UDC 621.396.61

M.Z.Yakubova[1], T.G.Serikov[2]

[1]*Almaty University of Power Engineering & Telecommunications;*
[2]*Kazakh National Technical University*
*(E-mail: Tansaule_s@mail.ru)*

# IP PBX Asterisk NOW telecommunication network and choice of tools for carrying out attacks. Development and research of the attack scheme to the developed client–server network on the basis of Wi-Fi

Communication of clients with the server passes through a wireless point of Wi-Fi access. The attacking device is the laptop which has the software package of CommView for Wi-Fi. The analysis of stability program by automatic telephone exchange on the basis of Asterisk NOW from unauthorized access to a telecommunication network is provided in this article. The software product on the basis of Asterisk NOW uses as the server. As softfon and client base laptops, computers, and gadgets on which passes test are considered. Communication of clients with the server passes through a wireless point of Wi-Fi access. The attacking device is the laptop on which the software package of CommView for Wi-Fi is established. By the result of carried out test the analysis of network's vulnerability was made. Recommendations about a measure of protection from unauthorized access are made. The optimum option of network protection is offered.

*Key words:* Wi-Fi, wireless network, attacks, address, network devices, server, access, Asterisk NOW.

For the developed network of the technology of systems and communications chair of Karaganda state technical university established laboratory will be test on carrying out attack is carried out from malicious to a network for definition of weak spots in a network. And the measures taken on its protection.

Performance of productivity requires consideration of a question according to the solution of the following tasks:

1. Development of the software product of modeling of attacks in the CommView for Wi-Fi network.
2. Development of the scheme of attack malicious on a network the client server.
3. Analysis of results of attack and development of offers on taking measures of protection of a network**.**

1. Development of the software product of modeling of attacks in the CommView for Wi-Fi network.

CommView for Wi-Fi is the software product intended for monitoring and the analysis of network packages in wireless networks of standards of 802.11 a/b/g/n/ac, productivity uniting in itself, flexibility and convenience of use. Development of the scheme of attack of a network the client server when the studied technology of attack is wireless is actual.

CommView for Wi-Fi has opportunity to take all network packages broadcast for the subsequent detailed display of important information: list of points of access and knots, statistics on each knot and channel, level of a signal, list of packages and network connections, schedules of distribution of protocols, etc. By means of this information of CommView will help us to look through and in detail to analyze each package, to reveal problems in work of networks. The VoIP module intended for the profound analysis, record and reproduction of voice messages of SIP protocol and H.323 also is a part of CommView for Wi-Fi. Packages can be decoded with use of the user keys of WEP or WPA-PSK and to decode up to the lowest level. Supporting more than 70 protocols, CommView for Wi-Fi allows to study in detail the taken packages, using convenient, tree system of display of legal levels and headings of packages [1].

2. Development of the scheme of attack malicious on a network the client server. The developed scheme of attack to a network is given in Figure 1.

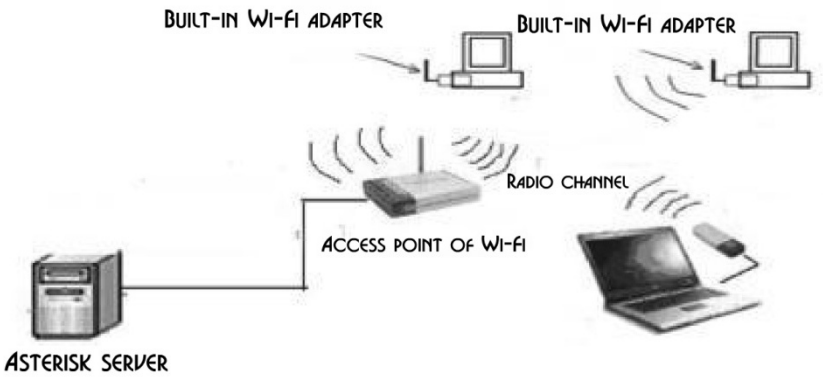


Figure 1. Scheme of wireless attack of a network the client — the server

In the given drawing a network the client server is constructed on the basis of automatic telephone exchange of AsteriskNow which is the server, personal computers, laptops mobile devices in which are registered softfona can be clients. Communication of clients with the server passes through a wireless point of access of Wi-Fi. The attacking device is the laptop on which the software package of CommView for Wi-Fi is established [2].

The fragment of results of attack of the videoconference of a LAN used during on the basis of automatic telephone exchange of AsteriskNow is given in Figure 2. Apparently from drawing in the course of attack the quantity of the packages created thus and other data are revealed on MAC address of computers of participants of a video conference.

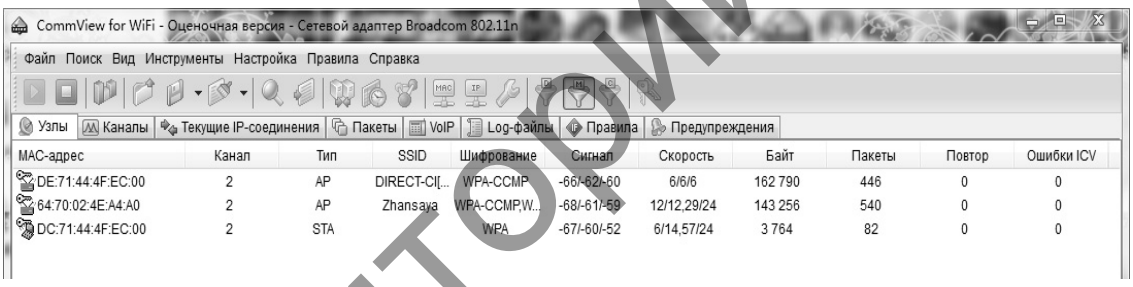


Figure 2. Results of attack to a LAN

If CommView for Wi-Fi isn't started, our adapter will be able to exchange data with other wireless hosts or points of access as as if we use the original driver provided by the producer of our card. If CommView for Wi-Fi is started, our adapter will be transferred to the passive mode of monitoring in the promiscuous mode. In Figure 3 results of MAC addresses of other computers which are within the working range of network functioning are given.

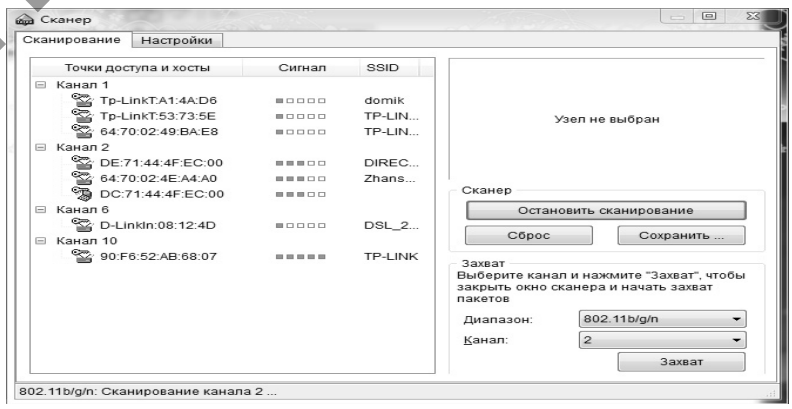


Figure 3. Results of attack when the driver isn't adjusted on the attacked network

The VoIP module intended for the profound analysis, record and reproduction of voice communications of the SIP and H.323 standards is a part of CommView for Wi-Fi. CommView for Wi-Fi supports decoding ofthe following protocols: ARP, FTP, HTTP, HTTPS, ICMP, ICQ, IPsec, IPv4, IPv6, IPX, SSH, TCP, TELNET, TFTP, 802.1Q, 802.1X [3; 78].

CommView for Wi-Fi is the full-function and available tool for administrators of wireless networks, experts in the field of network safety, network programmers or those who wants to see all picture of a traffic in a wireless network. In Figure 4 the statistics of a network traffic, and is given in Figure 5 statistics of distribution of a traffic in a network.

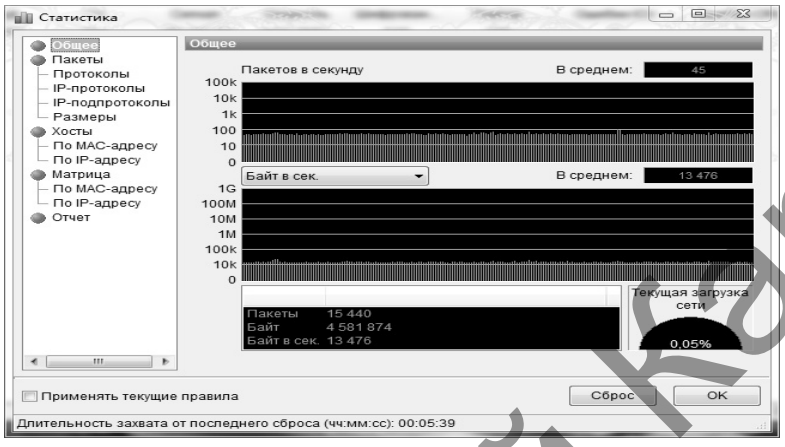


Figure 4. Statistics of distribution of a traffic in a network

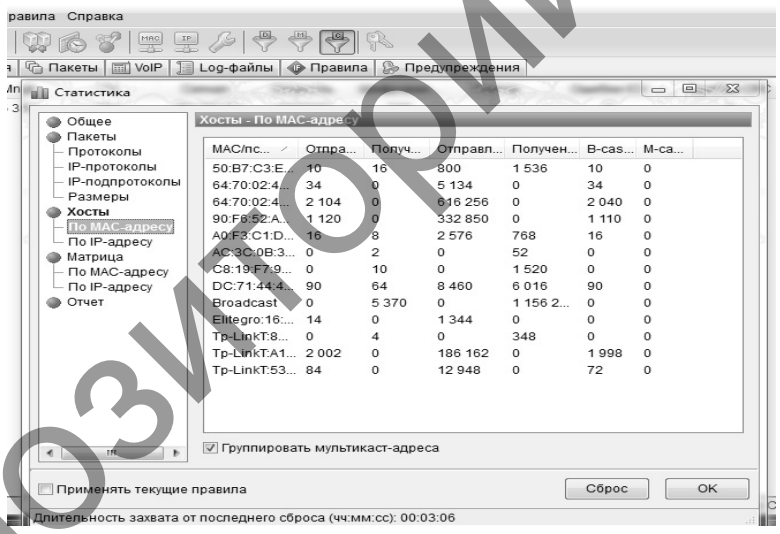


Figure 5. The report on IAC to addresses of the sent and received packages

In Figure 5 the report showing the received and sent packages to the addresses taken by IAC In the experiment given on drawing 1 server is provided is connected to an access point on wire technology.

3. Analysis of results of attack and development of offers on taking measures of protection of a network.

We will consider option when a network the client server is completely wireless. For this purpose it is necessary:

1. To establish the program FTP110 file the server on the computer and we will adjust the server FTP parameters.

2. To establish on other FileZilla computer and to adjust its parameters.

3. To develop the scheme of attack, the server through a wireless point of access AP-3200.

On the laptop of the malefactor we will start the ComView for Wi-Fi program.

To appoint the IP address of the client according to Figure 6.

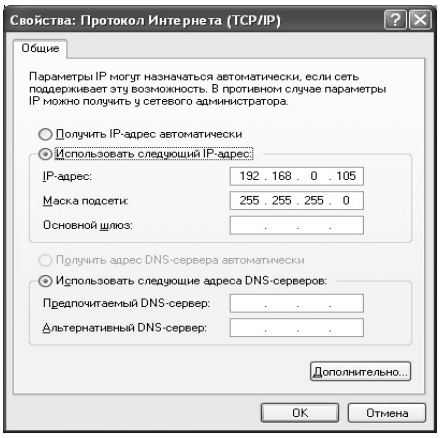


Figure 6. IP installation of the address of the client

To adjust the FTP server with the following parameters the user — samal, the password — 12345 and etc. as shown in Figure 7.

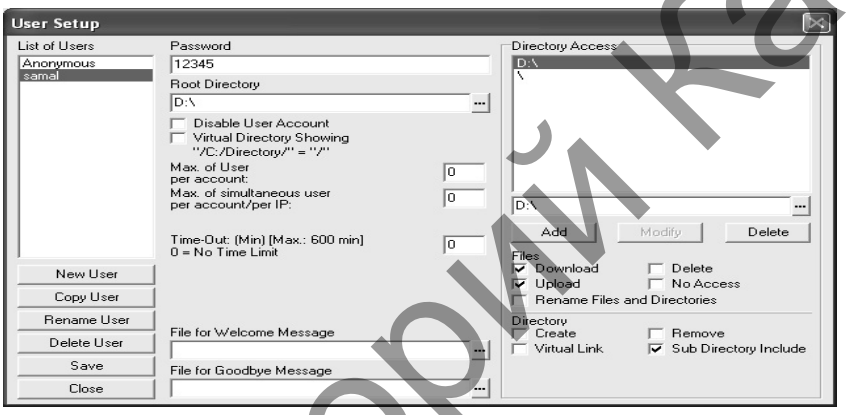


Figure 7. The FTP installation of the server with the specified parameters

To adjust the FTP parameter of the client, according to the below-specified Figure 8.

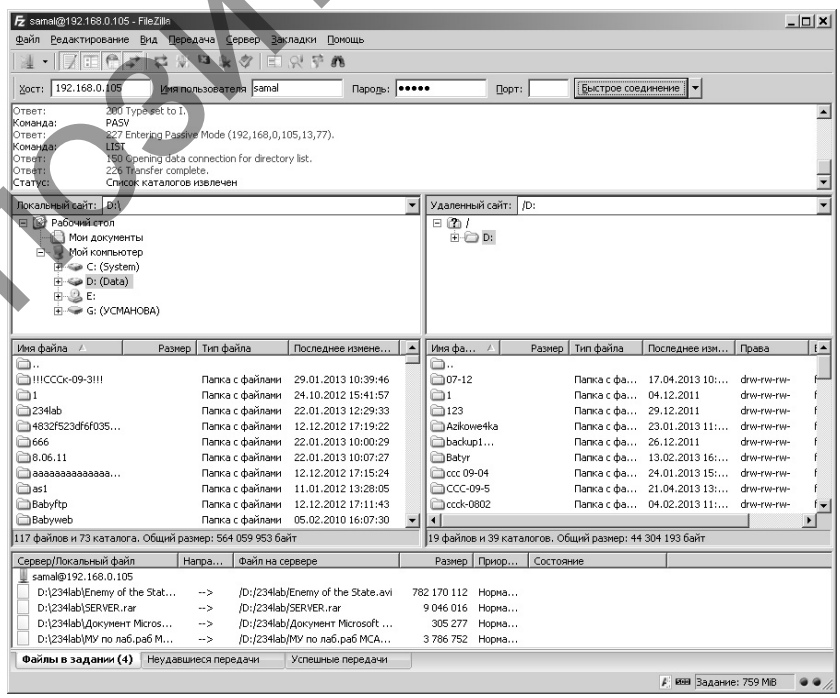


Figure 8. Control of the FTP parameter of the client

On the FTP program of the client we press the Fast Connection button, thus appears server directories in Figure 8 on the right.

On the left side Figure 8 we note the folder and a dragging method a mouse from server directories the chosen file in this folder.

The malefactor adjusts the software package of CommView for Wi-Fi on the computer. At the malefactor it is possible to see information provided on Figure 9.

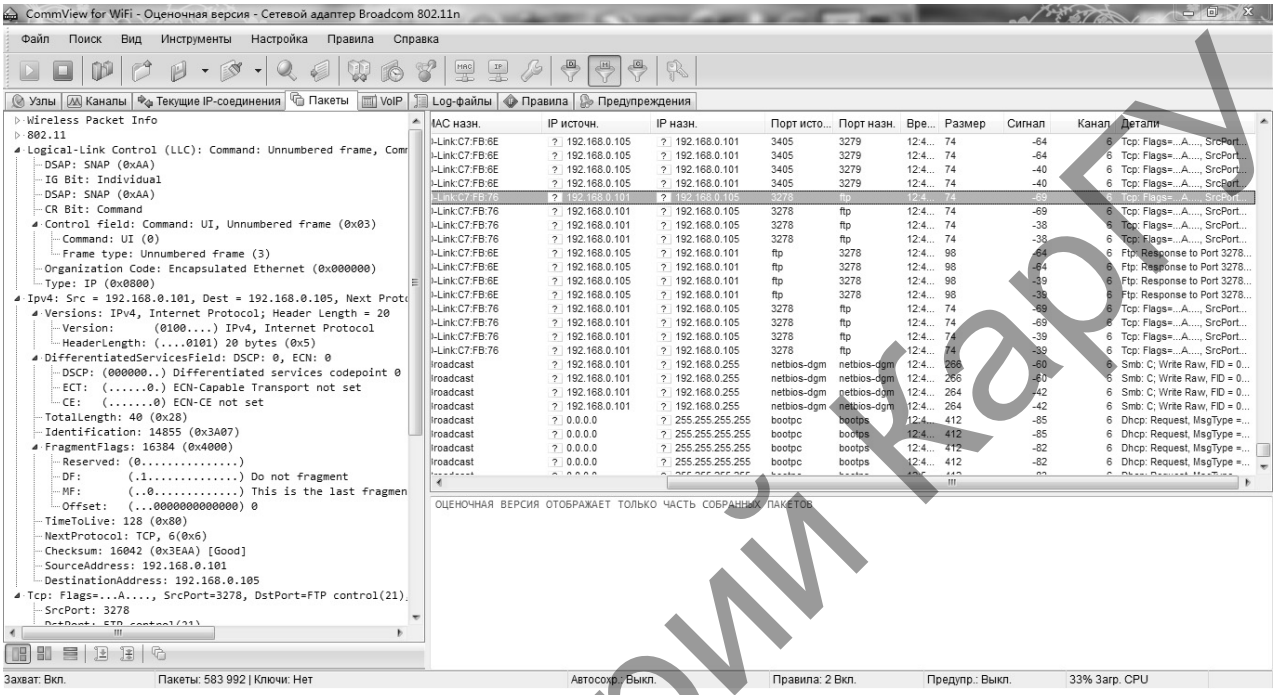


Figure 9. CommView for Wi-Fi Interface

9. We press two times on the chosen FTP protocol of the right button of a mouse and we receive drawing the showing FTP protocol interface between the client and the server the Figure 10 explaining session TCP.

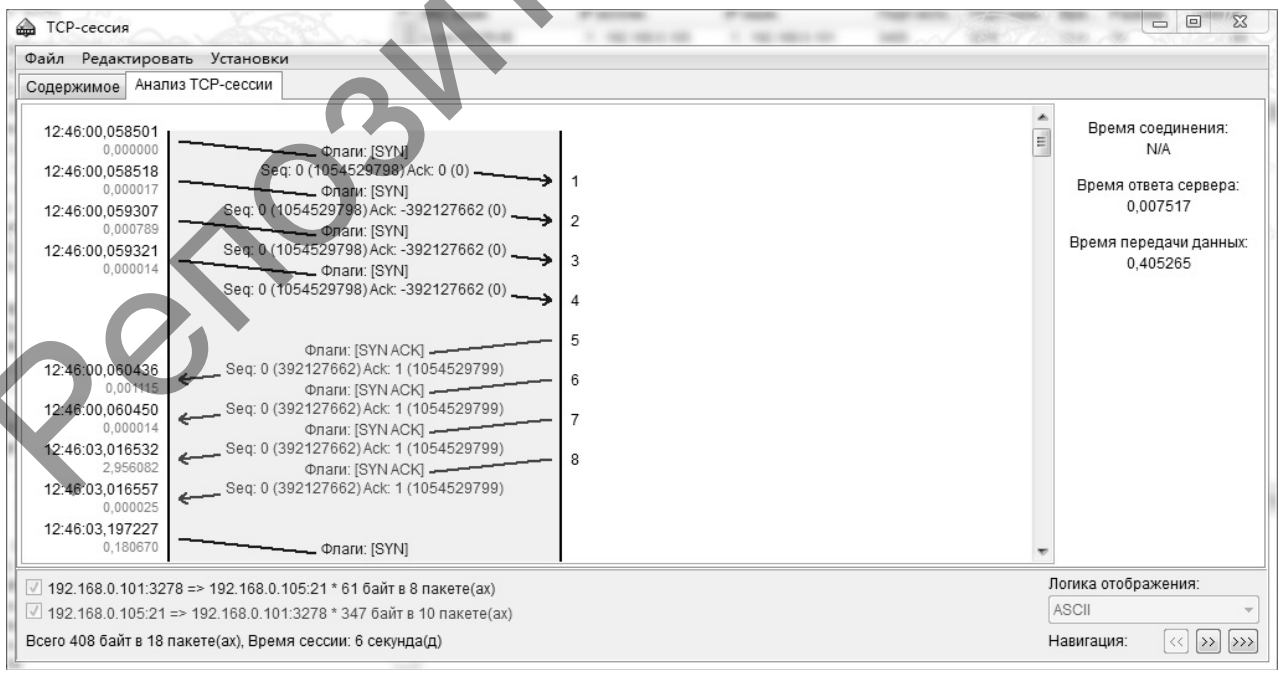


Figure 10. TSR session

10. Pressing the Contents tab we receive the login and the password of the server found by the malefactor as it is recorded in Figure 11.

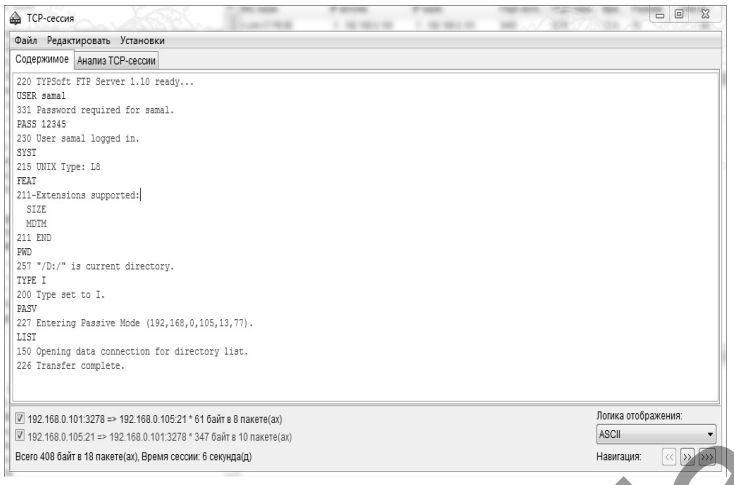


Figure 11. Tab contents

Apparently from the conducted research any networks need to be protected as it is easily possible as a result of receiving unauthorized access to resources of a wireless network, the malefactor can:

• to get access to internal network resources of a wireless network;

• to intercept a network traffic of a wireless network for its further research;

• to use connection to the Internet for the needs.

We will understand prevention of unauthorized access for the malefactor to network resources as protection of the wireless Wi-Fi networks.

There are following methods of protection: restriction of access to internal resources of a network.

It is necessary to provide differentiation of access rights to internal resources of a wireless network. This measure allows to protect internal resources of a network even when receiving by the malefactor access to the most wireless network [1]. Modern network devices (Wi-Fi routers etc.) allow to realize the firewall (painted walls) limiting possibility of unauthorized access to a wireless network from the outside with use of the built-in software. The algorithm of operation of the network device generally, and the network screen in particular, is defined by the current version of an insertion of the network device. Producers of network devices in process of detection of mistakes and potential vulnerabilities in insertions, let out their updatings. Therefore it is extremely desirable to update in due time an insertion of the network device and to use only its latest version in work.

Enciphering of a network traffic. Besides connection to network resources the malefactor also has possibility of interception of the traffic generated in the course of its work. Modern network devices support a wide range of the opportunities of enciphering based on the WPA technology (Wi-Fi Protected Access) and its modifications (WPA2, WPA-PSK etc.) [4, 5]. Use of the WPA technology not only allows to provide enciphering of a network traffic in a wireless network, but also to prevent unauthorized connection to it: for connection to the wireless network protected with use of WPA, the client has to specify the access key established by the administrator. Within the network device there is an opportunity to define the list of physical addresses (MAC addresses) which will have access to a wireless network (or on the contrary — which access to a wireless network will be forbidden) [6]. Having determined the filter by MAC addresses, there is an opportunity to limit access to a wireless network even without use of algorithms of enciphering.

Treat advantages of IP-telephony: its low cost, reliability, high speed of communication and simplicity of use. It uses the most advanced technology of compression of our voice signals, and completely uses the capacity of telephone lines. Therefore packages of data from different inquiries, and even their various types, can move on the same line to one and too time the Internet, but also in other networks of data transmission with package switching (local, corporate, regional) [5].

As a result of the conducted researches it is revealed that at expansion of corporate networks there is a sense to introduce program IP PBX instead of electronic and digital automatic telephone exchanges,

the prize turns out not only at cost, but also on acquisition of technologies which electronic and digital automatic telephone exchanges don't provide.

The carried-out calculations show that in a point of access to a network with Asterisk the multimedia stream thus is had enough to have an access point the speed of transfer of 54 Mgb providing for a multimedia traffic and a pass-band 2 GHz.

The scheme of wireless attack of a network the client — the server is developed and experiment on attack of a network the client the server is made.

On the developed scheme of a network on chair test on carrying out attack for the first time is carried out from the malefactor on a network for definition of weak spots to networks and offers of taking measures to its protection, problems are for this purpose solved on:

– To studying and development of the program instrument of modeling of attacks in the CommView for Wi-Fi network.
– Experiments in the developed network of attack of the malefactor are made and results in drawings and tables of screenshots are given.
– On the basis of research of results of attack offers on taking measures of protection of a LAN are also developed.

References

1 *Якубова М.З*. Разработка топологии сетевой атаки на основе пакета программ Wireshark // ПОИСК Международный научный журнал-приложение РК. Серия естественных и технических наук. Высш. шк. Казахстана. — 2013. — № 2 (2). — [ЭР]. Режим доступа: http://www.aipet.kz/article/facultet/frts/ikt/15/9.pdf

2 *Шахнович И*. Современные технологии беспроводной связи. — М.: Техносфера, 2006. — 288 с.

3 *Рошан П., Лиэри Дж*. Основы построения беспроводных локальных сетей стандарта 802.11. — М.: Бук-Пресс, 2004. — 428 с.

4 *Якубова М.З*. Разработка критериев и требований по информационной безопасности // ПОИСК. Международный научный журнал-приложение РК Серия естественных и технических наук. Высш. шк. Казахстана. — 2013. — № 2 (2). — [ЭР]. Режим доступа: http://szgmu.ru/upload/files/Документы%20кафедр/СБОРНИК_ОЗИЗ_2013.pdf

5 Беспроводные сети: Вегешна Шринивас: пер. с англ. — М.: Изд. дом «Вильямс», 2003. — 26 с.

6 *Якубова М.З*. Разработка экспериментальной технологии пассивной атаки // ПОИСК Международный научный журнал-приложение РК. Серия естественных и технических наук. Высш. шк. Казахстана. — 2013. — № 2 (1). — [ЭР]. Режим доступа: http://www.aipet.kz/article/facultet/frts/ikt/15/6.pdf

М.З.Якубова, Т.Г.Сериков

## IP PBX Asterisk NOW телекоммуникация желісі және шабуыл жасау үшін құралдарды таңдау. Wi-Fi негізінде құрастырылған клиент–сервер желісіне шабуыл жасау үшін схемаларды өңдеу және зерттеу

Клиенттер мен сервердің арасындағы байланыс сымсыз байланыс нүктесі Wi-Fi арқылы жүзеге асады. CommView for Wi-Fi программаның жиынтығы қондырылған ноутбук шабуыл жасаушы негізгі құрал болады. Мақалада Asterisk NOW базасындағы программалық АТС-тің телебайланыс жүйесіне рұқсатсыз қосылысқа тұрақтылық сараптамасы жүргізілген. Сервер ретінде Asterisk NOW базасындағы программалық өнім зерттелген. Программалық телефон және клиенттік база ретінде сынақ жүргізілген ноутбуктар, компьютерлер және гаджеттар алынған. Сынақтар жасалған кезде алынған нәтижелер бойынша желінің төзімділігі талданды. Рұқсатсыз байланыстан қорғану мақсатында ұсыныстар берілді. Желіні қорғауға арналған оңтайлы шешім ұсынылды.

М.З.Якубова, Т.Г.Сериков

# Телекоммуникационная сеть IP PBX Asterisk NOW и выбор инструментальных средств для проведения атак. Разработка и исследование схемы атаки на разработанную сеть клиент–сервер на базе Wi-Fi

В статье отмечено, что связь клиентов с сервером проходит через беспроводную точку доступа Wi-Fi. Атакующим устройством является ноутбук, на котором установлен пакет программ CommView for Wi-Fi. Авторами приведен анализ устойчивости программного АТС на базе Asterisk NOW от несанкционированного доступа к сети телекоммуникации. В качестве сервера выступает программный продукт на базе Asterisk NOW, в качестве софтфонов и клиентской базы рассмотрены ноутбуки, компьютеры и гаджеты, на которых проходит испытание. Связь клиентов с сервером проходит через беспроводную точку доступа Wi-Fi. По результатом проведенных испытаний сделан анализ уязвимости сети. Даны рекомендации по мере защиты от несанкционированного доступа. Предложен оптимальный вариант защиты сети.

## References

1 Yakubova M.Z. *POISK International scientific magazine-application of RK Series of natural and technical science of the higher school of Kazakhstan*, 2013, 2 (2) Kazakhstan, [ER]. Access mode: http://www.aipet.kz/article/facultet/frts/ikt/15/9.pdf

2 Shakhnovich I. *Modern technologies of a wireless communication*, Moscow: Tekhnosfera, 2006, 288 p.

3 Roshan P., Lieri Dzh. *Bases of creation of wireless local networks of the standard 802.11*, Moscow: Bouck Press, 2004, 428 p.

4 Yakubova M.Z. *POISK International scientific magazine-application of RK Series of natural and technical science of the higher school of Kazakhstan*, 2013, 2 Kazakhstan, [ER]. Access mode: http://szgmu.ru/upload/files/Документы%20кафедр/СБОРНИК_ОЗИЗ_2013.pdf

5 Wireless networks: Vegeshna Shrinivas. The lane with English, Moscow: Williams publishing house, 2003, 26 p.

6 Yakubova M.Z. *POISK International scientific magazine-application of RK Series of natural and technical science of the higher school of Kazakhstan*, 2013, 2 (1) Kazakhstan, [ER]. Access mode: http://www.aipet.kz/article/facultet/frts/ikt/15/6.pdf