 ISSN 2226-3780

UDK 004.056.5
DOI: 10.15587/2312-8372.2015.51351

Драбик Я. В.,
Ластівка Г. І.

РОЗРОБКА КОМПЛЕКСНОГО ЗАХИСТУ ДАНИХ В СЕРВЕРНИХ ПРИМІЩЕННЯХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Представлено систему комплексного захисту серверних приміщень з використанням стійкої криптосистеми AES-256 у поєднанні з мовою високого рівня програмування Python. Виявлено недоліки сучасних комплексних систем захисту інформації (КСЗІ). Розроблено методику резервування даних, яка базується на поєднанні апаратного та програмного забезпечень.

Ключові слова: *комплексний захист, серверне приміщення, AES-256, Python, резервування даних.*

1. Introduction

On modern level of transition from an industrial society to information one, is becoming increasingly important obtain information and personal data security. That is why the necessity appears to develop and implement new methods of combating malicious online attack on private property. The problem is the inability of most methods to block all ways of information leakage remains a problem [1, 2].

In such a way we come to conclusion that an alternative approach to solve the information security problem is combination of hardware and software provisions. Hardware corresponds to aggregate of means which react on immediate penetration of malefactor to room which keeps data. It includes a variety of moving and smoke detectors, video surveillance system etc. Software corresponds to a program which can perform actions on private information including namely to encrypt it, archive, send it as a file protocols FTP and SMTP.

The developed system can be used in all areas of work which is related to the use of server space, and does not require highly qualified personnel to service the system. This corresponds to actuality of propounded research.

2. Analysis of literature data and problem definition

Potentially possible events, process or phenomenon which can cause destruction, integrity or confidentiality losses or annihilation of access to information are known to be the threat of security information. All possible potential dangers in complex systems can be divided into two classes (Fig. 1) [3].

Developed complex security uses AES cryptosystem which is fast in software and works efficiently on hardware level. This system works quickly even on small-sized devices as smart phones, smart-cards etc. AES provides higher security level due to increase of block size and long keys [4–7].

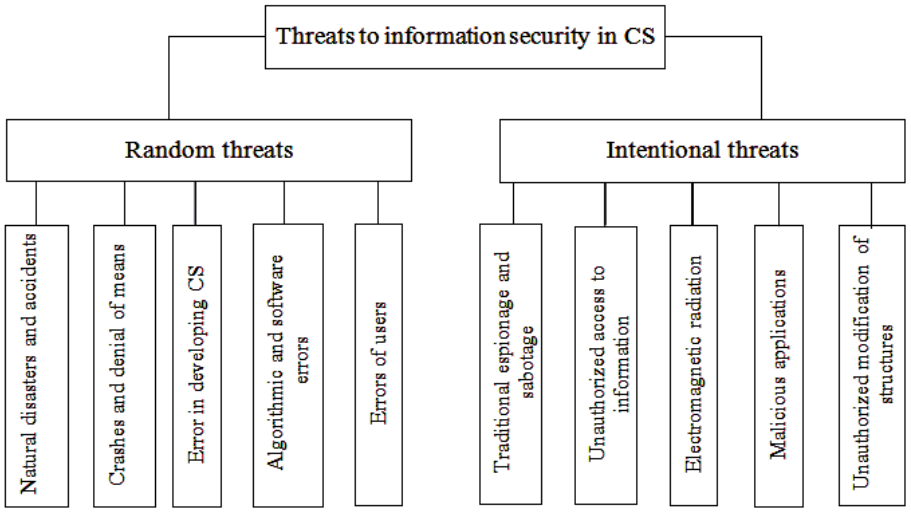

Fig. 1. Classification of information security threats in computer systems

Information Security System must have several levels which will supplement each other, and therefore such systems better to build on the principle of fractals [8]. In such case to obtain closed information the malefactor must 'crack' all protection levels (Fig. 2).

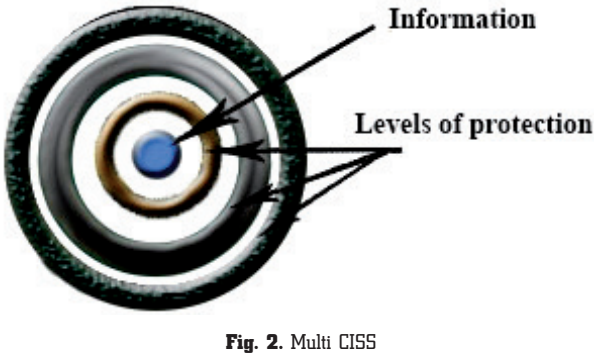

Fig. 2. Multi CISS

For Complex Information Security System (CISS) we can select 6 security levels:

1. Protection of territory of an object;
2. Protection of building;
3. Protection of room;
4. Protection of hardware;
5. Protection of software;
6. Data protection.

3. Object, aim and objectives of research

The object of research — high quality complex security of server rooms (CSSR).

The aim of work — development of complex security system of server room, which combines hardware and software. This system operates after the next algorithm: after triggering of any detector from hardware the alert goes to main frame of security system and sends a signal on server with appropriate software (Fig. 3).

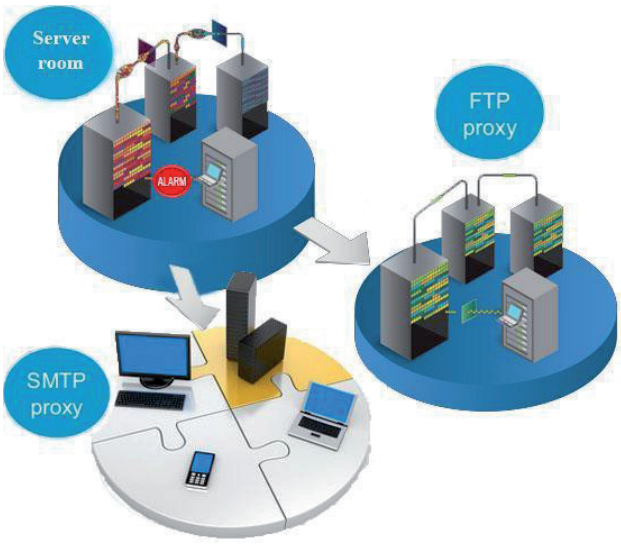

Fig. 4. Data reservation

Fig. 3. The combination of software and hardware method implementation schematic sequence

To achieve the aim next basic problems had to be solved:

1. Analysis of existing analogues of CSSR with determination of their advantages and disadvantages.
2. Simulation and creation of CSSR including advantages of existing analogues.
3. Testing of developed CSSR on the object of security.
4. Analysis of achieved results of developed CSSR.

4. Results and methodology for data reservation

Program part allows reservation data of up to 50 Mb (after the SMTP protocol) and over than 50 Mb (after the FTP protocol), with the speed of 15–20 sec (after the SMTP protocol) and 2–3 sec (after FTP protocol) if dimensions of file is 50 Mb.

Thanks to using symmetric cryptosystem AES-256 whose key length is 256 managed to achieve bit maximum crypto stability compared to alternative software-hardware complex information security system Secret Disk Secret NG 3.2 which uses cryptosystem DES with length key of 56. DES requires more powerful processor in comparison to AES which results into decrease of efficiency. AES is better than DES both in software and hardware [9, 10]. For instance to 'crack' AES-256 we need more than $3{,}78 \times 10^{63}$ years on condition that we go over a million keys per second.

Herewith as follows from (Fig. 4) developed CISS allows saving of private information even is a case of theft of equipment.

5. Conclusions

As a result of research:

1. An optimal cryptosystem for CSSR has been found, namely AES-256.
2. Reliable methodology of data reservation has been developed.
3. The speed of software part of program has been increased due to the use of high-level program language Python.
4. Managed to keep data integrity in a case of unauthorized access to the room.

References

1. Shcheglov, O. Yu. Zashchita komp'iuternoi seti ot NSD [Text] / O. Yu. Shcheglov. — SPb., 2004. — 384 p.
2. Skripnik, D. A. Obespechenie bezopasnosti personal'nyh dannyh [Text] / D. A. Skripnik. — M., 2009. — 78 p.
3. Zavgorodnii, V. I. Kompleksnaia zashchita informatsii v komp'iuternyh sistemah [Text] / V. I. Zavgorodnii. — M.: Logos, 2001. — 264 p.
4. Naji, A. W. Novel Approach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard [Text] / A. W. Naji, I. A. S. Muhamadi // Proceeding of World Academy of Science Engineering and Technology (WASET). — 2010. — Vol. 56, № 5. — P. 498–502.
5. Abomhara, M. Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard [Text] / M. Abomhara, O. Zakaria, O. Khalifa, A. Zaidan, B. Zaidan // International Journal of Computer and Electrical Engineering. — 2010. — Vol. 2, № 2. — P. 223–229. doi:10.7763/ijcee.2010.v2.141
6. Naji, A. W. Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques [Text] / A. W. Naji, S. A. Hameed, B. B. Zaidan, W. F. Al-Khateeb,

O. O. Khalifa // International Journal of Computer Science and Information Security. — 2009. — Vol. 3, № 1. — P. 73–78.
7. Hamdan, A. New Frame Work of Hidden Data with in Non Multimedia File [Text] / A. Hamdan, H. A. Jalab, A. A. Zaidan, B. B. Zaidan // International Journal of Computer and Network Security. — 2010. — Vol. 2, № 1. — P. 46–54.
8. Tehnicheskie sistemy zashchity informatsii [Text]: katalog. — M.: AOZT «Nelk», 1998. — 56 p.
9. Taqa, A. New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm [Text] / A. Taqa, A. A. Zaidan, B. B. Zaidan // International Journal of Computer and Electrical Engineering. — 2009. — Vol. 1, № 5. — P. 566–571. doi:10.7763/ijcee.2009.v1.87
10. Zaidan, A. A. A New System for Hiding Data within (Unused Area Two + Image Page) of Portable Executable File Using Statistical Technique and Advance Encryption Standared [Text] / A. A. Zaidan, B. B. Zaidan, H. A. Jalab // International Journal of Computer Theory and Engineering. — 2010. — Vol. 2, № 2. — P. 218–225. doi:10.7763/ijcte.2010.v2.143

РАЗРАБОТКА КОМПЛЕКСНОЙ ЗАЩИТЫ ДАННЫХ В СЕРВЕРНЫХ ПОМЕЩЕНИЯХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Представлена система комплексной защиты серверных помещений с использованием устойчивой криптосистемы AES-256 в сочетании с языком высокого уровня программирования Python. Выявлены недостатки современных комплексных систем защиты информации (КСЗИ). Разработана методика резервирования данных, основанная на сочетании аппаратного и программного обеспечения.

Ключевые слова: комплексная защита, серверное помещение, AES-256, Python, резервирование данных.

Драбик Ярослав Вікторович, *кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет ім. Ю. Федьковича, Україна,* ***e-mail: slava.drabyk@gmail.com****.*
Ластівка Галина Іванівна, *кандидат технічних наук, доцент, кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет ім. Ю. Федьковича, Україна.*

Драбик Ярослав Викторович, *кафедра радиотехники и информационной безопасности, Черновицкий национальный университет им. Ю. Федьковича, Украина.*
Ластивка Галина Ивановна, *кандидат технических наук, доцент, кафедра радиотехники и информационной безопасности, Черновицкий национальный университет им. Ю. Федьковича, Украина.*

Drabyk Yaroslav, *Yuriy Fedkovych Chernivtsi National University, Ukraine,* ***e-mail: slava.drabyk@gmail.com****.*
Lastivka Galyna, *Yuriy Fedkovych Chernivtsi National University, Ukraine*