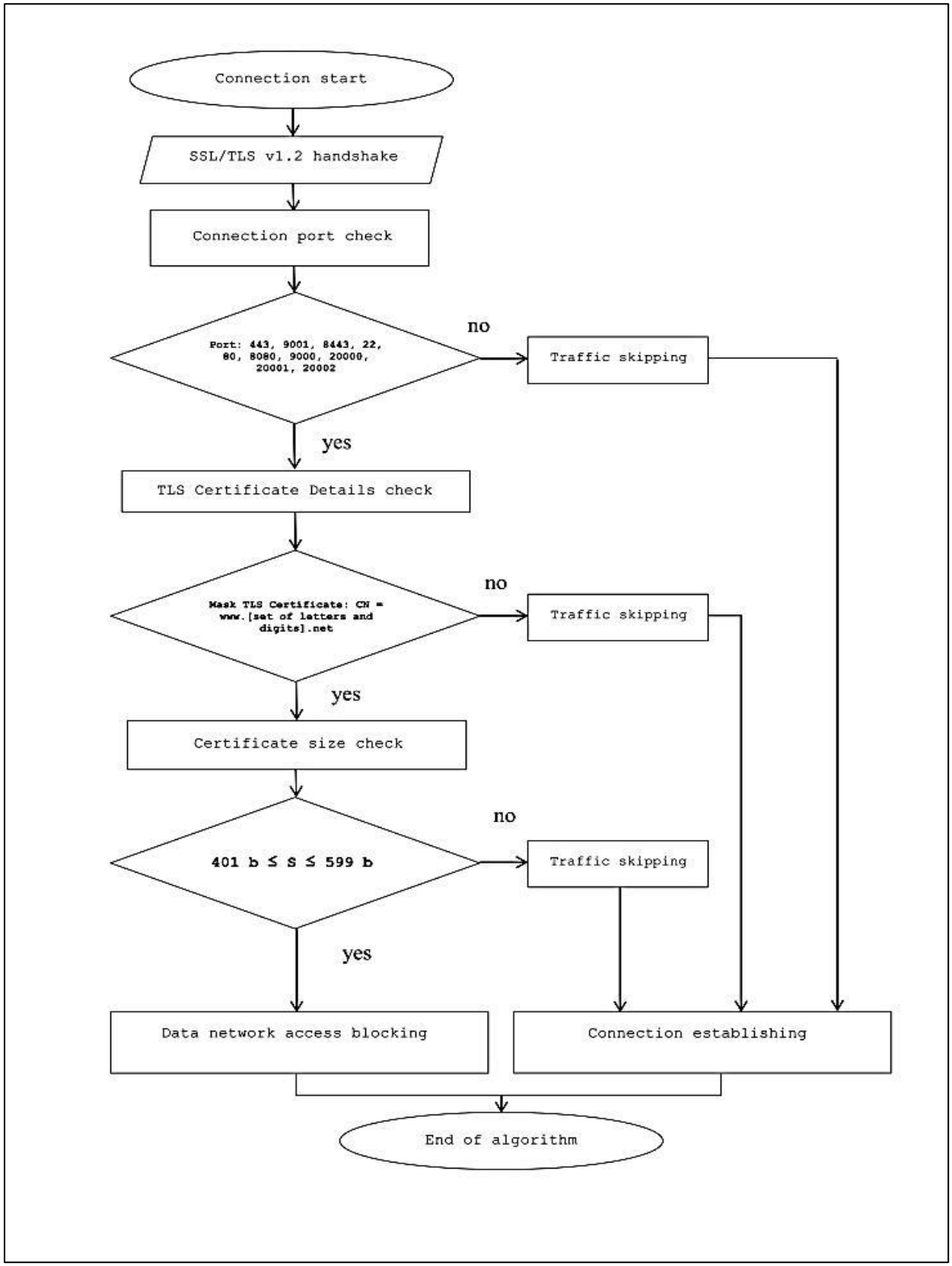

Figure 1: Algorithm for analyzing and blocking access to the Tor network

ОСОБЕННОСТИ ВЕРИФИКАЦИИ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ С ПОМОЩЬЮ ИНСТРУМЕНТА SCYTHER TOOL*

Елена Перевышина
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
lobova.elena702@gmail.com
Людмила Бабенко
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
lkbabenko@sfedu.ru

** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-01347*

АННОТАЦИЯ

Верификация безопасности протоколов является очень актуальной задачей, так как при разработке криптографических протоколов, не исключены ошибки, приводящие к возможности реализации атаки злоумышленником. Ошибки в протоколе могут быть неявными и трудно обнаруживаемыми. Существует множество примеров, когда ошибки обнаруживались в уже хорошо изученных протоколах.

Одним из средств автоматизированного анализа криптографических протоколов является средство Scyther tool.

Целью является изучение математического аппарата средства автоматической верификации Scyther tool, предназначенного для анализа безопасности криптографических протоколов.

КЛЮЧЕВЫЕ СЛОВА

Анализ безопасности, протокол Отвея-Рииса, Scyther tool.

1 ОПИСАНИЕ ПРОТОКОЛА ОТВЕЯ-РИИСА В СИНТАКСИСЕ ЯЗЫКА, ИСПОЛЬЗУЕМОГО В СРЕДСТВЕ SCYTHER TOOL

Scyther tool имеет собственный язык спецификации для описания протоколов. Спецификация протокола представляет собой описание ролей, которые содержат цепочку действий, последовательно выполняемых агентом, (события recv и send описывают получение и отправку сообщения соответственно). Свойства безопасности, которые нужно проверить являются частью описания протокола. Инструмент может установить, удовлетворены ли эти свойства или фальсификацию их.

Опишем протокол Отвея-Рииса в синтаксисе данного языка (см. рис. 1).

```
# Otway Rees

const Fresh: Function;
const Compromised: Function;

usertype String,SessionKey;

protocol otwayrees(I,R,S)
{
    role I
    {
        fresh Ni : Nonce;
        fresh M : String;
        var Kir : SessionKey;

        send_1(I,R, M,I,R,{Ni,M,I,R}k(I,S) );
        recv_4(R,I, M,{Ni,Kir}k(I,S) );

        claim_I1(I, Secret,Kir);
        claim_I2(I, Nisynch);
        claim_I3(I, Empty, (Fresh,Kir));
    }

    role R
    {
        var M : String;
        fresh Nr : Nonce;
        var Kir : SessionKey;
        var T1,T2: Ticket;

        recv_1(I,R, M,I,R, T1 );
        send_2(R,S, M,I,R, T1, { Nr,M,I,R }k(R,S) );
        recv_3(S,R, M, T2, { Nr,Kir }k(R,S) );
        send_4(R,I, M, T2 );

        claim_R1(R, Secret,Kir);
        claim_R2(R, Nisynch);
        claim_R3(R, Empty, (Fresh,Kir));
    }

    role S
    {
        var Ni,Nr : Nonce;
        var M : String;
        fresh Kir : SessionKey;

        recv_2(R,S, M,I,R, { Ni,M,I,R}k(I,S), { Nr,M,I,R }k(R,S) );
        send_3(S,R, M, { Ni,Kir }k(I,S) , { Nr,Kir }k(R,S) );
    }
}
```

Рисунок 1: Листинг протокола Отвея-Рииса

Объявим протокол с именем «otwayrees», который имеет три роли: «I», «R», «S». В конце каждой роли добавляются требования аутентификации и возможность проверки секретности некоторого терма.

Проверим секретность ключа между Алисой и Бобом claim_I1(I, Secret, Kir); свойство безопасности Nisynch (Non-injective synchronisation) – сущест-вование коммуникационного партнера, означает, что все полученные сообщения R действительно отправляются коммуникационным партнером (отправителем) и были получены другим коммуникационным партнером (получателем), это выражается в требовании claim(R, Nisynch).

2 ВЕРИФИКАЦИЯ ПРОТОКОЛА ОТВЕЯ-РИИСА С ПОМОЩЬЮ СРЕДСТВА SCYTHER TOOL

Промоделируем протокол Отвея-Рииса с помощью инструмента Scyther tool.

В результате моделирования протокола видно (см. рисунок 2), что в этом протоколе нарушено свойство безопасности nisynch, таким образом, протокол Отвея-Рииса обладает уязвимостью, приводящей к атаке, которая позволяет выдать одной из сторон себя за другую сторону в новом сеансе с другой стороной.

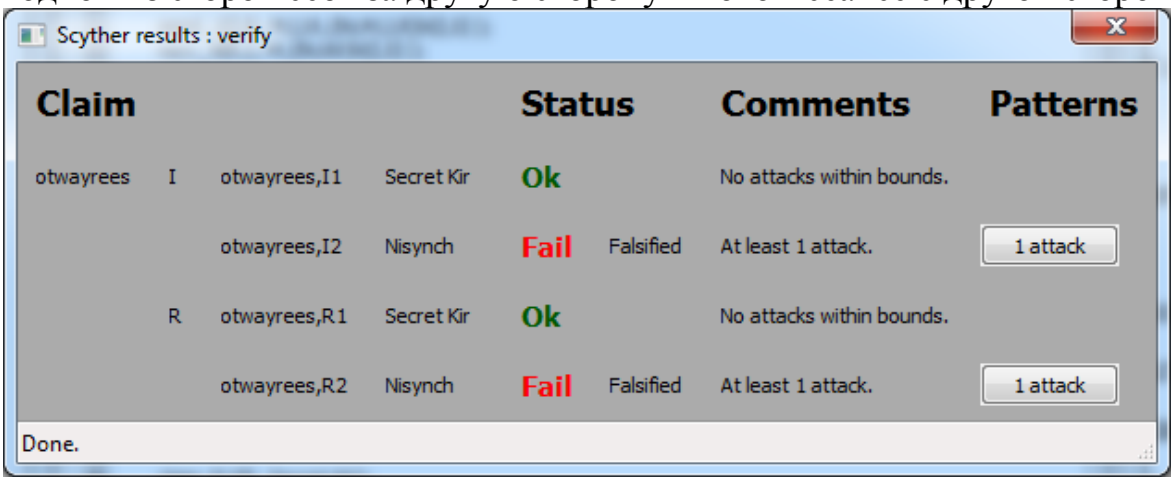

Рисунок 2: Результат проверки протокола

3 ЗАКЛЮЧЕНИЕ

Результатом является описание языка, который используется для составления модели в рассматриваемом инструменте; описаны взаимодействующие стороны, передаваемые данные, порядок передаваемых сообщений между сторонами; проведена верификация безопасности криптографического протокола Отвея-Рииса с помощью инструмента Scyther tool на предмет наличия атак на аутентификацию.

В результате моделирования протокола Отвея-Рииса установлено, что в протоколе нарушено свойство безопасности nisynch (Non-injective synchroni-sation-существование коммуникационного партнера), таким образом, протокол Отвея-Рииса обладает уязвимостью, приводящей к атаке, которая позволяет выдать одной из сторон себя за другую сторону в новом сеансе с другой стороной.

СПИСОК ЛИТЕРАТУРЫ

[1] Протокол Отвея Рииса. - URL: http://chinapads.ru/c/s/protokol_otveya _riisa

[2] Cas J.F. Cremers. The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols Tool Paper. Department of Computer Science, ETH Zurich, Switzerland. - URL: https://link.springer.com/content/pdf/10.1007%2F978-3-540-70545-1_38.pdf

[3] Cas J.F. Cremers. Unbounded Verification, Falsification, and Characterization of Security Protocols by Pattern Refinement

[4] Cas Cremers. Scyther User Manual

ОСОБЕННОСТИ ВЕРИФИКАЦИИ БЕЗОПАСНОСТИ ПРОТОКОЛОВ С ПОМОЩЬЮ ИНСТРУМЕНТА SPIN*

Елена Перевышина
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
lobova.elena702@gmail.com
Людмила Бабенко
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
lkbabenko@sfedu.ru

** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-01347*

АННОТАЦИЯ

Для оценки качества и безопасности разработанных протоколов применяют различные верификаторы безопасности. Существует ряд верификаторов, специально разработанных для анализа безопасности криптографических протоколов, такие как Scyther, Avispa, ProVerif, Cryptoverif и др. Однако, средства, ориентированные на верификацию протоколов безопасности, используются для верификации стандартных свойств (конфиденциальности, аутентификации), в то время как универсальные средства применяются для верификации более сложных свойств.

Средство формальной верификации SPIN использует проверку на моделях с применением темпоральной логики. Он не был специально разработан для проведения верификации безопасности протоколов. Этот инструмент более сложный, но гибкий и позволяет разработчику криптографического протокола создать модель своего протокола на требуемом ему уровне абстракций, и проверить его на соблюдение поставленных целей проверки. В модели необходимо самостоятельно описать криптографические функции, стороны, передачу сообщений, знания сторон, взаимодействие сторон, модели злоумышленника, цели верификации.

КЛЮЧЕВЫЕ СЛОВА

Верификация, криптографические протоколы, SPIN.

1 ВЕРИФИКАЦИЯ ПРОТОКОЛА НИДХЕМА-ШРЕДЕРА С ПОМОЩЬЮ ИНСТУМЕНТА SPIN

Смоделируем сокращенный протокол Нидхама-Шредера на языке Pro-mela.

В модели присутствует возможность проверки протокола в случае активных атак злоумышленника, в частности, атаки Лоу и подмены случайного числа.

Проведем верификацию модели при наличии злоумышленника первого типа. В инструменте SPIN переходим во вкладку «Verification», включаем использование "never claim" в соответствующем поле и производим верификацию кнопкой "Run". Обнаружилась ошибка (см. рисунок 1).

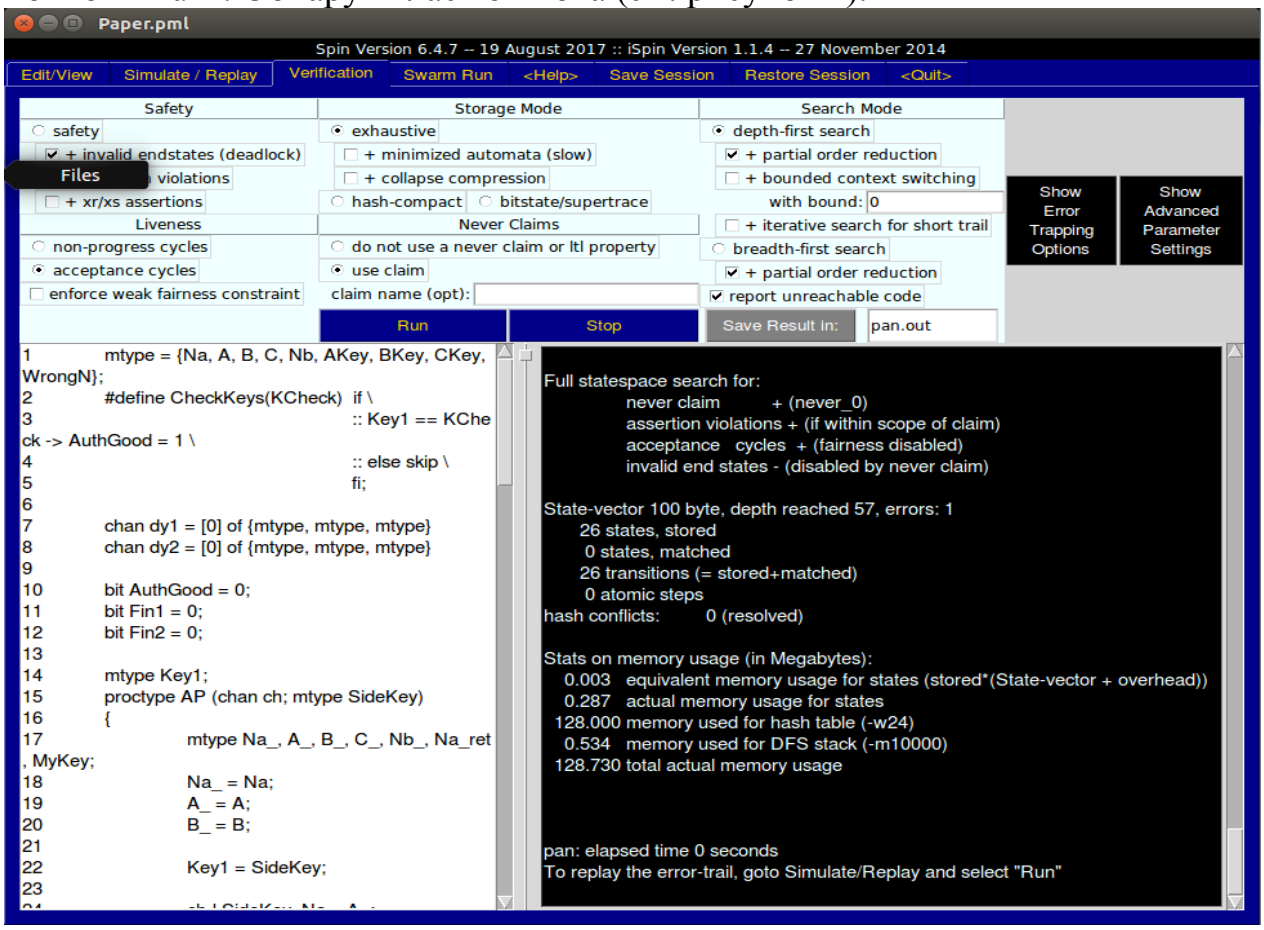

Рисунок 1: Ошибка при верификации

Для более подробного рассмотрения причины ошибки во вкладке «Simulate / Replay» строим схему взаимодействия сторон (см. рисунок 2).

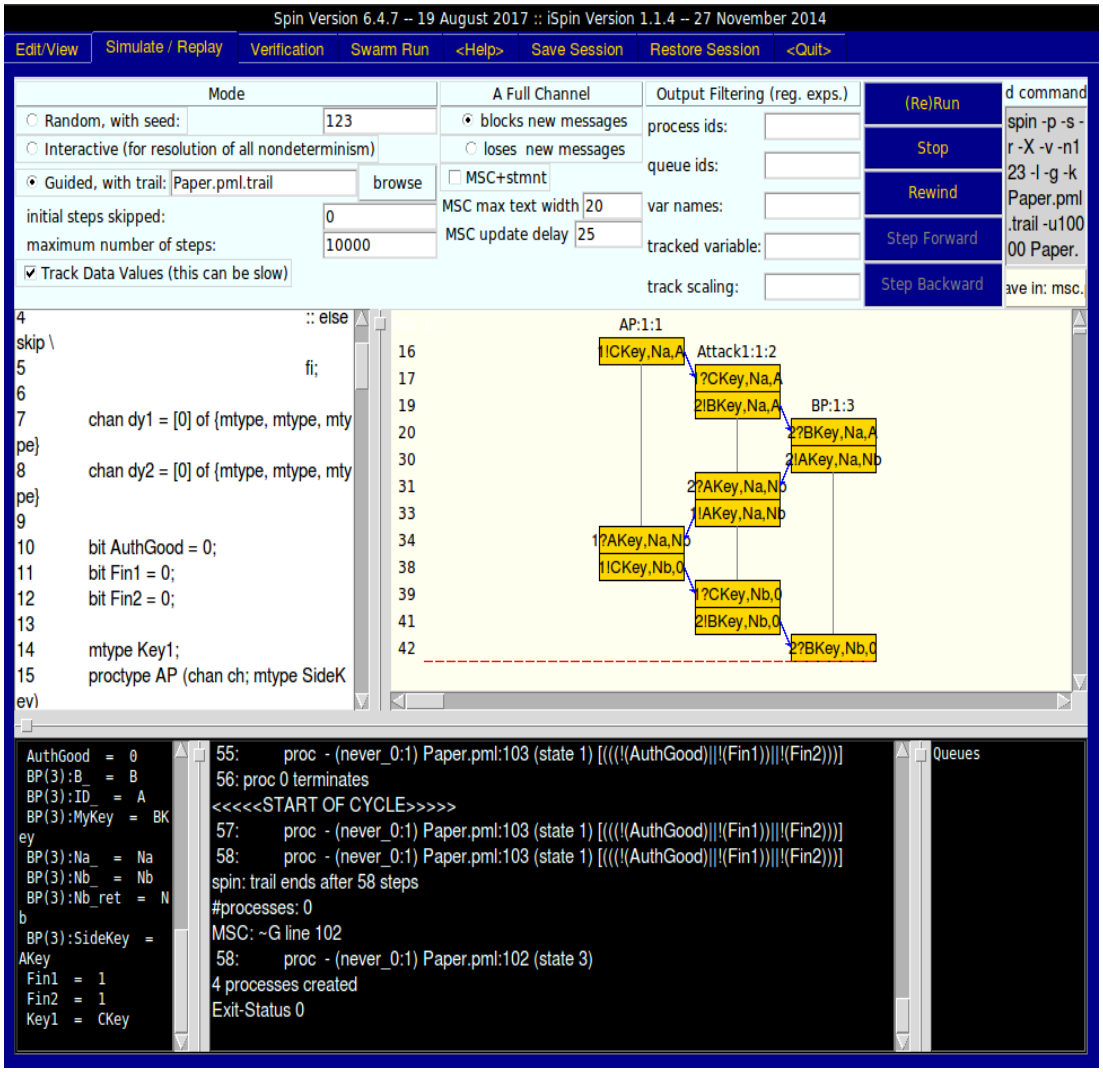

Рисунок 2: Схема атаки на протокол при наличии злоумышленника первого типа

Как видно из схемы в данном случае производится атака Лоу. Так же в левом нижнем окне выводятся значения переменных в последнем состоянии. Из этих значений можно выяснить, какие флаги не были установлены в единицу и где произошла ошибка. В данном случае флаг «AuthGood» оказался равным нулю. Это свидетельствует о том, что было подменено сообщение при передаче из стороны A к B, в частности содержимое сообщения осталось таким же, но ключ шифрования был использован разный. В случае второго типа злоумышленника верификация так же показывает ошибку. В данном случае производится атака на подмену случайного числа, и схема взаимодействия выглядит как на рисунке 3.

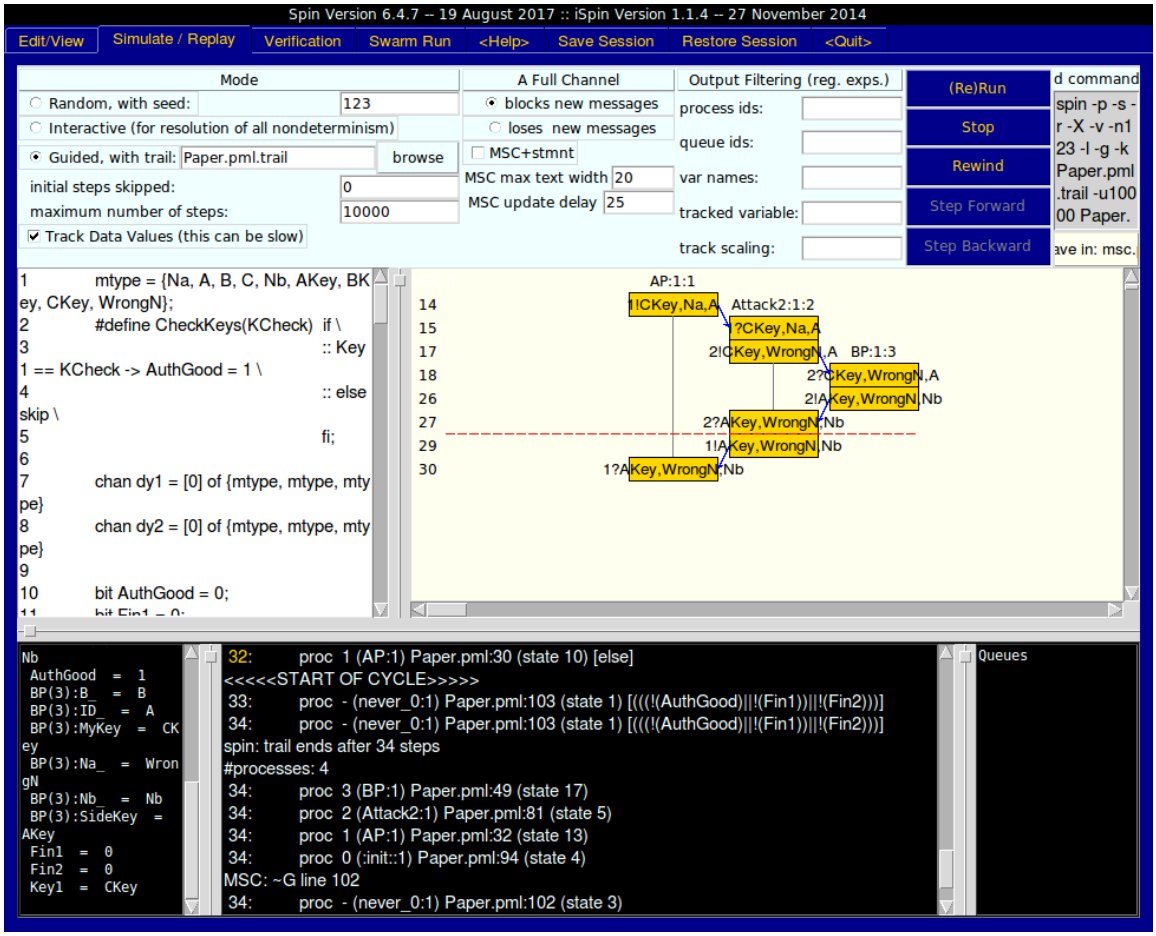

Рисунок 3: Схема атаки на протокол при наличии злоумышленника второго типа

По схеме можно увидеть, что протокол перестал выполняться после 2 сообщения. Злоумышленник, перехватив первое сообщение поменял значение случайного числа «Na» на «WrongN». Так же в данном случае значение контрольных флагов «Fin1» и «Fin2» принимают значение нуля. Это свидетельст-вует о том, что протокол на обеих сторонах не был выполнен до конца, в частности из-за некорректной проверки на возвращенное случайное число, которое было подменено злоумышленником.

2 ЗАКЛЮЧЕНИЕ

Рассмотрен метод определения атак на криптографические протоколы с помощью формального верификатора SPIN, который основан на проверке на моделях с применение линейной темпоральной логики LTL. В качестве примера приводится протокол Нидхема-Шредера. Описан язык Promela, который используется для составления модели в рассматриваемом инструменте. Показана модель протокола для определения атак на аутентификацию сторон. Описаны взаимодействующие стороны, передаваемые данные, порядок передаваемых сообщений

между сторонами. Проведена верификация безопасности криптографического протокола с помощью инструмента SPIN на предмет наличия атак на аутентификацию.

СПИСОК ЛИТЕРАТУРЫ

[1] И.В. Шошмина, Ю.Г. Карпов «Введение в язык Promela и систему комплексной верификации Spin» Санкт-Петербургский государственный политехнический университет, 2009.

[2] Holzmann G. J. The model checker SPIN //IEEE Transactions on software engineering. – 1997. – Т. 23. – №. 5. – С. 279-295.

[3] Barnat J., Brim L., Stříbrná J. Distributed LTL model-checking in SPIN //International SPIN Workshop on Model Checking of Software. – Springer, Berlin, Heidelberg, 2001. – С. 200-216.

[4] Holzmann G. J., Peled D. The state of SPIN //International Conference on Computer Aided Verification. – Springer, Berlin, Heidelberg, 1996. – С. 383-389.

[5] Needham R. M., Schroeder M. D. Using encryption for authentication in large networks of computers //Communications of the ACM. – 1978. – Т. 21. – №. 12. – С. 993-999.

[6] Lowe G. An Attack on the Needham− Schroeder Public− Key Authentication Protocol //Information processing letters. – 1995. – Т. 56. – №. 3.

ВЕРИФИКАЦИЯ БЕЗОПАСНОСТИ РЕАЛИЗАЦИЙ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ НА ОСНОВЕ ДИНАМИЧЕСКОГО АНАЛИЗА*

Людмила Бабенко
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
lkbabenko@sfedu.ru
Илья Писарев
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
ilua.pisar@gmail.com

**Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-01347*

АННОТАЦИЯ

Криптографические протоколы являются основой безопасности любой системы. С помощью них осуществляется передача данных, которые нуждаются в

защите от третьих лиц. Как правило, криптографический протокол разрабатывается, анализируется с помощью средств формальной верификации [1-3] и в случае, если признается безопасным, получает свою реализацию на языке программирования, с помощью которого разрабатывается система. Однако, при практической реализации криптографического протокола могут возникнуть ошибки из-за человеческого фактора, дополнения протокола, которые необходимы для возможности его реализации, которые влекут за собой подрыв его безопасности. Таким образом, получается, что изначально сам протокол считался безопасным, но его реализация на деле не является таковой. Помимо этого, формальная верификация использует довольно абстрактные понятия и не позволяет полностью проанализировать протокол.

КЛЮЧЕВЫЕ СЛОВА

Верификация безопасности, криптографические протоколы, динамический анализ.

Целью работы является повышение безопасности систем, использующих криптографические протоколы с помощью применения верификации безопасности криптографических протоколов по исходным кодам на основе динамического анализа. Для возможности проведения более эффективной верификации предлагается использовать новый подход, основанный на применении динамического анализа. Динамический анализ представляет собой исполнение системы с различными параметрами и данными в различных режимах, и обнаружение некорректной отработки алгоритмов, при которых возникают атаки на протоколы. Однако, производить динамический анализ непосредственно в коде рассматриваемой системы может быть проблематичным из-за сложности подготовительных работ для начала исполнения протокола, которыми могут быть загрузка каких-либо данных для работы системы, которые напрямую не связаны с протоколом, запуск подготовительных процессов обработки данных и прочее. Для того чтобы избежать лишних действий системы и проанализировать непосредственно саму реализацию только протокола используется извлечение структуры полного описания протокола [4]. В ней содержится полная информация о деталях реализации протокола, такие как использование определенной функции шифрования или генерации случайного числа, проверка возвращаемых значений. На базе полной структуры протокола необходимо построить так называемую урезанную систему. В такой системе будет содержаться только непосредственно реализованные в ней протоколы, в которых получение изначальных данных для пересылки, являющихся не случайным числом, например, когда данные получаются с клавиатуры или с диска, заменяется на тестовые данные. Кроме того, при создании урезанной версии системы несмотря на количество сторон при передаче данных добавляется еще одна сторона - злоумышленник. Все сообщения, пересылаемые

между сторонами, проходят через сторону злоумышленника, используя модель Долева-Яо. На стороне злоумышленника возможно производить любые манипуляции в рамках модели Долева-Яо. При этом критерием проверки наличия атаки является так называемый принцип ложного завершения. Он основан на использовании меток успешного завершения протокола на всех сторонах, а также сравнении отправленных данных на стороне отправителя и стороне получателя. В случае если сторона злоумышленника произвела некоторые манипуляции с передаваемыми данными, отправленные данные на стороне получателя и отправителя не совпадают, но при этом протокол был корректно исполнен на всех сторонах, то это свидетельствует о наличии атаки на протокол. В результате работы был предложен алгоритм динамического анализа, который основан на принципе ложного завершения. Динамический анализ позволит находить ранее не известные атаки на протоколы, которые не удастся обнаружить с помощью классических подходов, основанных на формальной верификации. Кроме того, анализ непосредственно реализации криптографического протокола на выбранном языке программирования позволит максимально эффективно провести верификацию, поскольку в данном случае протокол имеет уже конечную форму и существует возможность получать дополнительную информацию о протоколе непосредственно из исходного кода.

СПИСОК ЛИТЕРАТУРЫ

[1] Viganò L. Automated security protocol analysis with the AVISPA tool //Electronic Notes in Theoretical Computer Science. – 2006. – Т. 155. – С. 61-86.

[2] Cremers C. J. F. The scyther tool: Verification, falsification, and analysis of security protocols //International Conference on Computer Aided Verification. – Springer, Berlin, Heidelberg, 2008. – С. 414-418.

[3] Küsters R., Truderung T. Using ProVerif to analyze protocols with Diffie-Hellman exponentiation //Computer Security Foundations Symposium, 2009. CSF'09. 22nd IEEE. – IEEE, 2009. – С. 157-171.

[4] Бабенко Л. К., Писарев И. А. Алгоритм анализа исходного кода C# для извлечения структуры криптографических протоколов //Вопросы кибербезопасности. – 2018. – №. 4. – С. 28.

ПРОБЛЕМА ПОЛНОСТЬЮ ГОМОМОРФНОЙ ОБРАБОТКИ ЦЕЛЫХ ЧИСЕЛ*

Илья Русаловский
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
ilya.rusalovskiy@mail.ru
Людмила Бабенко
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
lkbabenko@sfedu.ru

**Работа поддержана грантом Министерства Образования и Науки Российской Федерации № 2.6264.2017/8.9.*

Криптография с давних пор обеспечивает безопасную передачу данных в незащищенной среде. Эта наука прошла огромный путь своего развития, на протяжении которого возникали новые алгоритмы, вытесняющие старые. В наше время набирают популярность такие направления криптографии, как малоресурсная криптография и гомоморфная криптография. В данном тезисе рассмотрены основные проблемы гомоморфной криптографии, возможные пути их решения, а также существующие алгоритмы полностью гомоморфного шифрования.

Гомоморфная криптография – достаточно молодое направление криптографии, основателями которого считаются авторы алгоритма RSA, которые впервые сформировали понятие «гомоморфное шифрование».

Гомоморфная шифрование – это особая форма шифрования, позволяющая выполнять определенные математические операции над зашифрованными данными без их предварительной расшифровки.

Эта особенность гомоморфного шифрования открывает огромные возможности его использования в области облачных вычислений – данные можно обрабатывать на сервере, не раскрывая их при этом. Большой вклад в дальнейшее развитие гомоморфного шифрования внес Крейг Джентри.

Именно он является автором первого полностью гомоморфного шифра. Также он внес огромный вклад в развитие и изучение проблем гомоморфного шифрования. Им были выдвинуты критерии полностью гомоморфных шифров.

Первоначально гомоморфные шифры разделялись на полностью и частично гомоморфные по критерию числа поддерживаемых операций над зашифрованными данными – сложения и умножения.

Частично гомоморфные алгоритмы поддерживают только одну операцию – или сложение или умножения, полностью гомоморфные – обе.

После разработки своего алгоритма Джентри расширил требования к полностью гомоморфным алгоритмам двумя критериями: корректность и компактность[1].

Как было сказано ранее, гомоморфное шифрование имеет огромные перспективы использования в области защищенных облачных вычислений. Нет необходимости пересылать на сервер ключ шифрования по защищенным каналам. А данные могут быть «испорчены» злоумышленником, но не могут быть расшифрованы. На данный момент сделано много разработок в области гомоморфного шифрования, созданы различные полностью и частично гомоморфные алгоритмы. Также представлены некоторые готовые реализации программных продуктов. Однако большинство из них поддерживаю обработку исключительно бит или массивов бит, но для решения прикладных задач и в сфере облачных вычислений необходима обработка целых числе, а не бит. На основании вышесказанного возникает проблема полностью гомоморфного шифрования целых чисел. Второй проблемой, которая будет рассмотрена в данном документе, является проблема гомоморфного деления.

В области гомоморфного шифрования разработаны несколько алгоритмов полностью гомоморфного шифрования. Для некоторых из них выполнены практические реализации. наибольшую известность имеют две библиотеки:

- библиотека HElib сделанная Шаем Хавели и Виктор Шоуп которая реализует криптосистему BGV с GHS оптимизацией

- библиотека FHEW, сделанная Лео Дуглас и Даниэль Миккианакио, которая является реализацией комбинации криптосистемы обучения с ошибками Регева и техники создания гибкой схемы Алперин-Шериффа и Пейкерта.

Однако они поддерживают только обработку бит. Реализация же целочисленных операций на основе гомоморфного алгоритма, обрабатывающего только биты, невозможна из-за проблемы переноса бита. При логической обработке бита результат умещается в исходной размерности, а при арифметической обработке возможен переход в старший разряд. Однако невозможно узнать, когда этот переход происходит в зашифрованных данных.

Как следует из вышесказанного, необходимо использовать алгоритмы или модификации алгоритмов, поддерживающие обработку целых чисел. Одним из таких алгоритмов является алгоритм Джентри над целыми числами. Также Джентри предлагает модификацию своего алгоритма – технологию бутстреппинга, которая снимает ограничение на число последовательных гомоморфных операций.

Ранее уже была рассмотрена проблема гомоморфного деления[2].

---

[1] C. Gentry A Fully Homomorphic Encryption Scheme. PhD thesis, Stanford University, 2009. 199 p. URL: https://crypto.stanford.edu/craig/craig-thesis.pdf

[2] Русаловский И.Д. Проблема гомоморфного деления // Студенческая наука для развития информационного общества: сборник материалов VII Всероссийской научно-технической конференции (г. Ставрополь, 26-28 декабря 2017 года). – Ставрополь, 2018. – С. 434-437.

Существующие схемы и алгоритмы гомоморфного шифрования не позволяют использовать операцию деления над зашифрованными данными. Для решения данной проблемы мной предложено использовать некую абстракцию, построенную над шифротекстом и расширяющую возможности по выполнению математических операций над ним. Для этого будет необходимо выделить два уровня представления данных – криптографический и математический. На криптографическом уровне может быть реализован любой полностью гомоморфный алгоритм шифрования над целыми числами. А на математическом уровне зашифрованные гомоморфно числа будут представлены в виде простых дробей. Все операции над числами в предложенном методе – это операции над простыми дробями, а после всех операций числитель и знаменатель необходимо расшифровать и разделить результаты. Предложенным выше способом возможна реализация гомоморфного деления, однако она не решает проблему деления на ноль. Подробнее метод гомоморфного деления будет рассмотрен в другой статье.

СПИСОК ЛИТЕРАТУРЫ:

[1] Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В. Защищенные вычисления и гомоморфное шифрование // Программные системы: теория и приложения. – 2014. – 25 с.

[2] Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В. Методы полностью гомоморфного шифрования на основе матричных полиномов // Вопросы кибербезопасности. – 2015. – С. 14-25.

[3] Гомоморфное шифрование [Электронный ресурс]. URL: https://habrahabr.ru/post/255205/ (дата обращения: 10.08.2019 г.).

[4] Полностью гомоморфное шифрование [Электронный ресурс]. – URL: http://cryptowiki.net/index.php?title=Полностью_гомоморфное_шифрование (дата обращения: 10.08.2019 г.).

[5] Русаловский И.Д. Проблема гомоморфного деления // Студенческая наука для развития информационного общества: сборник материалов VII Всероссийской научно-технической конференции (г. Ставрополь, 26-28 декабря 2017 года). – Ставрополь, 2018. – С. 434-437

АНАЛИЗ КИБЕР-ФИЗИЧЕСКИХ УГРОЗ ДЛЯ СИСТЕМ ГРУППОВОГО УПРАВЛЕНИЯ РОБОТАМИ*

Олег Макаревич
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
obmakarevich@sfedu.ru

Андрей Степенкин
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
stepenkin@sfedu.ru

** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-00212*

АННОТАЦИЯ

В данной работе производится обзор и анализ угроз, специфичных для систем группового управления роботами (СГУР), применяемыми в неконтролируемой среде. Отличительной чертой СГУР от прочих информационных систем является существование физического взаимодействия с окружающей средой. В результате этого вида взаимодействия возникают связанные с ним угрозы. В результате внешних физических воздействий может быть нарушена доступность некоторых узлов СГУР, или нарушение целостности данных, получаемых от сенсорной системы узлов. Поскольку узлы СГУР для принятия решений используют данные сенсорной системы об окружающей среде, то внешнее физическое воздействие способно оказывать влияние на результат.

КЛЮЧЕВЫЕ СЛОВА

Угрозы, атаки, мобильные роботы, групповое управление, сетевая безопасность, методика тестирования, беспроводные сети

1 ВВЕДЕНИЕ

Групповые робототехнические системы обладают высоким потенциалом в решении разнообразных задач. Такие системы крайне зависимы от условий эксплуатации. Естественная среда является недетерминированной. По этой причине система должна обладать способностью адаптироваться к изменчивым условиям. Также системы могут быть более уязвимы при эксплуатации в неконтролируемой среде. В таких условиях источник внешнего воздействия может быть естественным или искусственным. В зависимости от характера и силы воздействия может быть затруднено или нарушено выполнение поставленных целей, связь между узлами группы или работоспособность отдельных узлов.

2 СТРУКТУРА СИСТЕМЫ ГРУППОВОГО УПРАВЛЕНИЯ

Система группового управления роботами (СГУР) применяется для выполнения распределения целей и контролирования их исполнения. Для распределения целей могут использоваться различные алгоритмы [1-3]. Мобильные узлы имеют ограниченные энергетические ресурсы, что повышает важность эффек-

тивного целераспределения [4]. Под эффективностью целераспределения понимается такое разделения задач между узлами, что для их выполнения будет затрачено наименьшее количество энергетических и временных ресурсов. Для эффективного целераспределения необходимы точные сведения об узлах группы: текущее местоположение, доступные ресурсы, исполняемые функции; сведения о целях: начальное положение, изменение во времени, конечное положение; сведения о местности [5-6]: карта местности с метками о сложности перемещения через область, наличие динамических препятствий, областей со слабой связью.

Для выполнения задач каждый узел должен обладать мобильностью. Мобильность может обеспечиваться различными аппаратными платформами для различных условий: наземные колесные и гусеничные платформы; водные и подводные; воздушные планеры и мультикоптеры.

Для получения информации об окружающей среде узлы оборудуются сенсорами: системы позиционирования, инфракрасные/ультразвуковые дальномеры, лидары, датчики удара, датчики пройденного расстояния, камеры с системами компьютерного зрения и др. На основе данных с сенсоров узел может определить свое собственное положение и обновить информацию об окружающей среде.

Для обработки данных сенсоров, принятия решений по выполнению поставленных задач и участия в процессе распределения задач необходим бортовой вычислитель. Вычислитель должен обладать достаточной памятью для хранения информации, требуемой для работы в составе группы: исполняемые файлы, данные для аутентификации в группе, карта местности и др. а также достаточной мощностью для исполнения программ СГУР.

Для обмена сообщениями СГУР требуется канал связи. Как правило, применяется защищенный радиоканал. В условиях ограниченных ресурсов и габаритов приемопередатчики и антенны имеют ограниченную мощность. Следствием ограничений может быть снижение скорости передачи данных и снижение размера зоны работы приемопередатчиков.

3 КИБЕР-ФИЗИЧЕСКИЕ ВОЗДЕЙСТВИЯ НА СГУР

Воздействие на исполнительные механизмы может снизить их производительность. В результате выполнения доступных действий будет затрачено большее количество энергетических и временных ресурсов. При излишней силе воздействия механизм может быть поврежден и способность исполнять некоторые функции будет нарушена.

В общем случае применяются физические сенсоры, реагирующие на изменения в какой-либо среде: оптической, звуковой и т.д. Величина изменения может передаваться в виде аналогового или цифрового сигнала. Работоспособность сенсора может быть нарушена прямым ограничением доступа к наблюдаемой среде или повреждением сенсора. Данные, передаваемые сенсором, могут быть

искажены путем создания помех в наблюдаемой среде.

В случае перехвата узла сенсорная система может подвергнуться модификации. В случае несанкционированной модификации данные могут подменяться злоумышленником для воздействия на процесс принятия решения и нарушения работы отдельного узла или всей СГУР.

Защитить используемый радиоканал от внешнего воздействия в неконтролируемой среде невозможно. Взаимодействия с радиоканалом можно разделить на два вида: пассивное и активное. При пассивном взаимодействии производится прослушивание канала и сохранение передаваемых сообщений. При передаче сообщений по радиоканалу в общем случае используется шифрование. В зависимости от параметров используемого радиоканала существует угроза расшифровки сообщений и нарушения конфиденциальности. Перехваченные сообщения без расшифровки могут использоваться для определения местоположения узлов, количества узлов, иерархии среди узлов, маршрутов передачи данных, интенсивности участия в групповом взаимодействии.

Активное воздействие на радиоканал предполагает использование передатчиков и вмешательство во взаимодействие узлов. Оно может осуществляться путем проведения сетевых атак и зашумления канала связи. В результате зашумления канала скорость передачи данных в сети может быть снижена или сеть может быть недоступна. Размер области с нарушениями доступности зависит от используемого оборудования на узлах и мощности генератора шума.

Узлы, эксплуатируемые в неконтролируемой зоне, могут быть перехвачены злоумышленником. Захваченные узлы могут подвергнуться обратному инжинирингу программной и аппаратной платформы, извлечению и анализу информации, хранящейся в ОЗУ и ПЗУ. Также захваченный узел может быть подвергнут несанкционированной модификации программного и аппаратного обеспечения. Модифицированный узел может быть возвращен в группу для нарушения эффективности и работоспособности СГУР.

Окружающая среда, в которой размещена СГУР, может содержать естественные и искусственные препятствия, среди которых могут присутствовать динамические. Эти препятствия могут изменить свое положение или форму находясь за пределами сенсоров любого из узлов, что приведет к несоответствию имеющейся карты проходимости и реальной обстановки. В результате таких изменений могут стать недоступными выбранные ранее маршруты, либо возникнуть новые более оптимальные. Преднамеренное изменение положения и количества препятствий может привести к повышенным расходам ресурсов или полной блокировки отдельных узлов.

4 ЗАКЛЮЧЕНИЕ

Представленные выше воздействия на СГУР способны затруднить или приостановить выполнение поставленных задач. Эти воздействия не предполагают

непосредственного информационного вмешательства, что делает их не обнаружимыми для классических систем обнаружения вторжения. В результате оказания некоторых из перечисленных воздействий может быть нарушена целостность информации без нарушения аутентичности сообщений и конфиденциальности. Узлы могут подвергаться физическому воздействию на исполнительные механизмы, что может быть расценено как атака на исчерпание ресурсов. Из всего вышесказанного следует, что для СГУР существует угроза неинформационного воздействия, способная нарушить выполнение поставленных задач, и классических средств обеспечения безопасности может быть недостаточно.

СПИСОК ЛИТЕРАТУРЫ

[1] Dobroczynski D. Multi-agent behavioral control system for a group of mobile robots //Proceedings of the Second International Workshop on Robot Motion and Control. RoMoCo'01 (IEEE Cat. No. 01EX535). – IEEE, 2001. – С. 115-119.

[2] Cognetti M. et al. Cooperative control of a heterogeneous multi-robot system based on relative localization //2014 IEEE/RSJ International Conference on Intelligent Robots and Systems. – IEEE, 2014. – С. 350-356.

[3] Lucidarme P., Simonin O., Liégeois A. Implementation and evaluation of a satisfaction/altruism based architecture for multi-robot systems //Proceedings 2002 IEEE International Conference on Robotics and Automation (Cat. No. 02CH37292). – IEEE, 2002. – Т. 1. – С. 1007-1012.

[4] Wu D. et al. Gini coefficient-based task allocation for multi-robot systems with limited energy resources //IEEE/CAA Journal of Automatica Sinica. – 2017. – Т. 5. – №. 1. – С. 155-168.

[5] Dissanayake G., Durrant-Whyte H., Bailey T. A computationally efficient solution to the simultaneous localisation and map building (SLAM) problem //Proceedings 2000 ICRA. Millennium Conference. IEEE International Conference on Robotics and Automation. Symposia Proceedings (Cat. No. 00CH37065). – IEEE, 2000. – Т. 2. – С. 1009-1014.

[6] Howard A. Multi-robot simultaneous localization and mapping using particle filters //The International Journal of Robotics Research. – 2006. – Т. 25. – №. 12. – С. 1243-1256.

ОБНАРУЖЕНИЕ НЕИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА СИСТЕМЫ ГРУППОВОГО УПРАВЛЕНИЯ РОБОТАМИ*

Олег Макаревич
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
obmakarevich@sfedu.ru

Андрей Степенкин
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
stepenkin@sfedu.ru

** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-00212*

АННОТАЦИЯ

В данной работе предлагается дополнение к системам обнаружения вторжения на основе доверия для систем группового управления роботами (СГУР), позволяющее определять внешнее неинформационное воздействие. Неинформационное воздействие на СГУР становится возможным по причине существования физического взаимодействия с окружающей средой. Для обеспечения этого взаимодействия узлы СГУР обладают сенсорной подсистемой для получения информации о среде и исполнительные механизмы для воздействия на среду. Неинформационное воздействие может оказывать влияние на информацию, получаемую от сенсорной системы: искажение или подмена, или вызывать повышенный расход энергетических ресурсов. Обнаружение неинформационного воздействие может осуществляться на основе различий в наблюдаемых сенсорами параметрах и перекрестной проверки узлами друг друга. Отличительной особенностью дополнения является существование доверия между узлами, а также между каждым узлом и областям среды.

КЛЮЧЕВЫЕ СЛОВА

Угрозы, атаки, мобильные роботы, групповое управление, сетевая безопасность, методика тестирования, беспроводные сети, доверие, неинформационное воздействие, обнаружение вторжения

1 ВВЕДЕНИЕ

Системы группового управления роботами могут эксплуатироваться в различных средах. При применении СГУР в неконтролируемых средах возникают угрозы неинформационного воздействия на узлы – воздействие посредством изменения окружающей среды, несанкционированная модификация узлов и воздействие на сенсорную систему узлов для манипулирования СГУР.

Трудности обеспечение безопасности в таких условиях связаны со сложностью выделения четких критериев, позволяющих отличить преднамеренное деструктивное воздействия и естественные изменения, влияния среды. Поскольку решаемые СГУР задачи связаны с физическими взаимодействиями и перемещениями в пространстве, то негативные эффекты могут быть значительно удалены

во времени от оказываемого воздействия. Для обеспечения безопасности в подобных условиях наиболее перспективными будут подходы, комбинирующие методы на основе обнаружения аномалий и методы на основе доверия и репутации.

2 ДОВЕРИЕ И СИСТЕМЫ ГРУППОВОГО УПРАВЛЕНИЯ

Доверие и репутация являются количественной величиной, обозначающей надежность выбранного объекта [1]. Доверие ко всем объектам рассчитывается каждым узлом самостоятельно на основе наблюдаемых параметров. Репутация – параметр, значение которого формируется на основе доверия третьих субъектов к выбранному объекту [2]. В пределах одного субъекта значение доверия и репутации к одному объекту может отличаться. Показатели доверия изменяются в соответствии с выбранным алгоритмом как реакция на действия наблюдаемых объектов [3]. Для эффективного целераспределения [4] в СГУР необходимо на момент принятия каждого решения обладать актуальными сведениями обо всех узлах. Можно выделить следующие сведения: текущее местоположение узла, его ориентация в пространстве, текущая скорость, траектория движения, текущая задача, оставшиеся энергетические ресурсы, текущее энергопотребление. При наличии аппаратных средств, таких как системы компьютерного зрения, радио или оптические метки, уровень сигнала при передаче сообщений, некоторые из сведений могут подтверждаться другими узлами. Для распределения целей и осуществления перемещения в пространстве для СГУР необходимо обладать сведениями об окружающей среде, доступных для передвижения областях и существующих препятствий. При эксплуатации в неконтролируемой среде положение, размер и количество препятствий может изменяться, поэтому узлы СГУР должны иметь сенсоры для обнаружения препятствий и обновления итоговой карты препятствий [5-6]. Обо всех наблюдаемых изменениях должны оповещаться все остальные узлы СГУР. Другие узлы должны оповещаться обо всех наблюдаемых событиях. Наибольшей важностью обладают события, связанные с подтверждением и опровержением имеющихся сведений. Поскольку каждое из возникших событий могло произойти под действием со стороны окружающей среды, то эти события должны содержать метку о месте и времени возникновения. Все последующие решения, принимаемые узлом во время решения задач, должны указывать на произошедшие события, повлиявшие на выбранное решение. Таким образом все действия узлов СГУР должны сформировать граф. На этом графе существуют следующие типы вершин:

узлы – роботы, являющиеся частью СГУР;

- пространственные метки – области в среде, около которых возникают события;

- информация – сведения, полученные от сенсорной системы одного из узлов, имеет связь с узлом, сгенерировавшим информацию, и пространственной меткой, вблизи которой она была сгенерирована. Может содержать обновление

сведений о препятствиях, наблюдение за точками интереса СГУР, пересечение с другим узлом, изменение собственных параметров и др.;

- действия – решения, принятые узлом для выполнения задач, поставленных перед СГУР, данная вершина имеет связи с узлом, информацией и пространственной меткой;

- конфликты и подтверждения – при добавление новых вершин, имеющих противоречия с уже существующими, должна формироваться конфликтная ситуация и наоборот должны помечаться факты подтверждения имеющихся сведений.

При возникновении конфликта может быть построено дерево узлов причастных к этому инциденту. Данная структура позволит производить определение атак на основе изоморфизма между деревьями нескольких инцидентов. Также из различных инцидентов статистически могут быть выделены узлы – источники конфликтов.

3 ЗАКЛЮЧЕНИЕ

Неинформационное воздействие – вид угроз, специфичный для робототехнических средств. Классические средства защиты не предназначены для таких условий. Здесь была предложена структура, которая должна обеспечить обнаружение внешних воздействий на основе поведения отдельных узлов, выявления аномалий в их поведении и поиска источника этих отклонений. Источником может являться узел, являющийся частью СГУР, который подвергся несанкционированной модификации, либо получил повреждения в ходе решения задач. Также источником может являться среда, в которой функционирует СГУР. Можно предположить, что если источником аномалий является среда, то события будут сгруппированы в определенных областях и воздействию подвергнуться различные узлы, находящиеся в этой области. Таким образом, в системе расчета доверия и репутации должны отражаться не только узлы, принадлежащие СГУР, но и точки, принадлежащие окружающей среде. Эти показатели доверия к среде могут использоваться при построении траекторий движения и распределении задач между узлами для избегания внешних воздействий. Еще одним способом применения доверия может быть перераспределение узлов для проверки подозрительных объектов. Можно выделить два способа перераспределения: узел с высоким уровнем доверия может быть направлен в область с большим количеством конфликтных ситуаций для их разрешения, либо узел, являющийся источником многих конфликтных ситуаций, может быть перенаправлен в область с другими узлами, имеющими высокий уровень доверия. Так как защита СГУР от неинформационных воздействий во многом полагается на перекрестную проверку между узлами, то таким образом можно сформировать обратную связь от системы доверия к СГУР для повышения количества и качества этих проверок.

СПИСОК ЛИТЕРАТУРЫ

[1] Zahariadis T. et al. Trust management in wireless sensor networks //European Transactions on Telecommunications. – 2010. – Т. 21. – №. 4. – С. 386-395.

[2] Ebinger P., Bißmeyer N. TEREC: Trust evaluation and reputation exchange for cooperative intrusion detection in MANETs //2009 Seventh Annual Communication Networks and Services Research Conference. – IEEE, 2009. – С. 378-385.

[3] Bao F. et al. Trust-based intrusion detection in wireless sensor networks //2011 IEEE International Conference on Communications (ICC). – IEEE, 2011. – С. 1-6.

[4] Wu D. et al. Gini coefficient-based task allocation for multi-robot systems with limited energy resources //IEEE/CAA Journal of Automatica Sinica. – 2017. – Т. 5. – №. 1. – С. 155-168.

[5] Montemerlo M. et al. FastSLAM: A factored solution to the simultaneous localization and mapping problem //Aaai/iaai. – 2002. – Т. 593598.

[6] Tan W. et al. Robust monocular SLAM in dynamic environments //2013 IEEE International Symposium on Mixed and Augmented Reality (ISMAR). – IEEE, 2013. – С. 209-218

КРАТКИЙ ОБЗОР СОВРЕМЕННЫХ ПРОБЛЕМ МОБИЛЬНЫХ РОБОТОВ

Екатерина Толоманенко
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
kattea@mail.ru

АННОТАЦИЯ

Робототехнические системы различного вида проникают во все сферы жизнедеятельности человека. Технологии не стоят на месте, позволяют совершенствоваться как разработчикам, создающим такие системы, так и злоумышленникам, которые активно исследуют предлагаемые технологии на предмет наличия уязвимостей в системе и затем используют данные уязвимости с целью получения материальной выгоды.

Наиболее часто в последнее время мы сталкиваемся с мобильной робототехникой, а именно: квадрокоптеры, дроны, беспилотные летательные аппараты используются как в повседневной жизни, так и в коммерческих целях, и, даже в военизированных направлениях. Также распространены такие системы, как «умный дом» или «умный город», не относящиеся к мобильным.

КЛЮЧЕВЫЕ СЛОВА

Криптография, мобильная робототехника, компьютерные сети, сенсорные

сети.

1 ОБЗОР ЛИТЕРАТУРЫ

Система «Умный дом» [1] позволяет объединить в себе все возможные системы жизнеобеспечения, запрограммировать их взаимодействие между собой, осуществлять контроль над домом, наблюдать за домом через Интернет или удалённое видеонаблюдение с учетом всех потребностей хозяина. Из этого можно сделать вывод, что будет обрабатываться всевозможная конфиденциальная информация, передаваться по сети Интернет, а также между всеми датчиками, расположенными в доме, с помощью, например, сенсорной сети. На данном этапе возникает вопрос защищенности такой системы, как обезопасить все потенциально уязвимые данные о доме, которые может перехватить злоумышленник и навредить их владельцу. Система «умный город» [2], очевидно, содержит во много раз больше конфиденциальных данных, которыми может завладеть злоумышленник, что может нанести урон не только большой группе людей, но и городской инфраструктуре в целом.

Что касается мобильной робототехники, то речь может идти об одиночных аппаратах и групповой робототехнике. Групповая робототехника [3], или рой роботов представляет собой коллективное взаимодействие участников между собой, при этом поведение каждого участника регулируется в соответствии с поведением других участников и особенностями окружающей их среды.

Все участники роя, как правило, взаимодействуют друг с другом с помощью беспроводной сети, которая может стать объектом взлома.

В работе [4] описывается моделирование атаки на один из алгоритмов взаимодействия мобильных роботов, так называемый муравьиный алгоритм. По полученным результатам моделирования авторы выяснили, что в первую очередь реализацию данного алгоритма необходимо дополнить механизмами информационной безопасности.

2 СУЩЕСТВУЮЩИЕ ДОПОЛНЕНИЯ МЕХАНИЗМОВ БЕЗОПАСНОСТИ

Одно из главных существующих дополнений механизмов безопасности, предложенных авторами работы [4] – это механизм защиты от аномалий, отслеживание и выявление возникающих не декларированных ситуаций в системе.

Следующая проблема связана с проблемой аутентификации роботов в рое, возникает необходимость в уточнении «своего» или «чужого» участника в рое. При этом алгоритм аутентификации необходим не только на этапе организации роя, существует потребность в периодической аутентификации ключевых участников группы, так как они могут быть скомпрометированы злоумышленником. Как известно, процесс аутентификации является достаточно ресурсоемким, поэтому необходима такая схема, которая позволит мобильным участ-

никам группы тратить минимальное количество энергии для аутентификации друг друга.

Также авторы отмечают необходимость в дополнении системы защитой от компрометации ключей по побочным каналам, в случае если кто-либо из участников окажется вне контролируемого периметра. Если злоумышленник перехватит летательный аппарат, то это позволит ему перехватить ключ, например, сняв диаграмму энергопотребления.

3 ВОЗМОЖНЫЕ ВАРИАНТЫ РЕШЕНИЯ ПОСТАВЛЕННЫХ ПРОБЛЕМ

Исходя из проанализированных вышеперечисленных источников, можно предложить несколько путей, позволяющих решить поставленные проблемы, связанные с безопасностью робототехнических систем, в том числе и мобильных робототехнических систем. Некоторые проблемы можно решить, например, с помощью применения схемы гомоморфного шифрования [5] – способа, позволяющего выполнять над шифртекстами математические операции и получать зашифрованный результат, который будет соответствовать результатам выполнения тех же математических операций над открытым текстом. Но главная проблема гомоморфного шифрования состоит в том, что он потребляет много ресурсов, поэтому существующие схемы не могут быть использованы в мобильной робототехнике.

Вторым вариантом защиты мобильных роботов является малоресурсная криптография. Данный вид шифрования используется для шифрования и, например, хранения конфиденциальной информации в памяти робота, как правило в ППЗУ. Все процессы зашифрования и расшифрования осуществляются с минимизацией затрат энергии, что является удобным и актуальным свойством. К сожалению, малоресурсные алгоритмы не решают проблемы авторизации, они не позволят определить участникам, кто из них «свой», а кто «чужой». Но при этом при правильном подборе криптографического ключа взлом легковесного алгоритма может оказаться для злоумышленника слишком трудоемкой задачей и это не позволит ему перехватить хранимую в ППЗУ секретную информацию.

СПИСОК ЛИТЕРАТУРЫ

[1] Домашняя автоматизация [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Домашняя_автоматизация

[2] Умный город [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Умный_город

[3] Групповая робототехника [Электронный ресурс]. URL: https://ru.wiki-pedia.org/wiki/Групповая_робототехника

[4] Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики, 2013, № 5 (87)

[5] Гомоморфное шифрование [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Гомоморфное_шифрование

РАЗРАБОТКА СИСТЕМЫ АНАЛИЗА И ВЕРИФИКАЦИИ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ (IOC)

Денис Туманов
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
dtampli@yandex.ru
Евгений Абрамов
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
abramoves@sfedu.ru

АННОТАЦИЯ

В статье рассматриваются некоторые базовые требования к разработке системы сбора и анализа индикаторов компрометации (Threat Intelligence Platform, TIP).

КЛЮЧЕВЫЕ СЛОВА

Индикатор компрометации, анализ угроз, информационная безопасность, Indicators of Compromise, IoC, Threat Intelligence Platform, TIP.

1 ТРЕБОВАНИЯ К АРХИТЕКТУРЕ TIP

Сам процесс киберразведки можно отобразить в форме цикла, который включает в себя 5 ключевых этапов [1]:

1) На этапе планирования устанавливаются цели, требования к получаемой информации и расставляются приоритеты.

2) Этап сбора включает в себя различные этапы деятельности по сбору информации для удовлетворения поставленных на первом этапе целей. Кроме собственных источников информации, на этом этапе используются и данные провайдеров Threat Intelligence, среди которых можно выделить такие компании, как Group-IB, Palo Alto, ESET, Kaspersky Lab, FireEye и др.

3) На этапе обработки собранные исходные данные интерпретируются, транслируются и унифицируются.

4) Подготовка данных включает в себя процесс уточнения и слияния информации, обработанной на предыдущем этапе.

5) Заключающим этапом цикла становится распространение информации

конечным потребителям, в роли которых могут выступать как внешние потребители, так и собственные подразделения ИБ в филиалах, дочерних и зависимых бизнес-единицах компании.

Для автоматизации этого цикла используются специализированные платформы — Threat Intelligence Platform (сокр. TIP).

Некоторые инциденты безопасности могут быть достаточно сложными, требующими расширенного анализа и обратного инжиниринга. Когда все эти образцы собраны, то результат называют индикатором компрометации (Indicator of Compromise, IOC). IOC – это активность и/или вредоносный объект, обнаруженный в сети или на конечной точке, который можно идентифицировать и, таким образом, улучшить возможности по обнаружению будущих атак.

В качестве источников данных об индикаторах компрометации TI-система должна уметь рассматривать:

–информацию от производителей СЗИ,

–информацию из третьих источников об обнаруженных уязвимостях в СЗИ,

–фиды и твитер-каналы (в т.ч. для предыдущих источников) исследователей уязвимостей,

–OSINT и IOC фиды (в формате OpenIOC, STIX/TAXII),

–российские подписные фиды ГосСОПКА, ФинЦЕРТа, Касперский, BI.ZONE, Group-IB,

–базы сигнатур (Snort-style, ET-open, Talos),

–Telegram-каналы и формирование IOC аналитиком,

–проверка в Sandbox или VirusTotal и формирование IOC аналитиком,

–данные журналов регистрации событий (системные и сетевые) – предобработка/агрегация фильтрами, формирование IOC аналитиком.

В качестве Open Source решения, которое может служить точкой сбора, агрегирования и обработки данных, могут выступать:

1. GOSINT [2]. Решение по автоматизации сбора, проверки индикаторов компрометации и их передаче в систему обработки.

Преимущества - открытый код, неограниченное число источников, поддержка API (Cisco Umbrella, VirusTotal, Twitter API), возможность шаблонизации проверки полученных IOC, консолью управления на JavaScript.

Недостатки - регулярные обновляет GOSINT, необходимость поддержки. Сложность с использованием в КИИ.

2. Spiderfoot [3].

Преимущества - предназначен для сбора информации о подозрительных вредоносных IP, автоматизирует стадию сбора информации по цели для обогащения IOC. Сохранение результатов в SQLite. Пользовательский интерфейс основан на вебе. Модульность. Любой законченный функционал - модуль, написанный на Python. Визуализация. Встроенная визуализация, основанная на JavaScript, возможность экспорта в GEXF/CSV для использования в других инструментах,

например, в Gephi.

Недостатки - ориентирован больше на сбор информации с целевых адресов и поиск уязвимостей, а не на работу с фидами.

3. Apache Metron (Cisco OpenSOC) [4]. Платформа для анализа больших данных в области кибербезопасности.

Достоинства - агрегирует несколько open-source решений по Threat Intelligence, включая Flume - распределенный инструмент для сбора и агрегации больших объемов данных из разных источников в разных форматах (Syslog, SNMP, Netflow, JMS, HTTP, файлы, PCAP и т.д.), Kafka, Storm, Elasticsearch и другого ПО для организации параллельной обработки и поиска по сообщениям.

Недостатки - большой сложный проект, включающий в т.ч. излишние для нашей задачи функции. Потенциально большая сложность освоения.

В целом, мы считаем оптимальным выбором продукт GOSINT.

Для сбора данных мы предлагаем следующие решения:

– ввод данных через API (Cisco Umbrella, VirusTotal, Twitter API, другие API),

– парсинг фидов,

– автоматический ввод данных, собранный с сайтов с помощью краулеров, построенных на Scrapy,

– ручной ввод данных, собранных.

2 ВЕРИФИКАЦИЯ IOC

Система TI требует проведения проверки сообщения и содержимого, и может предоставлять автоматизированную проверку, инструментарий для ручной проверки, или оба варианта.

Существует ряд необходимых шагов проверки, которые необходимо выполнить, прежде чем использовать индикаторы, полученные при ручном обмене. Эти шаги также могут быть применены к автоматической обработке.

Вопросы, на которые надо получить ответы при верификации сообщения об IOC [5]:

1. Проверка источника сообщения - автоматически.

2. Связаться с отправителем IOC по отдельному каналу связи - руками

3. Проверка целостности сообщения с IOC – автоматически

4. К какой компании (текущей или исторической) по распространению малвари относятся полученные IOC – автоматически, поиск - по ключевым словам, + ручная

5. Относится ли IOC к целевым секторам, в которые входит организация? – автоматически + руками

6. Каков уровень сложности атаки? Уязвимости ПО или социальная инженерия/фишинг - вручную

7. Цель злоумышленников - нарушить работу или кража конфиденциальной

информации? Вручную

8. Если рассматривается несколько IOC - есть ли связь между индикаторами? Должны ли они быть объединены или использованы как отдельные объекты? Автоматически с дополнительной ручной проверкой

9. Какие временные рамки применяются? Необходимо ли использовать архивную информацию? - автоматически

10. Существует ли конкретная среда для практического применения индикаторов? Необходимо ли их проверить в песочнице, на рабочих станциях, серверах или определенных устройствах, или сетях? Вручную, можно попробовать автоматически по анализу сообщения

11. Какова ожидаемая реакция на индикатор – блокирование/изоляция либо дополнительный анализ поведения? Блокирование вручную с дополнительной проверкой источника, анализ поведения – автоматически.

СПИСОК ЛИТЕРАТУРЫ

[1] Автоматизация процессов кибер-разведки на основе решений класса Threat Intelligence Platform (TIP) https://www.anti-malware.ru/practice/methods /threat-intelligence-platform#part32.

[2] The GOSINT framework, https://github.com/ciscocsirt/GOSINT

[3] Spiderfoot, http://www.spiderfoot.net/download/.

[4] Apache Metron (Cisco OpenSOC), https://metron.apache.org/.

[5] Raise the Red Flag: Guidelines for Consuming and Verifying Indicators of Compromise, https://securityintelligence.com/raise-the-red-flag-guidelines-for-consuming-and-verifying-indicators-of-compromise

SECURE SYSTEM FOR THE TRANSMIT OF CONFIDENTIAL INFORMATION BASED ON THE PRINCIPLE OF VLC TECHNOLOGY

Lyudmila Babenko
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
lkbabenko@sfedu.ru
Dmitry Alexeev
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
dalekseev@sfedu.ru
Alexandr Shumilin
Department of Information Technology Security
Southern Federal University, Taganrog, Russia
sasha.shumilin42@gmail.com

ABSTRACT

In this article, the application of VLC technology based on the use of visible optical radiation for information transmission is considered. The relevance of using the technology under consideration while providing secure data transfer is justified.

KEYWORDS

Information security, visible light, technology, transmitting data, confidential data.

1 INTRODUCTION

The transfer of information using Wi-Fi networks in organizations is one of the most vulnerable places for unauthorized access by attackers to information. The VLC (visible light communication) data transmission method is considered as one of the approaches to solving the problem of high vulnerability of a corporate network.

2 STRUCTURE OF VLC TECHNOLOGY

The basis of VLC technology is an open optical communication system in which the transmitting module is mounted in the lighting system of the serviced room [1, 2].

The principle of VLC technology in a room that requires an increased level of information security shows on Figure 1.

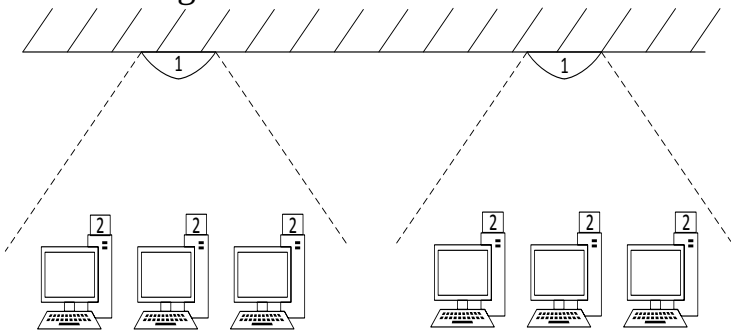

Figure 1: The principle of operation of VLC technology indoors (1-transmitting module; 2-receiving module)

Proof. In the process of using Wi-Fi networks, the potential risk zone can be 10-30 meters.

Using the organization of a corporate network based on VLC technology, you can reduce such zone to several meters. The structural diagram of the VLC-system is shown in Fig. 2.

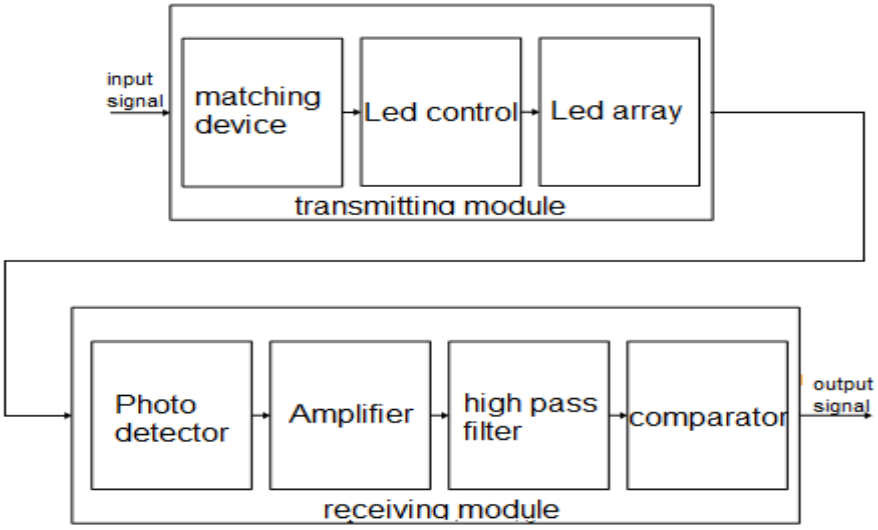

Figure 2: System block diagram implementing VLC technology

The transmitting module consists of a matching device, which converts the parameters of the input digital signal to parameters suitable for controlling the LED block using the corresponding control device.

Thanks to the photodetector, the optical signal is converted into an electric signal in the receiving module on the subscriber unit and amplified by power through a signal amplifier. The high-pass filter (HPF) allows you to get rid of unwanted noise. The comparator is installed at the circuit output to convert the analog signal to digital.

Thus, the method of signal transmission based on VLC technology is potentially more relevant than existing Wi-Fi solutions in terms of information security and can form the basis of a secure corporate network.

ACKNOWLEDGMENTS

The team of authors is grateful to Lyudmila Klimentyevna Babenko, supervisor of studies, for valuable advice in planning the study and recommendations for the design of the article.

REFERENCES

[1] Sindhubala and B. Vijayalakshmi. Design and implementation of visible light communication system in indoor environment // ARPN Journal of Engineering and Applied Sciences. - VOL. 10. №. 7. - 2015. – pp. 2282-2286

[2] Jitender Singh and Jitender Vikash. A New Era in Wireless Technology using Light-Fidelity// International Journal of Recent Development in Engineering and Technology. - Volume 2. Issue 6. – 2014. –pp. 46-49

ПРИНЦИПЫ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ СИСТЕМ ОБНАРУЖЕНИЯ АТАК*

Симон Симаворян
Кафедра прикладной математики и информатики
Сочинский государственный университет, г. Сочи
simsim58@mail.ru
Арсен Симонян
Кафедра прикладной математики и информатики
Сочинский государственный университет, г. Сочи
oppm@mail.ru
Елена Улитина
Кафедра прикладной математики и информатики
Сочинский государственный университет, г. Сочи
elenaulitina@mail.ru

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

Аннотация. Решается задача формирования принципов построения интеллектуальных систем управления деятельностью систем обнаружения атак на базе системно-концептуального подхода с использованием принципа минимальной сложности.

Ключевые слова. Интеллектуальные системы управления защитой информации, нейросетевые системы обнаружения атак, принцип минимальной сложности.

На основе системного подхода к проектированию систем защиты информации [1], а также анализа методов, алгоритмов и мероприятий интеллектуального противоборства злоумышленников и службы защиты информации в АСОД [2] можно сформулировать базовую последовательность принципов построения перспективных интеллектуальных систем управления деятельностью различных систем обнаружения атак (СОА).

В настоящее время, одним из перспективных направлений является направление разработки систем защиты информации на основе нейросетевых систем обнаружения атак и механизмов искусственных иммунных систем, которая характеризуется переходом от парадигмы адаптивного раздельного управления деятельностью СОА к парадигме интегрированного интеллектуального управления на базе системного подхода [3,4,5,6]. На основе анализа принципов, методов и алгоритмов построения интеллектуальных систем управления АСОД можно

сформулировать базовую концепцию построения перспективных интеллектуальных систем управления защитой информации, основанную на применении основополагающих системных принципов:

Сформулируем перечень этих основных принципов:

1) принцип построения единой интегрированной интеллектуальной системы управления защитой информации от несанкционированных атак как во внешней зоне защиты, так и во внутренней зоне защиты информации в АСОД, по стандартизированным технологиям обработки информации на различных этапах жизненного цикла АСОД. Для корректной постановки и решения задач проектирования интегрированных систем защиты информации в АСОД, в рамках предложенной в [1,2] концепции, требуется разработка универсальных моделей, алгоритмов и методик систем управления защитой информации, обеспечивающих минимизацию сложности проектных решений на основе энтропийного подхода к оценке и оптимизации показателей защищённости информации и сложности алгоритмов управления защитой информации.

2) принцип согласования режимов работы всех подсистем управления защитой информации при условии выполнения концептуальных требования к основным конструктивным элементам системы управления защитой информации, а именно полноты выполняемых функций управления защиты, адекватности задач управления защитой, надёжности средств управления защитой и адаптируемости к изменяемой внешней и внутренней среде.

3) принцип иерархической организации обработки поступающих запросов в АСОД, означающий построение системы управления для отражения атак извне с помощью СОА, т.е. на этапе поступления запросов на обработку, так и на этапе завершения их обработки с помощью процесса мониторинга состояния системы после обработки запроса. Процесс мониторинга осуществляется с целью выявлению необнаруженных злоумышленных атак. Это означает построение многоуровневой иерархической системы управления с разделением (декомпозицией) ее на уровни во всех типовых структурных компонентах АСОД, отличающиеся выбором целей управления, средствами и методами реализации. А именно на следующие уровни:1) уровень планирования, обеспечивающий выбор средств и механизмов управления исходя из текущей ситуации в условиях неопределенности; 2) уровень координации, обеспечивающий адаптацию характеристик защищенности информации к изменениям внешней и внутренней среды, координацию работы подсистем нижнего уровня и реконфигурацию этих подсистем при изменении ситуации управления; 3) исполнительный уровень, обеспечивающий активное управление защитой информации при полном и динамическом взаимодействии службы защиты информации с подсистемами защиты информации во всех режимах функционирования АСОД;

4) принцип комплексного применении как стандартных методов управления защитой информации, так и новых методов интеллектуального управления защитой информации на основе нейронных сетей, нечеткой логики, генетических алгоритмов и др. полагающий выбор наиболее простой структуры алгоритмов

управления защитой информации с учетом изменения защищённости информации и условий защиты информации;

5) принцип минимальной сложности [7], предполагающий выбор наиболее простой структуры алгоритмов интеллектуального управления защитой информации с учетом изменения режимов работы системы защиты информации, внешних и внутренних условий функционирования АСОД при оптимальном использовании организационных, информационных, лингвистических, аппаратно-программных, нормативно-правовых и вычислительных ресурсов системы управления.

СПИСОК ЛИТЕРАТУРЫ

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

2. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян Р.А. Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД // Известия Сочинского государственного университета. 2014. № 4-1 (32). С. 15-23.

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

4. Симаворян С.Ж., Симонян А.Р., Кочконян Р.Э. Задача обнаружения злоумышленных действий в АСОД с помощью нейронных сетей // В сборнике: Актуальные задачи математического моделирования и информационных технологий Материалы Международной научно-практической конференции. Научные редакторы Ю.И. Дрейзис, И.Л. Макарова, А.Р. Симонян, Е.И. Улитина. 2017. С. 94-96.

5.Симаворян С.Ж., Симонян А.Р., Копьева В.В. Задача обнаружения злоумышленных действий в ВСИС с помощью иммунных систем // В сборнике: Актуальные задачи математического моделирования и информационных технологий Материалы Международной научно-практической конференции. Научные редакторы Ю.И. Дрейзис, И.Л. Макарова, А.Р. Симонян, Е.И. Улитина. С. 91-94.

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

7. Васильев В.И., Валеев С.С. Проектирование интеллектуальных систем управления ГТД на основе принципа минимальной сложности // Вестник Уфимского государственного авиационного технического университета. 2007. Т. 9. № 2. С. 32-41.

ОСОБЕННОСТИ ВЕДЕНИЯ КИБЕРВОЙН

В. Ахметшин
Кафедра информационных технологий
Сочинский государственный университет, г. Сочи
avr3000@mail.ru
Т.Л. Салова
Кафедра информационных технологий
Сочинский государственный университет, г. Сочи
salova@mail.ru

Аннотация. Приводится анализ такого современного феномена, как информационные войны или кибервойны. Выявляются особенности их ведения и приводится перечень задач для обеспечения защиты и предотвращения.

Ключевые слова: кибервойна, информационная война, кибератаки, киберпространство, обеспечение кибербезопасности.

Кибервойна - лишь одно из проявлений информационной войны, получившее в связи с расширением виртуального информационного пространства (киберпространства) все права на самостоятельное существование.

Термин «информационная война» достаточно молод. Он появился в на-шем лексиконе приблизительно в середине семидесятых. На Западе отцом термина «информационная война» называют ученого-физика Томаса Рона, который в 1976 (разгар «холодной войны») назвал информацию самым слабым звеном вооруженных сил и обороны.

Под информационной войной многие понимают ведение действий против информационных систем и современных информационных технологий с помощью все тех же информационных систем и технологий. Возможно, следует рассматривать информационную войну немного шире: в качестве информационного оружия может выступать и дезинформация противника, и ведение направленной пропаганды.

Одно из определений информационной войны гласит: «Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой нашей собственной информации и информационных систем» [1].

Сегодня внимание в основном направлено на всевозможные уязвимости систем, то и дело возникающие в условиях возрастающей информатизации политической и военной сферы современного государства. Объектами, интересующими

военных, стали любые информационные системы, включая линии передач, информационные центры, людей, связанных с такими объектами, и информационные технологии, использующиеся в современных системах вооружения. Состояние современной инфраструктуры таково, что даже незначительное изменение информационного объекта может привести к выходу из строя всей системы. Например, в энергетике блокирование информационных центров может повлечь за собой, если не ядерную катастрофу, то, по крайней мере, прекращение подачи электроэнергии в города или целые районы.

Для предотвращения подобных действий необходимо строить и постоянно модифицировать системы защиты информационных ресурсов. Однако некоторые государства, помня о том, что лучшая оборона - это нападение, не ограничиваются развитием пассивной составляющей информационной защи-ты, создавая специальные военные формирования для проведения кибератак на информационные системы предполагаемого противника. Так, интересы военных все больше перемещаются из реального мира в киберпространство.

Кибервойна основана на действиях, направленных на уничтожение, блокирование или модификацию информации телекоммуникационных систем. Это война без прямых человеческих жертв: здесь не встречаются армии, нет рукопашных, нет раненых. Противник может до определенной поры даже не догадываться о том, что война против него в полном разгаре.

Кибервойна дошла и до социальных сетей, пользователи которых интересуются последними событиями, происходящими в мире. Именно там ведутся активные информационные бои, направленные на изменение сознания человека с тем, чтобы он начал ставить под сомнение интересы и позицию властей своей страны. Нередко для этого в социальные сети вбрасывается провокационная дезинформация.

Независимо от вида атаки, почти никогда нельзя точно выяснить, кто именно выступает организатором кибердудара: хакеры-одиночки, организованные хакерские группы либо государственные структуры.

Арсенал кибервойны составляют «изящные» формы вооружения: различные виды компьютерных атак, позволяющие пробраться в атакуемую сеть, компьютерные вирусы, позволяющие модифицировать и уничтожать информацию (данные или программы) или блокировать работу вычислительных систем.

И это оружие очень дешево. Кибероружие позволяет значительно снизить военные расходы, так как компьютеры намного дешевле кораблей и самолетов, а успешные операции на электронном поле боя с лихвой окупят затраты на защиту собственных информационных ресурсов.

Кибервойна дает возможность ведения военных действий малыми силами, которые к тому же могут быть распределены (децентрализованы) и тщательно замаскированы, существенно затрудняя тем самым их обнаружение и уничтожение.

Кибервойна — это война без границ. Атаки в ней могут вестись как с территории нападающего, так и с других (вовсе не смежных) территорий.

Большинство специалистов предсказывало начало времени кибервойн только в XXI веке [2], однако, они ведутся уже сегодня, пускай пока еще не в масштабах, описанных в ряде произведений писателей-фантастов. Боевые действия, развернутые хакерами против стран НАТО, показали, что объявление войны перестает быть прерогативой государств и правительств. Ее может начать как маленькая группа людей, так и один человек.

Для обеспечения кибербезопасности странам необходимо всемерно развивать технологии интернет-разведки и разведки по открытым источникам (OSINT) для решения практических задач сбора и аналитической обработки оперативно значимой информации в интересах подразделений кибербезопасности различных ведомств. Для этого требуется согласованное решение следующих задач:

– обеспечение скрытности присутствия в Сети;

– сбор информации из глубинного («серого») Интернета, а также из социальных сетей: специализированные инструменты поиска, базирующиеся в облаке, позволяют вести долгосрочное скрытое наблюдение за заданными сетевыми ресурсами;

– анализ профилей пользователей в социальных сетях: детальный поведенческий анализ на основе принципов психометрии позволяет выявлять пользователей с заданными психическими свойствами и отклонениями (склонность к алкоголю и наркотикам, жестокость, суицидальные наклонности, экстремизм и т.д.); эта информация в последующем используется при формировании контрактных и специальных подразделений;

– анализ пользовательских групп в социальных сетях: методы облачной обработки больших данных (включая нейронные сети, нечеткую логику и др.) позволяют выявлять места скопления целевой аудитории для планирования и проведения операций в сфере информационной войны;

– мониторинг Интернета вещей в целях выявления плохо защищенных компонентов инфраструктуры других стран, как военной, так и транспортной, энергетической и др.;

– контроль собственной защищенности: анализ хакерских атак нового поколения показал, что традиционные антивирусы и сканеры не справляются с защитой критических ресурсов, нужны новые комплексные решения;

– раннее обнаружение утечек критической и конфиденциальной информации: организация облачной системы контроля распространения информации позволяет оперативно обнаруживать утечки важной информации как общегосударственного, так и военного применения.

Таким образом, решение перечисленных проблем с успехом может быть ис-

пользовано для выполнения комплекса оперативно-стратегических задач в киберпространстве в интересах обороны и безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Брусницын Н.А. Информационная война и безопасность. М.: Вита-Пресс, 2001.

2. Девяткина, А.Г. Информационные войны в современных международных отношениях. // Актуальные проблемы современных международных отношений. 2014. №3. С. 54-59.

НАУЧНАЯ ШКОЛА «ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ» (ОЛЕГУ БОРИСОВИЧУ МАКАРЕВИЧУ 13.09.2019 ГОДА – 85 ЛЕТ)

Олег Макаревич
Кафедра Безопасности Информационных Технологий
Южный Федеральный Университет, Таганрог, Россия
obmakarevich@sfedu.ru

1 ВВЕДЕНИЕ

Макаревич Олег Борисович –доктор технических наук (1983 г.), профессор (1996 г.), действительный член Международный Академии информатизации (1994 г.), работает в Университете (ТРТИ, ТРТУ, ЮФУ) с 1962 года. В период формирования научной школы (1993 г.) в научном коллективе состояло 15 сотрудников и аспирантов, все они в будущим защитили кандидатские (Аникеев М.В., Хусааинов Н.Ш., Шелудько В.М., Шелудько И.А., Цопкало Н.Н., Коробко А.Ю., Пескова О.Ю., Юрков П.Ю., Брюхомицкий Ю.А., Федоров В.М., Спиридонов О.Б., Спиридонов Б.Г.) и докторские диссертации (Бабенко Л.К., Чефранов А.Г., Витиска Н.И.). Многие из упомянутых членов научной школы в настоящее время работают в ЮФУ и возглавляют уже свои научные школы, например, профессор Бабенко Л.К., профессор Чефранов А.Г.

2 МАКАРЕВИЧ О.Б. - РУКОВОДИТЕЛЬ

Макаревич Олег Борисович –доктор технических наук (1983 г.), профессор (1996 г.), действительный член Международный Академии информатизации (1994 г.), Заслуженный изобретатель РФ (1987 г.), Заслуженный деятель науки РФ (2001 г.), награжден медалями «За укрепление государственной системы защиты информации» 2-ой и 1-ой степени работает штатным сотрудником в Университете (ТРТИ, ТРТУ, ЮФУ) с 1962 года по настоящее время на должностях:

ассистент, доцент, зав. отделом в НИИ МВС, профессор, зав. кафедрой БИТ, профессор ЮФУ.

3 ВЕДУЩАЯ НАУЧНАЯ ШКОЛА

Ведущая научная школа профессора Макаревича О.Б. с названием «Алгоритмы и технологии параллельных вычислений в системах обработки и защиты информации» уже в 2003 году (протокол № 5 заседания Ученого Совета ТРТУ от 28.01.2003 г.) выдвигалась на конкурс по государственной поддержке исследований ведущих научных школ Российской Федерации. Все последующие годы до настоящего времени школа успешно функционирует.

4 КОЛИЧЕСТВО И СПИСОК ЧЛЕНОВ НАУЧНОЙ ШКОЛЫ, РАБОТАЮЩИХ В НАСТОЯЩЕЕ ВРЕМЯ В ЮФУ

В настоящее время на штатных должностях в различных подразделениях ЮФУ работает 23 участников научной школы, из них докторов наук 2, кандидатов наук 10, аспирантов 9 и других сотрудников (магистров) 2.

Конкретно:

1) Профессор Макаревич О.Б.
2) Профессор Бабенко Л.К.
3) Доцент Абрамов Е.С.
4) Доцент Басан А.С.
5) Доцент Рублев Д. П.
6) Доцент Мордвин Д.В.
7) Доцент Половко И. Ю.
8) Доцент Тумоян Е.П.
9) Доцент Аникеев М.В.
10) Доцент Брюхомитский Ю.А.
11) Доцент Федоров В.М.
12) Доцент Пескова О.Ю.
13) К.т.н. Благодаренко А.В.
14) Аспирант Басан Е.
15) Аспирант Сергиенко А.А.
16) Аспирант Редин А.С.
17) Аспирант Кущенко А. С.
18) Аспирант Трубников Я.А.
19) Аспирант Сторчак С.А.
20) Аспирант Никульшин А.С.
21) Аспирант Чеснаков Р.Д.
22) Аспирант Чистоходова А.А.
23) Магистрант Пестов В.А.
24) Магистрант Марченко Е. А

5 СОСТАВ УЧАСТНИКОВ

За годы существования научной школы состав участников, конечно, изменялся, но в среднем это было ежегодно 20 – 27 сотрудников, среди них 2 – 3 доктора наук, 10 – 12 кандидатов наук, 5 – 8 аспирантов, 3 – 4 студента.

5.1 Старшее поколение

Д.т.н., профессор Чефранов А.Г.	Научный руководитель кандидатской и консультант по докторской диссертации, совместные монографии, научные статьи, доклады.
Д.т.н., профессор Витиска Н.И.	Научный руководитель кандидатской диссертации, совместные монографии, научные статьи, доклады.
Д.т.н., профессор Бабенко Л.К.	Совместные монографии, научные статьи, доклады, гранты РФФИ, разработки по хоздоговорам, свидетельства о регистрации программ.
К.т.н. Сивцов С.А.	Научный руководитель диссертации, совместные научные статьи, доклады, разработки по хоздоговорам.
К.т.н. Карпов Е. В.	Научный руководитель диссертации, совместные научные статьи, доклады, разработки по хоздоговорам.

5.2 Среднее поколение

К.т.н., доцент Спиридонов Б.Г.	Совместные научные статьи, доклады, гранты РФФИ, разработки по хоздоговорам, свидетельства о регистрации программ.
К.т.н., доцент Абрамов Е.С.	Научный руководитель диссертации, совместные монографии, научные статьи, доклады, гранты РФФИ, разработки по хоздоговорам.
К.т.н., доцент Пескова О.Ю.	Научный руководитель диссертации, совместные монографии, научные статьи, доклады, гранты РФФИ, разработки по хоздоговорам.
К.т.н., доцент Шелудько И.А.	Научный руководитель диссертации, научные статьи, доклады.
К.т.н., доцент Аникеев М.В.	Научный руководитель диссертации, научные статьи, доклады, разработки по хоздоговорам.
К.т.н. Терешкин А.В.	Научный руководитель диссертации, научные статьи, доклады.
К.т.н., доцент Тумоян Е.П.	Научный руководитель диссертации, совместные научные статьи, доклады, гранты РФФИ, разработки по хоздоговорам.

5.3 Младшее поколение

К.т.н., доцент Рублев Д.	Научный руководитель диссертации, научные статьи, доклады, гранты РФФИ, разработки по хоздоговорам.
К.т.н. Косолапов Ф. А.	Научный руководитель диссертации, научные статьи, доклады.
К.т.н., доцент Мордвин Д.В.	Научный руководитель диссертации, научные статьи, доклады.
К.т.н., доцент Половко И.Ю.	Научный руководитель диссертации, научные статьи, доклады.
К.т.н. Абасов Н.Д.	Научный руководитель диссертации, научные статьи, доклады.
Аспирант Басан Е. С.	Научный руководитель диссертации, научные статьи, доклады.

К.т.н. Солина Н.И.	Научный руководитель диссертации, научные статьи, доклады

6 КОЛИЧЕСТВО КАНДИДАТСКИХ И ДОКТОРСКИХ ДИССЕРТАЦИЙ, ЗАЩИЩЕННЫХ В НАУЧНО-ПЕДАГОГИЧЕСКОМ КОЛЛЕКТИВЕ ЗА ПОСЛЕДНИЙ ПЕРИОД (10 ЛЕТ)

Диссертант, степень	Название	Научный руководитель	Год	Место работы
К.т.н. Казарин М.Н.	Разработка и исследование методов скрытного клавиатурного мониторинга	Профессор Макаревич О.Б.	2006	Частная фирма
К.т.н. Косолапов Ф.А.	Метотехнология защиты информационных ресурсов от вредоносного поведения программ.	Профессор Макаревич О.Б.	2006	Частная фирма
К.т.н. Рублев Д.П.	Разработка и исследование высокочувствительных методов стегоанализа	Профессор Макаревич О.Б.	2007	ЮФУ Частная фирма
К.т.н. Терешкин А.В.	Разработка и исследование метода защиты от удаленных атак на основе диверсикации программного обеспечения	Профессор Макаревич О.Б.	2007	ЮФУ Частная фирма
К.т.н. Аникеев М.В.	Разработка алгоритмических и программных средств, повышающих эффективность обнаружения вторжений на основе использования скрытых марковских моделей.	Профессор Макаревич О.Б.	2008	ЮФУ
К.т.н. Мордвин Д.В.	Разработка и исследование методов и алгоритмов автоматического построения правил фильтрации межсетевых экранов, адекватных заданной политике разграничения доступа в сети.	Профессор Макаревич О.Б.	2010	ЮФУ
К.т.н. Благодаренко А.В.	Разработка метода, алгоритмов и программ для автоматического поиска уязвимостей программного обеспечения в условиях отсутствия исходного кода	Профессор Макаревич О.Б.	2011	ВТБ г. Новороссийск
К.т.н. Половко И.Ю.	Разработка и исследование системы оценки качества СОА	Профессор Макаревич О.Б.	2012	ЮФУ
К.т.н. Абасов Н.Д.	Исследование Эффективности использования избыточного	Профессор Макаревич О.Б.	2015	ВТБ г. Краснодар

	модулярного кода для обеспечения целостности транзакционных данных АС обработки информации банка			
К.т.н. Басан Е.С.	Разработка системы управления защитой беспроводной сенсорной сети на основе доверия.	Профессор Макаревич О.Б.	2016	ЮФУ

7 КОЛИЧЕСТВО АСПИРАНТОВ В НАУЧНОМ КОЛЛЕКТИВЕ ЗА ПОСЛЕДНИЕ 10 ЛЕТ

Если исходить из того, что за все время работы в ЮФУ (ТРТУ, ТРТИ) у меня защитилось более 20 соискателей, а у докторов – участников данной школы пусть еще 10 соискателей, то общее количество аспирантов будет равно 30. В настоящее время в рамках школы работает 8 аспирантов

.

8 ОСНОВНЫЕ ПУБЛИКАЦИИ КОЛЛЕКТИВА ЗА 10 ЛЕТ

8.1 Статьи, монографии

1. Babenko L.K., Burtyka P., Makarevich O.B., Trepacheva A.V. «The General Model of » - . SIN 15, Sochi 2015.

2. Басан Е.С., Макаревич О.Б. «An Energy-efficient System of Counteraction against Attacks in the Mobile Wireless Sensor Networks» pp 403-410. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2015), China.

3. Буртыка Ф.Б., Макаревич О.Б. Разработка обфусцирующего компиллятора на основе полностью гомоморфного шифрования. Материалы X1V Международной н-т конференции «Информационная безопасность-2015», с. 278-283 Научно-практический журнал «Информационное противодействие угрозам терроризма» №24 2015 год.

4. Басан А.С., Басан Е.С. Макаревич О.Б. Development of Hierarchal Trust management System for Mobile Cluster-based Wireless Sensor Network .SIN 16, USA, 2016.

5. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Чесноков Р.Д., Трубников Я.А. Разработка и исследование программно-аппаратного комплекса для шифрования по алгоритму PRESENT для решения задач малоресурсной криптографии. ЮФУ. Технические Известия науки. 2014. № 2 (151). –с. 174 – 180.

6. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Чесноков Р.Д., Трубников Я.А. Инструментальная система анализа защищенности информации международная конференция по защите информации и связи, 2014 г. Глазго/ Великобритания. ID 182. – с. 339 – 345.

7. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б. Современные интеллектуальные пластиковые карты (научная монография). М.: Гелиос АРВ, 2015. – 416 с.

8. Абрамов Е.С., Басан Е.С. Анализ сценариев атак на беспроводные сенсорные сети. Материалы X111Международной научно-практической конференции «ИБ -2013». Ч1. Таганрог: Изд-во ЮФУ, с 60 – 71.

9. Абрамов Е.С., Басан Е.С. Разработка архитектуры системы обнаружения вторжений для беспроводных сенсорных сетей. Материалы X111 Международной научно-практической конференции «ИБ -2013». Ч1. Таганрог: Изд-во ЮФУ, с 71-79.

10. Гришечкина Т.А., Макаревич О.Б. Выявление вредоносных узлов в сетях AD HOC при различных типах атак. Материалы X111Международной научно-практической конференции «ИБ -2013». Ч2. Таганрог: Изд-во ЮФУ, с 136-142.

11. Половко И.Ю., Пескова О.Ю. Анализ функциональных требований к системам обнаружения вторжений. Известия «Технические науки». Тематический выпуск –ИБ. 2014 г.ЮФУ. с. 86-92.

12. Абрамов Е.С., Басан Е.С. Анализ сценариев атак на беспроводные сенсорные сети / Материалы XIII Международной научно-практической конференции «ИБ-2013» / Ч.1. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С.60-72.

13. Абрамов Е.С., Басан Е.С. Разработка архитектуры системы обнаружения вторжений для беспроводных сенсорных сетей / Материалы XIII Международной научно-практической конференции «ИБ-2013» / Ч.1. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С.72-79.

14. БасанЕ.С, Макаревич О.Б. АбрамовЕ.С. Development of a secure Cluster-based wireless sensor network model /SIN'13. Proceedings of the 6th International Conference on Security of Information and Networks /- November 26-28, 2013, Aksaray, Turkey, - С. 372-375.

15. Басан Е.С., Макаревич О.Б., Абрамов Е.С. Разработка системы обнаружения атак для кластерной беспроводной сенсорной сети / Информационное противодействие угрозам терроризма / №20 2013 г. Издательство ТТИ ЮФУ в г. Таганроге - С. 134-140.

16. Абрамов Е.С., Басан Е.С. Разработка модели, защищенной кластерной беспроводной сенсорной сети. / Известия ЮФУ. Технические науки. / № 12 (149), 2013 г. Тематический выпуск Информационная безопасность. Издательство ТТИ ЮФУ в г. Таганроге. - С. 48-56.

17. Абрамов Е.С., Басан Е.С. Разработка защищенного протокола управления мобильной кластерной сенсорной сетью / Информационное противодействие угрозам терроризма / Издательство: Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге. №23 (23) – 2014 г.- С.- 46-51.

18. Абрамов Е.С., Басан Е.С. Разработка набора метрик для выбора главы кластера в мобильной сенсорной сети / Информационное противодействие угро-

зам терроризма /Издательство: Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге (Таганрог). 23 (23) - 2014 г. С. - 52-55.

19. Абрамов Е.С., Басан Е.С., Лакшми В. Разработка защищенного протокола управления мобильной кластерной сенсорной сетью / Известия ЮФУ. Технические науки / Издательство: Южный федеральный университет (Ростов-на-Дону). № 2 (151) – 2014г.С. - 101-107.

20 .Басан Е.С., Макаревич О.Б., Абрамов Е.С. Trust management system for mobile cluster-based wireless sensor network. / SIN'15. Proceedings of the 8th International Conference on Security of Information and Networks /- September 8-10, 2015, Sochi, Russia. С. 203-209.

21. БасанЕ.С., Макаревич О.Б. An Energy-efficient System of Counteraction against Attacks in the Mobile Wireless Sensor Networks. / International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery/ Xi'an, Shaanxi, China, 2015 г. С. -403-410.

22. Е.С. Абрамов, Е.С. Басан, А.С. Басан Разработка системы управления уровнем доверия в мобильной кластерной беспроводной сенсорной сети. Известия ЮФУ. Технические науки. Издательство: Южный федеральный университет (Ростов-на-Дону). No 7 (168). 2015 г.С. 42-52.

23. Басан А.С., Басан Е.С., Макаревич О.Б. Development of the Hierarchal Trust management System for Mobile Cluster-based Wireless Sensor Network. Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks, 2016, С.116-122.

24. Благодаренко А.В. Статистический и динамический анализ программного обеспечения без исходных текстов. // Проблемы информационной безопасности в системе высшей школы: труды XIV всероссийской научной конференции. –М.: МИФИ, 2007. с. 33-34.

25. Благодаренко А.В. Полномаршрутное тестирование программного обеспечения без исходных кодов. // Материалы XIV общероссийской научно-технической конференции Спб. «Методы и технические средства обеспечения безопасности информации». 2007. с. 31.

26. Благодаренко А.В. Инструментальное средство для проведения сертификационных испытаний программного обеспечения без исходных кодов. // Известия ЮФУ. Технические науки. Тематический выпуск. Таганрог 2007, с. 212-215. Таганрог: Изд-во ТТИ ЮФУ, 2008. №1. 277 с,), с 111.

27. Благодаренко А.В. Пассивный honeypot на анализе спутникового трафика. // Сборник ЮФУ. Тематический выпуск. Информационная безопасность. Перспектива-2009. 2009. с 44-49.

28. Благодаренко А.В. Широковещательное распространение обновлений безопасности для ОС Linux через спутниковый канал. // Сборник ЮФУ. Тематический выпуск. Информационная безопасность. Перспектива-2009. 2009. с 210-

214.

29. К.Д. Ольшанов, А.Л. Речков, А.В Благодаренко. Метод последовательного внедрения ошибок для тестирования обработки аварийных ситуаций ПО. // Сборник трудов конференции «Молодежь и современные информационные технологии». Томск, 3 – 5 марта 2010 г., ч.2. Томск: Изд-во СПБ Графикс – 138 – 139 с.

30. Е.П. Тумоян, Ю.В.Лисова, А.В. Благодаренко. Исследование безопасности гетерогенных корпоративных сетей на основе методологии OSSTMM. // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч.2. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – с. 61-64.

31. Babenko, O. Makarevich, F. Burtyka, A. Trepacheva. The General Model of Secure Computation System. - SIN'15 Proceedings of the 8th International Conference of Security of Information and Networks. –September 08 – 10, 2015. –ACM, USA, Sochi, 2015 (SCOPUS).

32. L.Babenko, O.Makarevich, D.Bespalov, R.Chesnokov, Y.Trubnikov. Instrumental system for analysis of information system using smart cards protection. – SIN'14 Proceedings of the 7th International Conference of Security of Information and Networks. –September 09 – 12, 2014. – ACM, Glasgow, 2014 (SCOPUS).

33. Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева. Полностью гомоморфное шифрование. - 2015. - Полностью гомоморфное шифрование. - Вопросы защиты информации, Москва, 2015. - № 3. С. 3-26. (Перечень ВАК РФ.)

34. Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева. Обобщенная модель системы криптографически защищенных вычислений. - Известия Южного федерального университета, технические науки, Известия ЮФУ. Технические науки, (ВАК РФ), Таганрог, 2015. - №5 С. 77-88.

35. Бабенко Л.К., Макаревич О.Б., Чесноков Р.Д. Разработка и исследование средств малоресурсной криптографии на примере алгоритмов PRESENT и CLEFIA. Материалы конференции «Информационные технологии в управлении» (ИТУ-2014), - СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. – С. 571 – 575.

8.2 Свидетельство об официальной регистрации программ для ЭВМ

1. Бабенко Л.К., Беспалов Д.А., Лексин Д.М., Макаревич О.Б., Назаренко А.О. Модуль настройки команд управления драйверами ЭВМ. Свидетельство об официальной регистрации программ для ЭВМ № 2012611841. – М.: Роспатент, − 17.02.2012.

2. Бабенко Л.К., Беспалов Д.А., Лексин Д.М., Макаревич О.Б. На Модуль графического редактора универсальных скриптов для управления считывателем интеллектуальных пластиковых карт (ИПК) Заренко А.О. Свидетельство об официальной регистрации программ для ЭВМ № 2012611935. – М.: Роспатент, − 20.02.2012.

3. Бабенко Л.К., Беспалов Д.А., Лексин Д.М., Макаревич О.Б Модуль разбора конфигурационных файлов настройки программы управления считывателем интеллектуальных пластиковых карт (ИПК)

4. Бабенко Л.К., Беспалов Д.А., Лексин Д.М., Макаревич О.Б. Модуль трансляции универсальных скриптов для управления считывателем интеллектуальных пластиковых карт (ИКП). - Свидетельство об официальной регистрации программ для ЭВМ № 2012611810. – М.: Роспатент, − 29.08.2012.

5. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Трубников Я.А., Чесноков Р.Д. Программное средство управления базой данных для результатов анализа внутренней структуры и протоколов обмена для имитации поведения пластиковых карт. - Свидетельство об официальной регистрации программ для ЭВМ № 2016612152. – М.: Роспатент, − 19.02.2016.

6. Бабенко Л.К., Макаревич О.Б., Аникеев М.В., Белозеров А.А., Цопкало Н.Н., Пересыпкин В.А. Модуль лингвистической коррекции для системы оптического распознавания печатного текста. Свидетельство о государственной регистрации программ для ЭВМ № 2011618987. - М.: Федер. служба по интелл. собственности, - 17.11.11г.

7. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Трубников Я.А., Чесноков Р.Д. Программное средство для анализа внутренней структуры бесконтактных пластиковых карт. - Свидетельство об официальной регистрации программ для ЭВМ № 2916611921. – М.: Роспатент, − 15.02.2016.

8. Бабенко Л.К., Беспалво Д.А., Макаревич О.Б., Трубников Я.А., Чесноков Р.Д. Программное средство для имитации поведения контактных интеллектуальных пластиковых карт. - Свидетельство об официальной регистрации программ для ЭВМ № 2016611924. – М.: Роспатент, − 15.02.2016.

9. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Трубников Я.А., Чесноков Р.Д. Программное средство для анализа внутренней структуры контактных пластиковых карт. - Свидетельство об официальной регистрации программ для ЭВМ № 2016612048. – М.: Роспатент, − 18.02.2016.

10. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Трубников Я.А., Чесноков Р.Д. Программное средство для регистрации и анализа протоколов обмена контактных интеллектуальных пластиковых карт. - Свидетельство об официальной регистрации программ для ЭВМ № 2016612024. – М.: Роспатент, − 16.02.2016.

11. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Трубников Я.А., Чесноков Р.Д. Программное средство для имитации поведения бесконтактных интеллектуальных пластиковых карт. - Свидетельство об официальной регистрации программ для ЭВМ № 2016612021. – М.: Роспатент, − 16.02.2016

12. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б., Трубников Я.А., Чесноков Р.Д. Программное средство для регистрации и анализа протоколов обмена бесконтактных интеллектуальных пластиковых карт. - Свидетельство об официальной регистрации программ для ЭВМ № 2016611340. – М.: Роспатент, − 01.02.2016

13. Бабенко Л.К., Маро Е.А. Составление систем уравнений для нелинейных

преобразований алгоритмов шифрования / Бабенко Л.К., Маро Е.А.// Свид. о гос. регистрации программы для ЭВМ. - Федеральная служба по интеллектуальной собственности, патентам и товарным знакам. Свидетельство об официальной регистрации программы для ЭВМ №2012611932 от 20 февраля 2012

14. Бабенко Л.К., Ищукова Е.А. Дифференциальный криптоанализа учебного алгоритма шифрования. - Свидетельство об официальной регистрации программ для ЭВМ № 2012611931. - М.: Роспатент, 20.02.12г

15. Бабенко Л.К., Ищукова Е.А. Линейный криптоанализа учебного алгоритма шифрования. - Свидетельство об официальной регистрации программ для ЭВМ № 2012611843. - М.: Роспатент, - 17.02.12г.

16. Бабенко Л.К., Макаревич О.Б., Аникеев М.В., Белозеров А.А., Пересыпкин В.А. Модуль формирования индексных деревьев для быстрой коррекции распознаваемого текста по словарю и статистике

17. Бабенко Л.К., Макаревич О.Б., Аникеев М.В., Белозеров А.А., Пересыпкин В.А. Модуль формирования индексных деревьев для быстрой коррекции распознаваемого текста по словарю и статистике буквосочетаний. Свидетельство о государственной регистрации программ для ЭВМ № 2011618990. - М.: Федер. служба по интелл. собственности, - 17.11.11г.

18. Бабенко Л.К., Макаревич О.Б., Цопкало Н.Н., Белозеров А.А., Пересыпкин В.А. Программа поиска изображений символов на изображении известной текстовой строки. Свидетельство о государственной регистрации программ для ЭВМ № 2011618982. - М.: Федер. служба по интелл. собственности, - 17.11.11г.

19. Бабенко Л.К., Макаревич О.Б., Цопкало Н.Н., Белозеров А.А., Пересыпкин В.А. Программа считывания эталонных изображений символов различных шрифтов и размеров со страниц специального формата. Свидетельство о государственной регистрации программ для ЭВМ № 2011618988. - М.: Федер.служба по интелл. собственности, - 17.11.11г

20. Бабенко Л.К., Макаревич О.Б., Аникеев М.В., Белозеров А.А., Цопкало Н.Н., Пересыпкин В.А. Модуль лингвистической коррекции для системы оптического распознавания печатного текста. Свидетельство о государственной регистрации программ для ЭВМ № 2011618987. - М.: Федер. служба по интелл. собственности, - 17.11.11г.

21. Басан А.С., Басан Е.С., Макаревич О.Б. Программа анализа данных и вычисления доверия в беспроводной сенсорной сети. Свидетельство о государственной регистрации программы для ЭВМ №2016615606, 26 мая 2016 г.

9 ПЕРЕЧЕНЬ ХОЗЯЙСТВЕННЫХ ДОГОВОРОВ, НАУЧНЫХ ГРАНТОВ ЗА 5 ЛЕТ

№	Источник и форма поддержки структурного подразделения вуза	Наименование работы	Период поддержки	Объем финансового обеспе-

	(хоздоговора)		структурного подразделения вуза	чения поддержки за период, руб.
1	СЧ НИР «Катион-Т», заказчик ФГУП НТЦ «Орион», г. Москва Руководитель – проф. Макаревич О.Б.	Разработка программной системы распознавания текстовых изображений низкого качества, минимально зависящей от используемого шрифта	20.05.2009 - 20.11.2011	6 780 940,00
2	СЧ НИР «Торос-Т», заказчик ФГУП НТЦ «Орион», г. Москва Руководитель – проф. Макаревич О.Б.	Разработка методов контроля действия пользователей целевых компьютерных сетей с помощью программных агентов	15.04.2011 - 31.03.2013	12 199 141,00
3	СЧ НИР «Тролль-К4», заказчик ФГУП НТЦ «Орион», г. Москва Руководитель – проф. Макаревич О.Б.	Исследование проблем автоматизации анализа защищенности и разработка средств защиты интеллектуальных пластиковых карт	01.04.2014 - 31.10.2015	8 347 816,82
4	СЧ НИР «Траверс-К3», заказчик ФГУП НТЦ «Орион», г. Москва Руководитель – проф. Макаревич О.Б.	Исследование защищённости специализированных микроконтроллеров, применяемых в современных маршрутизаторах, от внешних воздействий	5.04.2016-30.06.2018	9 000 000,00
	ИТОГО:			**36327897 руб.**

10 ГРАНТЫ РФФИ

№	Источник и форма поддержки структурного подразделения вуза	Номер гранта	Наименование работы	Год	Объем финансового обеспечения поддержки за период, руб.
2	РФФИ, г. Москва Рук. О.Б. Макаревич	№16184	Разработка стеганографического метода скрытия информации в потоковой передаче аудиоданных, устойчивого к сжатию с потерями	2011	500 000,00
3	РФФИ, г. Москва Рук. О.Ю. Пескова	№16188	Разработка и исследование методов, методологии и средств автоматизированного создания виртуальных музеев и подготовка виртуального 3D-музея, посвященного 150-летию со дня рождения А.П. Чехова	2011	350 000,00
4	РФФИ, г. Москва Рук. Е.П. Тумоян	№ 16 189	Исследование разработка моде-	2011	350 000,00

			лей, методов и средств представления и хранения знаний в области информационной безопасности		
6	РФФИ, г. Москва Рук. О.Б. Макаревич		Разработка стеганографического метода скрытия информации в потоковой передаче аудиоданных, устойчивого к сжатию с потерями	2012	455 000,00
7	РФФИ, г. Москва Рук. О.Ю. Пескова	№16188	Разработка и исследование методов, методологии и средств автоматизированного создания виртуальных музеев и подготовка виртуального 3D-музея, посвященного 150-летию со дня рождения А.П. Чехова	2012	405 000,00
8	РФФИ, г. Москва Рук. Е.П. Тумоян	№ 10-07-00529-а	Исследование разработка моделей, методов и средств представления и хранения знаний в области информационной безопасности	2012	305 000,00
9	РФФИ, г. Москва Рук. О.Б. Макаревич	№12-07-92693-ИНД_а	Противодействие атакам на сетевые протоколы в мобильных сенсорных сетях Adhoc	2012	600 000,00
10	РФФИ, г. Москва Рук. О.Б. Макаревич	№ 12-07-00013-а	Разработка и исследование методов и средств оперативного анализа трафика ЛВС и автоматизированного построения моделей сетевых атак	2012	455 000,00
11	РФФИ, г. Москва Рук. Е.С. Абрамов	№ 12-07-00014-а	Разработка и исследование методики и средств построения и верификации адаптивных систем информационной безопасности критических систем информационной инфраструктуры	2012	410 000,00
12	РФФИ, г. Москва Рук. Д.П. Рублев	№ 12-07-00674	Разработка методов верификации пользователя по виброакустическим шумам, возникающим при работе с клавиатурой и манипулятором «мышь»	2012	400 000,00
13	РФФИ, г. Москва Рук. О.Б. Макаревич	№12-07-92693-ИНД_а	Противодействие атакам на сетевые протоколы в мобильных сенсорных сетях Adhoc	2013	600 000,00
14	РФФИ, г. Москва Рук. О.Б. Макаревич	№ 12-07-00013-а	Разработка и исследование методов и средств оперативного анализа трафика ЛВС и автоматизированного построения моделей	2013	570 000,00

			сетевых атак		
15	РФФИ, г. Москва Рук. Е.С. Абрамов	№ 12-07-00014-а	Разработка и исследование методики и средств построения и верификации адаптивных систем информационной безопасности критических систем информационной инфраструктуры	2013	470 000,00
16	РФФИ, г. Москва Рук. Д.П. Рублев	№ 12-07-00674	Разработка методов верификации пользователя по виброакустическим шумам, возникающим при работе с клавиатурой и манипулятором "мышь"	2013	400 000,00
17	РФФИ, г. Москва Рук. О.Ю. Пескова	№ 13-07-00244-а	Исследование и разработка методов, алгоритмов и методик создания, функционирования и обеспечения безопасности виртуальных экспозиций и электронных каталогов, построенных на основе облачных технологий	2013	400 000,00
18	РФФИ, г. Москва Рук. О.Б. Макаревич	№ НК-12-07-00013/14	Разработка и исследование методов и средств оперативного анализа трафика ЛВС и автоматизированного построения моделей сетевых атак	2014	600 000,00
19	РФФИ, г. Москва Рук. О.Ю. Пескова	№ НК 13-07-00244/14	Исследование и разработка методов, алгоритмов и методик создания, функционирования и обеспечения безопасности виртуальных экспозиций и электронных каталогов, построенных на основе облачных технологий	2014	400 000,00
20	РФФИ, г. Москва Рук. О.Б. Макаревич	№ НК 15-07-00595/15	Разработка и исследование комплексной модели для автоматизированного анализа защищенности интеллектуальных пластиковых карт	2015	800 000,00
21	РФФИ, г. Москва Рук. О.Ю. Пескова	№ НК 13-07-00244/15	Исследование и разработка методов, алгоритмов и методик создания, функционирования и обеспечения безопасности виртуальных экспозиций и электронных каталогов, построенных на основе облачных технологий	2015	500 000,00
22	РФФИ, г. Москва Рук. О.Б. Макаревич	№ НК 15-07-20393\15	Проект организации проведения восьмой международной конференции по информационной безопасности SIN-2015	2015	380 000,00

23	РФФИ, г. Москва Рук. О.Б. Макаревич	№ 15-07-00595\16	Разработка и исследование комплексной модели для автоматизированного анализа защищенности интеллектуальных пластиковых карт	2016	720 000,00
	ИТОГО:				**10520000 руб.**

11 ИСТОРИЯ СТАНОВЛЕНИЯ И РАЗВИТИЯ НАУЧНОЙ ШКОЛЫ

История становления и развития научной школы напрямую связано с работой Макаревич О.Б. в ТРТИ, ТРТУ и ЮФУ. Макаревич Олег Борисович закончил Таганрогский государственный радиотехнический институт в 1961 г. с дипломом инженера-электрика. С 1962г. по настоящее время О. Б. Макаревич работает в ЮФУ, начиная от должности инженера, младшего научного сотрудника, затем заведующего отделом НИИ МВС, доцентом, профессором, ведущим специалистом в области информационных технологий. С 1997 года по 2014 год он являлся заведующим кафедрой безопасности информационных технологий (БИТ), директором Южно-Российского регионального учебно-научного центра (ЮР РУНЦ) по проблемам информационной безопасности в системе высшей школы, в настоящее время работает профессором кафедры БИТ ЮФУ и научным руководителем ЮР РУНЦ ЮФУ. Кафедра БИТ, начиная с 2000 года, подготовила болеем 900 специалистов, которые успешно трудятся в ВУЗах Юга России, на предприятиях и в организациях РФ. Ежегодно, по мере возможностей, обновляется лабораторное оборудование, методическое и программное обеспечение. Результаты НИОКР используются преподавателями – участниками школы в лекциях и при выполнении лабораторных и практических работ.

За эти годы Макаревич О.Б. участвовал в выполнении более 40 НИОКР, разработал и внедрил ряд изделий цифровой техники, в частности:

- 1967-1969 г.г. - руководил разработкой и внедрением в серийное производство на Новосибирском полупроводниковом заводе серии интегральных микросхем цифровых интеграторов К-502, которая выпускалась десять лет;

- 1969-1975 г.г. - руководил разработкой микросхем однокристального цифрового интегратора, волнового коммутатора, настольной цифровой интегрирующей машины (на микросхемах серии К-502), содержащей 90 цифровых интеграторов, электронную коммутацию и возможность произвольного разделения решающего поля между тремя пользователями (см. Приложение 1);

- 1981-1995 г.г. - в качестве Главного конструктора разработал технические проекты и создал экспериментальные образцы многопроцессорной вычислительной системы ЕС-2703, векторного ускорителя к РС и персональной многопроцессорной суперЭВМ «ПАРУС_М» (см. Приложения 2,3,4 соответственно);

- 1995 г. - активно участвовал в открытии в ТРТУ нового направления информационных технологий - защиты информации, в частности специальности

220600 «Организация и технология защиты информации».

С 1997 года по настоящее время коллектив научно- педагогической школы успешно ведет научно-исследовательские и опытно-конструкторские работы по созданию и внедрению современных средств защиты информации, выполняемые по заказам Федеральной службы по техническому и экспертному контролю России, предприятий министерства обороны по программам министерства образования, грантам РФФИ. Заказчиками данных работ являются: НТЦ «Орион», ЗАО «РНТ», ЗАО «Концерн ВНИИМС» (г. Москва), ГНИИИ ПТЗИ ФСТЭК России (г. Воронеж). Кафедра плодотворно сотрудничает с ведущими Вузами: МИФИ, РГГУ, ИКСИ Академии ФСБ, Уфимским авиационным университетом, вузами Южного региона. Основные направления научных исследований коллектива это - разработка новых методов и средств, обеспечивающих выявление и идентификацию угроз нарушения информационной безопасности в компьютерных сетях, а также противодействие этим угрозам. Результаты НИОКР внедряются в учебный процесс в лекции преподавателей и диссертации аспирантов. На данное число у Макаревича О.Б. более двадцати его учеников защитили кандидатские диссертации, один – докторскую диссертацию. У профессора Бабенко Л.К. защитили кандидатские диссертации 12 аспирантов.

В коллектив научной школы Макаревича О.Б. в первую очередь входят его аспиранты, теперь уже кандидаты и доктора наук, а также те, кто еще не защитил свои диссертации. Профессор Чефранов А.Г. имеет научную школу, работает уже много лет в университете на Кипре. Д.т.н., профессор Бабенко Л.К. в настоящее время сама имеет научно - педагогическую школу по направлению – криптография. Члены научной школы являются экспертами в фонде РФФИ (Макаревич О.Б., Бабенко Л.К.), в журнале «Информация и безопасность» (Макаревич О.Б.), в журнале «Кибербезопасность» (Бабенко Л.К.).

С 1999 года Макаревич О.Б. организовал и провел более 15 региональных семинаров и международных конференции «Информационная безопасность». С 2009 г. он является сопредседателем от России Международной конференции «International Conference on Security of Information and Networks» (SIN). Англоязычная конференция SIN 2010 и SIN 2015 проводились в России (г. Таганрог и г. Сочи соответственно). В другие годы конференция проводилась: в Турции (2009 г.), Индии (2011 г.), Австралии (2012 г.), Турции (2013 г.), (Шотландии 2014 г.), (США 2016 г.). Сотрудники, аспиранты и студенты ЮФУ выступали с докладами. (см. Приложение 5).

Макаревич О.Б. состоял членом ряда советов по защитам докторских диссертаций, в настоящее время он является Председателем диссертационного совета по защите диссертаций на соискание ученой степени доктора технических наук в Южном федеральном университете по специальностям 05.13.19 - «Методы и средства защиты информации, и информационная безопасность» и 05.25.05 -

«Информационные системы и процессы». С 2007 г. в Совете защитили диссертации 43 соискателя. Все диссертации утвердил ВАК России.

12 АННОТИРОВАННОЕ ОПИСАНИЕ НАУЧНОЙ ШКОЛЫ

Научная школа «Интеллектуальные системы защиты информации» была создана за период с 1994 по 2004 год профессором Макаревичем Олегом Борисовичем. Школа возникла на базе отдела многопроцессорных систем НИИ МВС. Группа исследователей (сотрудники отдела, преподаватели, аспиранты, студенты ТРТИ) на протяжении многих лет реализует научно-исследовательскую программу по разработке методов, алгоритмов и методик анализа, существующих МВС и их защиты. С 2004 года тематика школы была скорректирована и полностью посвящена защите информации. По данной тематике выполнено более 15 проектов, проектов, поддержанных грантами Российского фонда фундаментальных исследований, госбюджетными и хоздоговорными НИР. За последние 5 лет в коллективе выполнен объем научно-исследовательских работ по проектам грантов на сумму более 10 млн. руб., по проектам хоздоговоров на сумму боле 36 млн. руб. Результаты НИОКР используются преподавателями – участниками школы в лекциях и при выполнении лабораторных и практических работ. Выполнен совместный международный проект с участием исследователей Джайпурского университета (Индия). Большую часть сотрудников научной школы составляет молодежь. Всего за время существования школы защищено 21 кандидатская диссертация и одна докторская Коллективом научной школы по исследуемой тематике опубликовано более 200 работ и учебных пособий, получено 43 свидетельства о государственной регистрации программ для ЭВМ. Сотрудники научной школы являются организаторами и сами регулярно участвуют в работе международных конференций, выступают с научными докладами по исследуемой тематике (см. Приложение 5).

Макаревич О.Б. является академиком МАИ, членом-корреспондентом РАЕН, имеет почетное звание Российской академии естествознания (РАЕ) "Основатель научной школы", «Заслуженный деятель наук РФ», «Заслуженный изобретатель РФ», профессор, имеет медали ФСТЭК России «За укрепление государственной системы защиты информации» 2-ой и 1-ой степени, эксперт РФФИ, член редколлегии журналов, входящих в перечень ВАК «Известия ЮФУ. Технические науки,» и «Информация и безопасность» (г.Воронеж). В настоящее время Макаревич О.Б. руководит 7 аспирантами. Им подготовлены и читаются курсы для аспирантов по следующим дисциплинам «Методы и средства защиты, информационная безопасность» и «Гуманитарные аспекты информационной безопасности». Основные направления научных исследований коллектива это - разработка новых методов и средств, обеспечивающих выявление и идентификацию угроз нарушения информационной безопасности в компьютерных сетях, а также

противодействие этим угрозам. Результаты НИОКР внедряются в учебный процесс в лекции преподавателей и диссертации аспирантов. На данное число у Макаревича О.Б. более двадцати его учеников защитили кандидатские диссертации, один – докторскую диссертацию.

13 НАСТОЛЬНАЯ ЦИФРОВАЯ ИНТЕГРИРУЮЩАЯ МАШИНА. РАЗРАБОТКА 1978 ГОДА

Предназначена для цифрового моделирования всех негипертрансцендентных функциональных зависимостей, а также процессов и явлений, описываемых дифференциальными и алгебраическими уравнениями и системами. Предусмотрено воспроизведение типичных нелинейностей.

Может заменить аналоговые машины в абсолютном большинстве традиционных для них областей применения.

Конструктивно представляет прибор в настольном исполнении, состоящий из центрального устройства, соединенного с блоком питания, и подключаемых к нему двух пультов операторов, цифропечати и графопостроителя. Элементная база решающих блоков – микросхемы серии К502.

13.1 Основные технические данные

•Количество решающих блоков – 90.

•Количество одновременно работающих операторов – до 3-х.

•Максимальная разрядность 22 двоичных разряда.

•Коммутация решающих блоков – электронная.

•Эквивалентное быстродействие 500.000 операций сложения в секунду.

•Вывод информации на индикацию, цифропечать, графопостроитель.

•Количество аналоговых выходов – 2.

•Элементы новизны – впервые создана цифровая интегрирующая машина с произвольным разделением поля решающих блоков между тремя пользователями, электронной полнодоступной коммутацией и большими вычислительными возможностями при малых габаритах. Использованы изобретения, защищенными авторскими свидетельствами № 328482, № 355631, № 572787.

Рисунок 1: Настольная цифровая интегрирующая машина (авторы: Кутовой А.С., Макаревич О.Б. (рук. проекта), Лапшин М.А. Спиридонов Б.Г.)

14 СОСТАВ РАЗРАБОТЧИКОВ ВК: НА БАЗЕ ЕС 2703

-научный руководитель работы – Каляев А.В.

-главный конструктор - Макаревич О. Б.

-зам. главного конструктора по разработке ПО – Николаев И.А.

-зам. главного конструктора по разработке ВК – Бабенко Л.К.

-ответственный исполнитель работы – Черняк М.М.

-основные разработчики блоков ВК: Катаев О.В., Карпов Е.В., Бартини В.Р., Спектор В.Р., Сметанко В. Е., Жила В.В., Сивцов С.А., Чирский А. С., Кутовой А.С., Старостин В.В. и др.

-основные разработчики программного обеспечения: Фомина Н.И., Ослопов М. Д., Черкасов А. М., Овчаренко О.И., Харина О.Д. и др.

Работа принята Межведомственной комиссией 25 октября 1986 года

Выводы комиссии

1. Технический проект ВК на базе процессора ЕС2703 по своему объему и качеству соответствует техническому заданию на разработку технического проекта и оформлен в соответствии с ЕСКД и ЕСПД. Считать комплект КД на ВК ЕС1061-ЕС2703 по исполнению соответствующим литере Т.

2. Разработка процессора ЕС2703 по ряду технических решений обладает оригинальностью и патентной чистотой.

3. Материалы технического проекта, научно-технического отчета с результатами исследований по оценке эффективности вычислительного комплекса ЭВМ ЕС1061-ЕС2703 при решении задач математической физики и результаты испытаний экспериментального образца комплекса в объеме утвержденной программы подтвердили высокий научно-технический уровень и перспективность выбранных архитектурных решений, структуры аппаратной части и программного обеспечения.

4. Использованная в экспериментальном образце конструктивно-технологическая и элементная база отражает современное состояние отечественной вычислительной техники.

5. Комиссия считает, что, используя имеющийся задел по разработке архитектурных и структурных решений в аппаратуре и программном обеспечении, следует приступить к проведению опытно-конструкторской работы по созданию многопроцессорного вычислительного комплекса с производительностью до одного млрд. оп/с, на базе ЭВМ ЕС «Ряд-4».

Рисунок 2: Состав разработчиков ВК: на базе ЕС 2703

15 ВЕКТОРНЫЙ УСКОРИТЕЛЬ К ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРАМ ТИПА IBM PC AT

Векторный ускоритель (ВУ) предназначен для увеличения производительности персональных ЭВМ. Повышение производительности достигается путем аппаратно-микропрограммного исполнения библиотечных операций, написанных на ассемблере ВУ. Подключение ВУ к персональному компьютеру позволяет увеличить производительность в 10-30 раз по сравнению с арифметическим сопроцессором 80287 (10 МГц).

Области применения ВУ: обработка многомерных массивов информации в задачах анализа изображений, радиолокации, гидроакустики, поиска рыбных скоплений и т.д.

Конструктивно ВУ выполнен в виде блока в настольном варианте, подключаемого к IBM PC через переходную плату, или в виде модуля из 2-х плат, вставляемых в свободный «слот» ПЭВМ ЕС 1855.Системное матобеспечение включает язык ассемблера, загрузчик, отладчик, тестовые программные средства. По отдельному заказу поставляется программная модель, позволяющая производить разработку и отладку библиотечных операций без векторного ускорителя. Прикладное матобеспечение включает библиотеку программ матричной алгебры, библиотеку сложных научно-технических расчетов различных объектов (турбин, лопаток, трубопроводов и т.д.) методом конечных элементов и библиотеку для расчета гидроакустических и рыбопромысловых задач [1]. Опытные образцы (2 шт.) изготовлены в НИИ ЭВМ г. Минск, техническая документация передана на Московский завод САМ в 1993 г. Разработка выполнена по заказу НИИ ЭВМ г. Минск для организации ЦНИИ АГ г. Москва. Разработчики: Макаревич О.Б. (главный конструктор), Бабенко Л.К. (зам. главного конструктора), Карпов Е.М., Чирский А.С.,Шилов А.К., Ослопов М.Д., Сивцов С.А., Войнов В, П. (НИИ МВС при ТРТУ г. Таганрог), Асцатуров Р. М., Савенков В.П. (НИИ ЭВМ г. Минск).

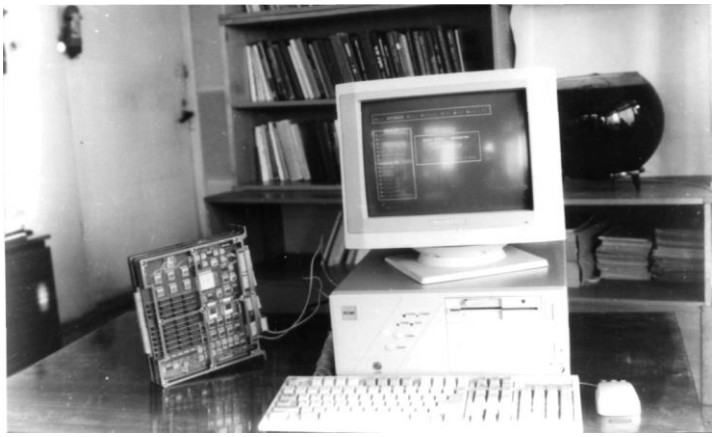

Рисунок 3: Векторный ускоритель к персональным компьютерам типа IBM PC AT

16 РАЗРАБОТЧИКИ ПЕРСОНАЛЬНОЙ МНОГОПРОЦЕССОРНОЙ СУПЕРЭВМ «ПАРУС-М»

СуперЭВМ «ПАРУС-М» является персональной параллельной многопроцессорной универсальной вычислительной системой и может использоваться для построения профессионально-ориентированных рабочих станций. Разработка выполнена по договору с НИИ приборостроения (г. Москва). Система реализована в единичном экземпляре. Оценка производительности на одном из важнейших классову народнохозяйственных задач (анализ и планирование разработки нефтяных месторождений) показала явную эффективность предложенной разработки по сравнению с другими отечественными и зарубежными средствами ВТ. Предложения по языку и системе программирования EVAL (Easy Vector Algorithmic Language) для разрабатываемой суперЭВМ имеют мировую новизну. Для обеспечения конкурентоспособности вычислитель многопроцессорной персональной суперЭВМ был выполнен на высоконадежном 32-х разрядном комплекте СБИС АМ 29с300 (в СССР он известен как серия 1843 – изготовитель ПО «Интеграл» г. Минск).

Основные технические характеристики суперЭВМ «ПАРУС-М»

1. Производительность: пиковая - 64 Мфлопс, на пакете LINPAK – 36 Мфлопс;

2. Число параллельно работающих макропроцессоров (МАП) – 4;

3. Обьем оперативной памяти одного МАП:

-память команд – 128 Кбайт, память данных – 2 Мбайта.

4. Форматы данных МАП (стандарт ИИИЭР754): 32 и 64 разряда с плавающей запятой, 32 разряда с фиксированной запятой.

- Программное обеспечение: параллельные языки высокого уровня на базе ФОРТРАН-77, СИ, Модула-2, профессиональный язык EVAL, АССЕМБЛЕР.

5. Набор стандартных макрокоманд – 200, несколько видов коммутации МАП.

6. Основная элементная база – мкомплект АМ 29с300: Число СБИС – 32 шт.

7. Конструктивное оформление: - число ТЭЗов – 14,- габариты ТЭЗов - 410х410 мм2.

Рисунок 4: Разработчики персональной многопроцессорной суперЭВМ «ПАРУС-М» (кафедра безопасности информационных технологий, 1989-1990 годы)

17 РАЗРАБОТКИ ПОСЛЕДНИХ ЛЕТ

На сегодняшний день под руководством О.Б. Макаревича на базе кафедры безопасности информационных технологий активно развивается направление, связанной с обеспечением информационной безопасности робототехнических комплексов. Основное назначение робототехнических систем заключается в мониторинге и управлении объектом, а также выполнении, поставленных перед ними задач. Использование систем группового управления для контроля работы мобильных подвижных объектов является эффективным решением, позволяющим достичь заданной цели за более короткое время, с наименьшей потерей ресурсов, что является критически важным в случае с автономными роботами, имеющими ограниченный запас энергии. С решением проблем группового управления связан рост интереса, как в научной, так и в промышленной и военной сфере.

Анализ систем группового управления с точки зрения безопасности выявил,

что подобного рода системах не заложены принципы обеспечения безопасности. Основными уязвимостями систем управления мобильными роботами являются: наличие беспроводной среды передачи данных; физическая незащищенность автономных мобильных робототехнических средств расположение мобильных устройств за пределами контролируемой зоны.

Основной проблемой связанной с разработкой системы обеспечения защиты для сети мобильных роботов, является отличие данного типа сети от привычных компьютерных сетей. Что требует разработки особых методов и подходов, которые должны учитывать следующие факторы: ограниченность вычислительных и энергетических ресурсов роботов, что делает применение таких математических решений, как искусственный интеллект, для обнаружения злоумышленника, сложным и ресурсоемким.

Для решения описанных выше проблем, связанных с повышением уровня безопасности наземных мобильных роботов выполнены следующие задачи.

В частности, проведена:

1. Разработка модели угроз и нарушителя для систем группового управления мобильными роботами. Данная модель угроз должна включать в себя все возможные угрозы, реализуемые злоумышленником на сетевом, физическом уровнях и на уровне управления сетью. Модель нарушителя для системы группового управления мобильными роботами. Модель нарушителя должна быть построена таким образом, чтобы дальнейшие решения в области безопасности носили комплексный характер и позволили бы обнаружить действия реального злоумышленника. Набор параметров для определения злоумышленника. Правильный выбор параметров для определения аномального поведения в сети позволит повысить уровень защищенности сети.

2. Разработка и реализация сценариев атак на систему группового управления мобильными роботами, тестирование сети мобильных роботов на уязвимости, а также план проведения атаки злоумышленником. Разработка сценариев атак позволит создать базу атак для сети мобильных роботов.

3. Разработка методов противодействия активным атакам со стороны внутреннего злоумышленника. Разработка имитационной модели со встроенными механизмами определения состояния узлов сети на основе вычисления доверия. Модифицированный метод вычисления уровня доверия в сети на основе порогового анализа параметров, фиксируемых мобильными роботами и передаваемых по каналам связи. Особенностью данного метода является то, что благодаря анализу изменения параметров окружающей среды или параметров самого робота можно определить оказывается ли на него деструктивное воздействие Разрабатываемый подход за счет анализа показателя доверия позволит расширить спектр атак, кроме того, за счет того, что при анализе поведения узла, головной узел сравнивает текущее состояние узла не с эталонным, а с результирующим состоянием узлов группы, повышается возможность выявления распределенных атак

злоумышленника, а также новых типов атак.

4. Разработка методов активного противодействия атакам со стороны злоумышленника, в случае использования им групп мобильных роботов, а также реализация разработанных методов. Пример защищенной сети мобильных роботов приведен на рисунке 5.

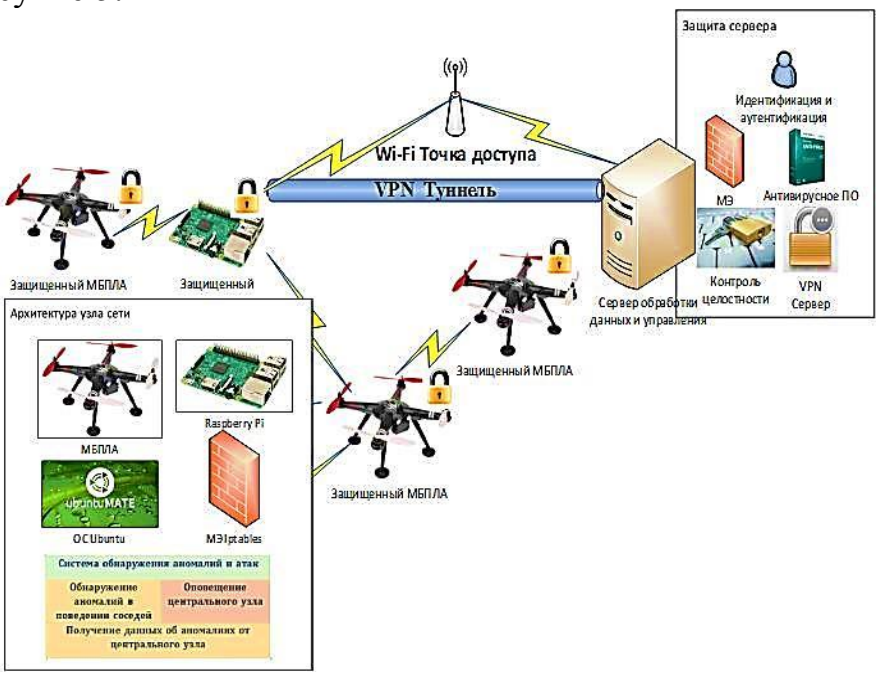

Рисунок 5: Архитектура защищенной группы малогабаритных летательных аппаратов

18 ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС (ПАК) «ТРАВЕРС»

Программно-аппаратный комплекс (ПАК) «Траверс» разработан для управления процессом формирования и применения сбоев в работе микроконтроллеров по питанию и частоте для решения задач обнаружения и эксплуатации уязвимостей микропроцессорных систем. Основной принцип организации сбоев с помощью ПАК реализуется путем создания скриптов, которые в последствии передаются на обработку в микроконтроллер. Данный подход обладает модульностью и обеспечивает гибкий подход к написанию программы сбоя. Ключевым моментом успеха сбоя является правильно выбранная форма сигнала сбоя. Так как сигнал может быть достаточно сложным для описания в скрипте, то для решения этой задачи разработан модуль, который позволяет генерировать сигнал визуально, а после завершения построения преобразует сигнал в скрипт, который отправляется на генератор, после чего генератор интерпретирует входные данные в форму сигнала сбоя.

18.1 Аппаратное обеспечение

ЭО ПАК представлено в виде отдельного модуля в корпусном исполнении. Предусмотрено подключение к ПЭВМ по стандарту USB. Модуль позволяет про-

водить загрузку программ в исследуемый микроконтроллер, предусмотрена отдельная подача сигналов на выводы микроконтроллера.

18.2 Программное обеспечение

ПАК состоит из общего ПО и функционального ПО (ФПО). Общее ПО, поставляемое с техническими средствами, входящими в состав ПАК, обеспечивают работу ЭО ПАК под управлением ОС Windows 7/8/8.1 X64. Функциональное ПО работает на языке высокого уровня C# в среде ОС Windows 7/8/8.1 X64 и обеспечивает:

- формирование вида и параметров воздействий, а также сценариев их применения в виде отдельных скриптов;
- статистическую обработку получаемых данных;
- визуализацию, полученных данных; ведение журналов;
- сохранение результатов экспериментов.

18.3 Обобщенная структура ЭО ПАК

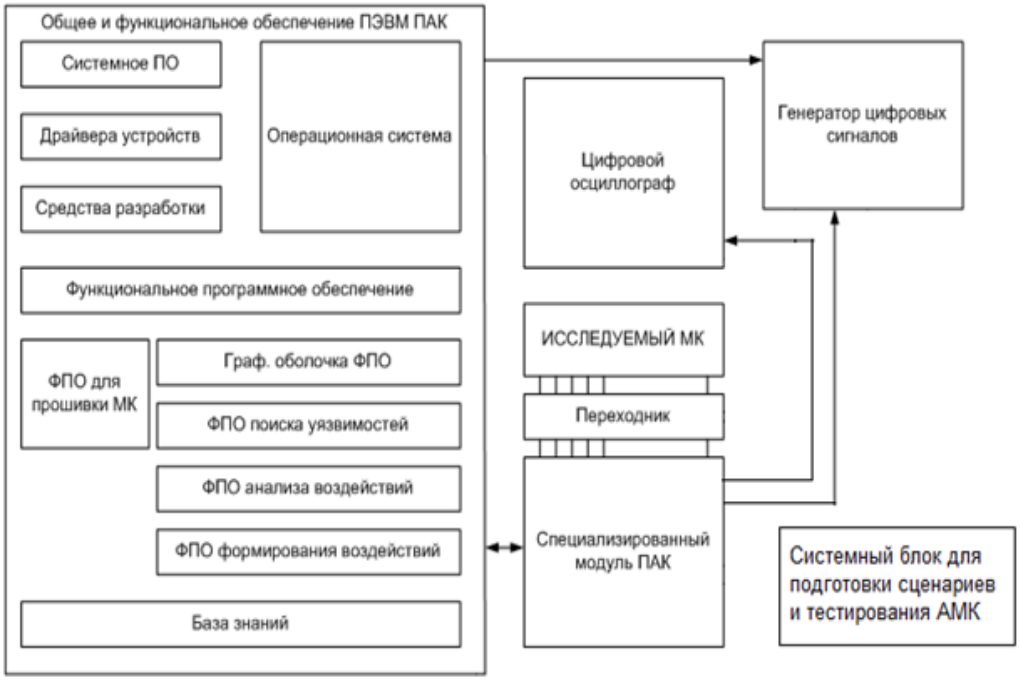

Рисунок 6: Обобщенная структура ЭО ПАК

На приведенной схеме можно выделить основные части ПАК:

1) Персональная ЭВМ, содержащая в себе общее и функциональное программное обеспечение, то есть стандартные инструменты ОС и сопровождающего ПО, а также разрабатываемый комплекс программных компонент (ФПО).

2) Системный блок для подготовки сценариев и тестирования анализируемых микроконтроллеров (АМК).

3) Отдельное устройство (анализирующий модуль - АМ), сопряженное посредством стандартизированных интерфейсов с ПЭВМ, цифровым осциллографом и генератором цифровых сигналов.

4) Цифровой осциллограф, выполняющий функции анализа цифровых и

аналоговых сигналов, проходящих по линиям связи между анализируемым микроконтроллером АМК и АМ.

5) Генератор цифровых сигналов, позволяющий воспроизводить воздействия свободной формы на отдельные выводы АМК.

18.4 Обобщенная структура программного обеспечения ЭО ПАК

Для взаимодействия с аппаратной частью комплекса, используется подсистема формирования бинарного протокола обмена данными. Конфигурация выводов микроконтроллера задается подсистемой распределения воздействий по выводам микросхемы.

Хранение данных о проведенных атаках и всей необходимой информации производится в базе данных посредством СУБД SQLite, что позволит обеспечить быстрый поиск, фильтрацию, а также даст возможность модифицирования и использования ранее проведенных атак.

Рисунок 7: Структурная схема функционального программного обеспечения

Целями программного комплекса является построение сценариев атаки посредством скриптового языка LUA с внедрением собственной библиотеки функций, запись, просмотр, фильтрация, редактирование и анализ проведенных атак.

Подсистема хранения информации позволяет работать с информацией, хранящейся в базе данных, а именно с данными произведенных атак. Благодаря этому модулю становится возможным производить хранение, поиск и фильтрацию атак, тем самым получая анализ о проделанных воздействиях и полученных результатов.

18.5 Подсистема исполнения сценариев воздействия (ПИС)

Работа с аппаратным модулем представляет собой сложный процесс отправки пакетов данных, прием и анализ ответов. Этот процесс является достаточно трудоемким для задания значений для каждого отдельного параметра, и интерпретация ответа в понятный человеку вид.

Вследствие чего был применен скриптовый язык LUA, который позволяет ускорить создание атак, направленных на микропроцессорные системы, и производить их анализ посредством вызова внутренних API-функций программного комплекса. Так как программный комплекс, согласно синтаксису написания скриптов, в автоматическом режиме строит пакеты данных, согласно каждой языковой конструкции, понятных аппаратной части ПАК, после чего принимает ответ с результатом работы скрипта, и приведет в понятный человеку вид, вследствие чего можно будет судить об успешности проведенной атаки.

Также в функционале блока содержатся не только данные о языковых конструкциях, содержащихся в скриптовом языке LUA, но и о дополнительных методах, которые необходимы для построения бинарного пакета атаки.

18.6 Подсистема генерации глитча (ПГГ)

Подсистема генератора глитча (ПГГ) предназначена для создания сигнала воздействия на ИО (используемый глитч воспроизводится аппаратной частью ПАК). Данный сигнал может быть произвольной формы или импульсной. После генерации глитча его можно сохранить как файл или импортировать в строку подсистемы скрипта. ПГГ представлено в виде окна вызываемое из основного.

Программный комплекс позволяет строить сигналы свободной формы двух типов:

1. С использованием интерполяции.
2. Без использования интерполяции.

В первом случае каждая точка задается на основе вычисления инкремента между начальной и конечной точкой как показано на рисунке 8.

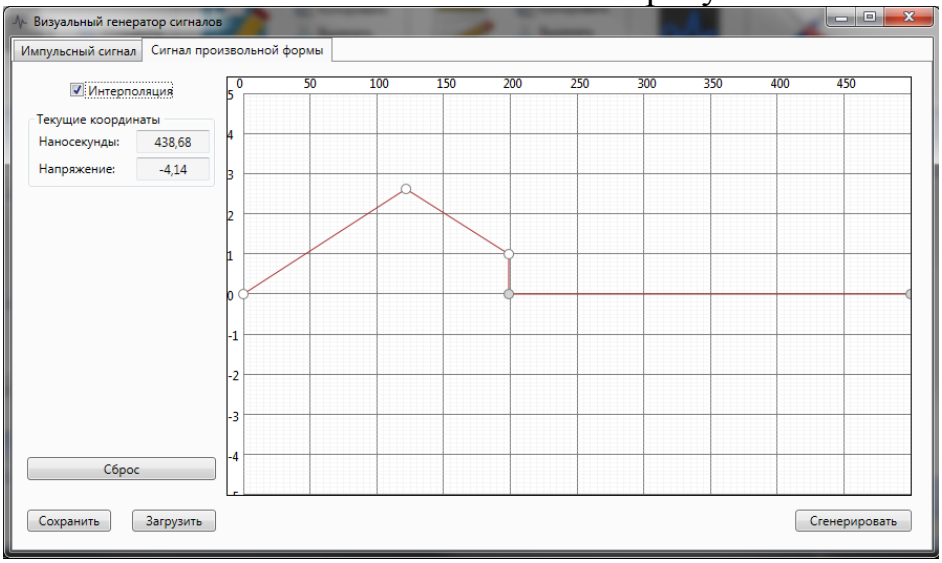

Рисунок 8: Случай, когда каждая точка задается на основе вычисления инкремента между начальной и конечной точкой

Что же касается сигналов свободной формы без интерполяции, то для расчета каждой точки между начальной и конечной, используется алгоритм DDA линии.

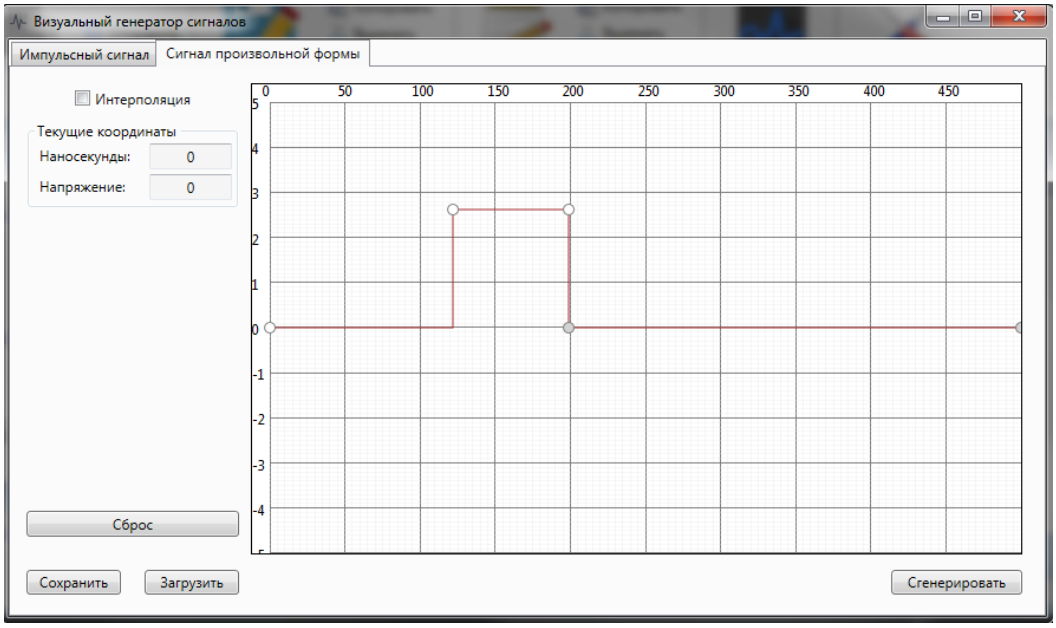

Рисунок 9: Сигналы свободной формы без интерполяции

18.7 Аппаратная часть ПАК, общее описание

Разработка вычислительного ядра аппаратной части комплекса проведена с использованием языка описания аппаратуры на базе программируемой пользователем вентильной матрицы архитектуры ПЛИС Altera MAX 10.

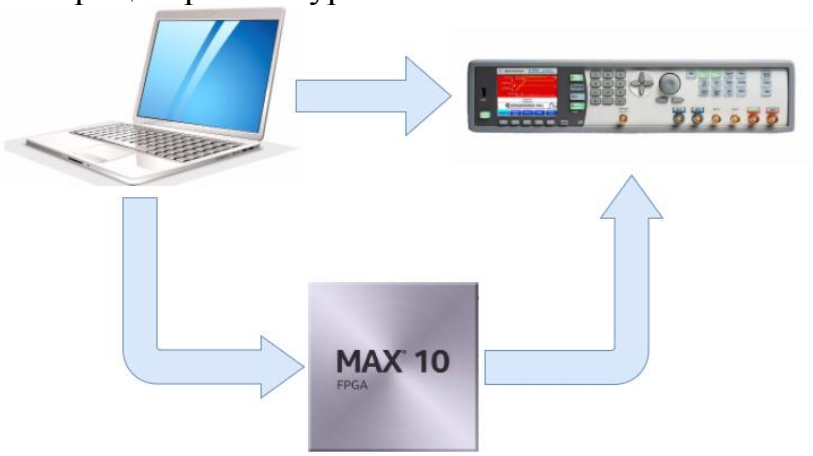

Рисунок 10: Базовая структура комплекса

В данном варианте устройство функционирует как приставка к фабричному генератору сигналов произвольной формы Keysight (Agilent) 81160A-001.

Основную задачу по формированию сигнала аппаратного сбоя выполняет генератор Keysight 81160A-001, предусматривающий два режима работы:

•Генерация импульсных сигналов сбоя (гличей) минимальновозможной длительности в 2 нс.

•Генерация сигналов произвольной формы в полосе частот до 330 МГц.

19. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ 10 МЕЖДУНАРОДНЫХ АНГЛОЯЗЫЧНЫХ КОНФЕРЕНЦИЙ SIN (С 2010 Г. ПО 2019 Г.) МАКАРЕВИЧ О.Б. – СОПРЕДСЕДАТЕЛЬ

19.1 Международная англоязычная конференция SIN 2010

Рисунок 11: Международная англоязычная конференция SIN 2010 в ЮФУ г. Таганрог

19.2 Международная конференция SIN 2012

Рисунок 12: Международная конференция SIN 2012 г. Джайпур (Индия)

19.3 Международная конференция SIN 2014

Рисунок 13: Международная конференция SIN 2014 г. Глазго (Шотландия). Делегация из ЮФУ: профессора Бабенко Л.К. и Макаревич О.Б., доцент Аникеев М.В., студент 5-го курса кафедры БИТ Гаркуша М.А.