Ministry of Education of the Republic of Belarus
Educational Institution
Belarusian State University of Informatics and
Radioelectronics

UDC 004.056.061

Аль-Аттар Абдалрауф Зухайр Рауф

MODELS AND TOOLS OF INFORMATION DEFENSE COMPONENTS IN CLOUD COMPUTING

ABSTRACT
for master's degree in technical sciences

Specialty 1-45 80 02 Telecommunication systems and computer networks

Scientific supervisor
Professor of the Department
"Infocommunicftion
Technologies"
Doctor of Science, Professor
.U.A. Vishnjakou

Minsk 2020

INTRODUCTION

The relevance of the research topic. Information security has assumed great importance, especially in cloud computing. There are many additionally threats in cloud area, so research topic, connecting with investigation in this direction is relevant and actual.

GENERAL DESCRIPTION OF WORK

Communication with major scientific programs and themes. The dissertation research is performed within the research project «New technologies of information management and e-marketing» № State registration 20162075 from 03.06.2016.

The aims and objectives of the study. The purpose of the master's work - to explore the methods and means of information security systems in cloud computing (CC).

To achieve this goal it is necessary to solve the following related tasks:

- an analysis of information means implementation of cloud computing;
- provide an analysis of models and protection systems in cloud computing;
- submit a software mobile applications in cloud computing with gipervise defense.

The object and subject of investigation. The object of the research is the methods and means of information protection applications in CC.

The subject of research is the protection of information systems in the CC.

The main provisions of the investigation for the defense:

1. Analysis of the methods and means of protection in cloud computing;
2. The analysis of the models of information protection in cloud computing;
3. Presents the software mobile applications in cloud computing with gipervise defense.

Testing results of the investigation. The main provisions of this study were presented at the XVII Belorussian-Russian scien.-technic. conf. «Technical Tools of Information Defense» (Minsk, 11 June 2019) in 2019, seminar «Coding and digital signal processing in infocommunications» (Minsk, April 2020). Minsk: BSUIR, 2020, 56 scientific cong. of PhD, Master and students of BSUIR (Minsk, April 2020). Minsk: BSUIR, 2020.

Publication of the results. The results of the study published three scientific papers (abstracts). Including 3 - in the materials of scientific conferences and seminar.

The structure and scope of the thesis. Structural parts of the thesis: introduction, general characteristics of the work, three chapters, conclusion, bibliography, consisting of 39 titles and 3 authors, 10 pictures , 7 tables.

Short description of work

1.Definition of concept CC security

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

2.Full virtualization - in which unmodified instances of guest operating systems are used, and to support the operation of these OSs, a common layer for emulating their execution on top of the host OS is used, the role of which is a regular OS. Paravirtualization - in which the guest OS kernel is modified, a new set of APIs is included in it, through which it can directly work with the hardware without conflict with other VMs.

3.statement of the problem

The purpose of this chapter of the master's work is to develop a method for unifying information communication between peripheral devices and a mobile application in the cloud, taking into account protection. In order to most effectively move towards the intended goal, we need to decompose it into smaller tasks, the solution of which individually and combining them together should lead us to the specified goal. Since the most popular brand of a mobile device is Apple’s IPhone campaign smartphone, and for it the most reliable devices for commercial tasks are LineaPro 5 and HoneywellSL 42, we will consider them as target devices.

Define the range of tasks to be solved:

• Explore SDK structures provided by LineaPro 5 and HoneywellSL 42 manufacturers.

• Develop a UML diagram of summarized data.

• Implement this approach in the form of a library written in the C # programming language using the VisualStudio 2013 tool.

• Implement a mobile application for communication with various company services that provide a web interface using the framework developed in the previous step.

• Introduce means for monitoring the processes of information interaction between applications and the hypervisor in the cloud.

The result of the solution of the tasks set should be a mobile application with a unified communication method for the most famous and reliable manufacturers of peripherals connected to mobile smartphones and means of monitoring the interaction of applications and the hypervisor in the cloud.

Conclusion

1. На основании анализа выявлены основные требования по безопасности к среде ОВ: круглосуточный мониторинг защищенности; детектирование вредоносного ПО в гостевых ОС и гипервизоре; защита самих ВМ; средства защиты не должны значительно сказываться на производительности подсистемы управления. Выход для провайдеров ОВ – использование специализированных средств защиты, учитывающих технологию виртуализации. целостность данных и приложений; защита периметра и разграничение сети.

2. Основные угрозы для среды ОВ: ВМ *динамичны, они* клонируются и могут «перемещаться» между физическими серверами, что влияет на разработку целостности системы безопасности; с*ерверы ОВ* и локальные физические кластеры используют одни и те же ОС и приложения, что увеличивает «атакуемую поверхность»; к*огда ВМ выключена*, она подвергается опасности заражения; п*ри использовании ОВ* периметр сети размывается или исчезает, что приводит к тому, что защита менее защищенной части сети определяет общий уровень безопасности; д*ля защиты от функциональных атак* для каждого сегмента среды ОВ необходимо использовать следующие средства защиты: для сервера контроллера домена − эффективную защиту от DoS-атак, для Веб-сервера − контроль целостности страниц, для сервера приложений − экран уровня приложений, для системы хранения данных – резервное копирование, разграничение доступа; б*ольшинство пользователей подключаются к облаку*, используя браузер (атаки Cross Site Scripting, «кража» паролей, перехваты сессий браузера, атака «человек посредине» и т. д.); *Большое количество ВМ*, требует наличие систем управления, вмешательство в которую может привести к блокированию работы ВМ; атака на гипервизор может привести к тому, что одна ВМ сможет получить доступ к памяти и ресурсам другой.

3. Определены основные принципы для использования мобильных устройств в облачной среде. Разработано мобильное приложение с использование периферийных устройств для оптимизации коммерческих задач.

4. Сформулировано условие нейтрализации атак на средства виртуализации: каждый компонент с должен обладать привилегиями, не превышающими минимально необходимые для его работы.

Author publications

1 Visniakou U.A. Analysis of users work in cloud computing environment / U.A. Vishniakou, Z.R. Al-Attar Abdulraouf // reports of XVII Belorussian-Russian scien.-technic. conf. «Technical Tools of Information Defense» (Minsk, 11 June 2019). − Minsk : BSUIR, 2019. – P. 11.

2. Visniakou U.A. Analysis and applications of information security in corporate information system, cloud computing and blockchain / Visniakou U.A., AL-Musawi Hani H.J., Z.R.AL-Attar Abdulraouf, R. KH. Khudier // Reports of int. seminar seminar «Coding and digital signal processing in infocommunications» (Minsk, april 2020). Minsk: BSUIR, 2020. – P

3. Visniakou U.A. Defense Tools in corporate information system, cloud computing and blockchain / Visniakou U.A., AL-Musawi Hani H.J., Z.R.AL-Attar Abdulraouf, R. KH. Khudier // Reports of 56 scientific conf. of PhD, masters and students of BSUIR (Minsk, 21 April 2020). Minsk: BSUIR, 2020. – P.