РАДИОФИЗИКА ЖӘНЕ ЭЛЕКТРОНИКА РАДИОФИЗИКА И ЭЛЕКТРОНИКА RADIOPHYSICS AND ELECTRONICS

UDC 654.028

M.Z. Yakubova¹, V.P. Razinkin², T.G. Serikov³, A.K. Muratova⁴

¹Almaty University of Power Engineering & Telecommunications; ²Novosibirsk State Technical University, Russia; ³Kazakh National Technical University, Almaty; ⁴Karaganda State Technical University (E-mail: mubor149@rambler.ru)

Protection of IP-telefony networks on the basis of Asterisk from interception of data

Nowadays the new round of technologies development on voice transfer, and IP-telephony is observed. In a type of the growing levels of demand and popularity of IP-telephony as bases of corporate communication infrastructure creation there is a question of ensuring at most a level of its safety. As the server of IP-telephony has direct access to the network the Internet, and authentication of subscribers happens to IP addresses. In this article the issue of safety of telephony on the basis of Asterisk from interception of these clients is resolved. As the network analyzer the software of Wireshark is used. As softfon and client base laptops, computers, and gadgets on which passes test are considered. Communication of clients with the server passes through a wire-less point of WiFi access. The attacking device is the laptop on which the software package of CommView for WiFi 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: IP-telefony, protocol, address, wireless attacks, server, portal, Asterisk.

For the developed information technology of telecommunication systems' chair of Karaganda state technical university established laboratory had tested on carrying out protection was carried out from malicious to a IP-telefony network for definition of weak spots in a network. And the results were taken on its protection. Generally information gets huge value, and modern technologies allow to bring her in every spot on the globe very quickly and without use of the expensive machinery and equipment. In fact, the mankind is mantering information century. Therefore transfer questions and information reception move to the forefront.

Transition from traditional telephone networks to networks of IP-telephony is noted. The main difference of new networks is the applied principle of switching, namely application of packages' switching. Telephony turns from complex structure with a huge number of the equipment and personnel into one of data's services transmission networks. Application of IP-telephony gives to the client a set of opportunities and minimum price for services. They provide services of a speech transfer and video traffic to any subscriber connected to network (for example, the Internet) [1].

One of the most widespread systems of IP-telephony is the system of IP-telephony Asterisk. This system allows to work with different protocols of IP-telephony, provides a broad set of services. The system is well programmed and is widespread [2].

The most popular protocol of IP-telephony is SIP (Session Initiation Protocol). This protocol differs in simplicity (and proximity to the HTTP protocol (HyperText Transfer Protocol)), independence of transport protocols, integration with a stack of protocols of TCP/IP, a possibility of work with other protocols. Asterisk supports the SIP protocol and this protocol is applied on that most often. For this reason in this article the protocol of telephony is considered. With increase of the information price also need for its protection increases. There is a set of information's interception ways against to the fight for ensuring confidentiality of subscribers. To show vulnerability of the user data, we will use program providing Wireshark [3].

Wireshark is one of the most popular and powerful modern network analyzers. It is capable to carry out interception of a traffic, the analysis of shots headings, packages, etc. and to carry out viewing of directly transmitted data. The program is capable to analyze a traffic on many signs. In particular, it is capable to distinguish and give streams of audio and video. The built-in tools allow to allocate data flows and to present them in a convenient format (it's true for audio, it is possible to keep video as the block of data and to format) [4].

The purpose of the research is to resolve the issue of safety of telephony on the basis of Asterisk from interception of these clients by taking as the server of IP-telephony has direct access to the network the Internet, and authentication of subscribers happens to IP addresses and As the network analyzer the software of Wireshark is used. 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 WiFi access.

Let's review an example of such interception. The call between two users of Asterisk without enciphering has been for this purpose carried out. Wireshark established on IP-telephony server carries out interception of data.

As a result of the intercepted data's observations the following facts have been elicited.

Firstly, it is possible to watch frames of the SIP protocol and to look through them (including the user data). The password is ciphered by MD5 (Message Digest 5) algorithm and therefore it can't be read in opened, but there is a possibility of activity observation of users.

Secondly, there is a possibility of a talk interception. After the end of a call to Wireshark the choice of the Telephony menu, and in its subparagraphs of «RTP» (Real-time Transport Protocol) and «Show all streams» is carried out. The program displays streams (Fig. 1):

		etho	-	eshark 1.8.10 (S		nown fro	m unknown	1)]			
		_	W	/ireshark: RTP St	treams	_			_ 0	×	
	Det	tected 8 RTP si	reams. (Choose one for for	ward and rever	se directio	n for analysis	5			
rc IP addr 🗸	Src port	Dst IP addr	Dst po	ort SSRC	Payload	Packet	Lost	Max Delta	(ms)	м	
92.168.0.101	40100	192.168.0.108	14444	0x296CB056	g711U	1085	1 (0.1%)	72.13		6.	
92.168.0.101	40120	192.168.0.108	12802	0x3AB09FDD	D H264	1905	4 (0.2%)	126.01		2. 2,	Fime=187020
92.168.0.105	40100	192.168.0.108	15142	0xDC59909	g711U	1067	1 (0.1%)	68.79		4. 905	, Time=172
92.168.0.105	40120	192.168.0.108	18894	0x674F3D6	H264	1114	1 (0.1%)	142.67		5.	Time=18702
92.168.0.108	15142	192.168.0.105	40100	0x7F8E60DA	g711U	1085	1 (0.1%)	72.13		h l	, Time=172
2.168.0.108	14444	192.168.0.101	40100	0x402B9911	g711U	1066	2 (0.2%)	68.48			Fime=187020 , Time=1720
2.168.0.108	12802	192.168.0.101	40120	0x4DA028DF	H264	1108	7 (0.6%)	142.43		and contract of the	, Seq=1066
2.168.0.108	18894	192.168.0.105	40120	0xEFDBA0B	H264	1903	6 (0.3%)	126.00			1, Seq=436
	10004	192.100.0.10.									
	10004	152.100.0.10.									5, Seq=108
	10034	152.150.0.10.								60D/	A, Seq=143
	10054									60D/ 909	A, Seq=143 , Seq=1067
	10034	Sele	t a forw	ard stream with lef			n			60D/ 909	A, Seq=143 , Seq=1067 1, Seq=436
		Sele	t a forw ect a rev	ard stream with lef	Ctrl + left mou	se button				60D/ 909	A, Seq=143 , Seq=1067
Unselect	Find Reve	Sele	t a forw ect a rev	ard stream with lef				lyze	Close	60D/ 909	A, Seq=143 , Seq=1067 1, Seq=436
Unselect	Find Reve	Sele Sel Erse Save	t a forw ect a rev As	ard stream with lef	Ctrl + left mou	se button		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect	Find Reve	Sele	t a forw ect a rev As	ard stream with lef	Ctrl + left mou	se button		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect	Find Reve	Sele Sel Erse Save	t a forw ect a rev As	ard stream with lef	Ctrl + left mou	se button		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect	Find Reve	Sele Sel Erse Save	t a forw ect a rev As	ard stream with lef	Ctrl + left mou	se button		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect	Find Reve	Sele Sel Erse Save	t a forw ect a rev As	ard stream with lef	Ctrl + left mou	se button		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect	Find Reve	Sele Sel Erse Save	t a forw ect a rev As	ard stream with lef	Ctrl + left mou	se button		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect	Find Reve	Sele Sel Erse Save	t a forw ect a rev As	ard stream with lef	Ctrl + left mou	se button		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect ddress Resc	[Find Reve	Sele Sel Save Save	t a forw ect a rev As	ard stream with lef verse stream with (Mark Packets)	Ctrl + left mou	Copy		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect ddress Reso	Find Reve	Sele Se erse Save otocol (requ	t a forw ect a rev As est)	ard stream with lef verse stream with (Mark Packets) P	Ctrl + left mou repare Filter	g		lyze		60D/ 909	A, Seq=143 , Seq=1067 1, Seq=436
Unselect ddress Resc) ff ff ff 08 00 06	[Find Reve	Sele: Sei Save Ditocol (requ 00 01 6c 60 00 01 6c 60	t a forw ect a rev As est) 1d 67 1d 67	ard stream with lef verse stream with (Mark Packets) P	Ctrl + left mou	g		lyze		60D/ 909	A, Seq=143 , Seq=1067
Unselect ddress Resc ff ff ff ff 08 00 06 00 00 00	find Reve olution Pro	Sele Sel Prse Save Dtocol (requ 00 01 6c 60 c0 a8 00 01	t a forw ect a rev As est) 1d 67 1d 67	ard stream with lef verse stream with (Mark Packets) P 08 06 00 01 00 a8 00 64 00 00 00 00	Ctrl + left mou repare Filter	se button Copy g gd		lyze		60D/ 909	A, Seq=143 , Seq=1067

Figure 1. RTP streams, captured by Wireshark

By pressing of the Analyze button Wireshark provides the analysis of the chosen stream on shots. At the same time there is a possibility of a stream preservation (the Save payload button). The stream can be kept in a format of uncompressed data (.raw) or in an audioformat (.au) (the last is right for the G.711 audiocodec).

Follows from the aforesaid that additional measures are necessary for protection of the user traffic. Mechanisms of a traffic protection of telephony against interception are provided in Asterisk. The linking of the TLS (Transport Layer Security) and SRTP (Secure Real-time Transport) protocols is for this purpose used. TLS — the protocol of the fifth, session level of the OSI model providing information security by its transfer through package networks by establishment of the protected connection.

The protocol works as follows. The client sends inquiry for connection establishment to the server, and also sends data on available protocols of enciphering. The server having received these data determines parameters of the protected connection (in fact, makes the choice of the best algorithm). After that it sends to the client the certificate with an open key. The client ciphers the casual sequence of data an open key and sends it on the server. The server decodes the sequence, and, in case of lack of mistakes and failures, there is an establishment of the protected connection [5].

The protocol applies asymmetric enciphering. It means that only the party possessing the closed key can decipher the data ciphered by an open key. In this case such part is the server.

Secure Real-time Transport Protocol — the protocol of transport level intended for enciphering, protection against substitution of data and preservation of the data integrity transferred by the RTP protocol. Codes of AES (Advanced Encryption Standard) are used. Application of the TLS protocol is necessary to protect process of a secure channel establishment of SRTP.

Asterisk allows to use these protocols at the expense of special modules, in particular, of the res_srtp.so module. This module has already built in some distribution kits (for example, AsteriskNOW) and has already been ready to use. In case Asterisk has been separately installed, it is necessary to receive this module and to rebuild Asterisk with this module.

For generation of certificates ast_tls_cert script is provided. First of all it is necessary to download a script, it is carried out by the wget http://svn.asterisk.org/svn/asterisk/branches/11/contrib/scripts/ast_tls_cert team. That allows to load a script from svn-storage of data Asterisk. It should be noted the script is loaded into that folder in which the entrance before command execution has been carried out.

After downloading of a script we pass to his use. From the folder where the script has been loaded, we start team. / ast_tls_cert — C 192.168.0.106-O kontora — d/etc/asterisk/keys. Certificates for the server with the address 192.168.0.106, the name of the kontora organization in directory/etc/asterisk/keys is being generated.

Further it is necessary to generate certificates for clients. We start command./ast_tls_cert — m client — with /etc/asterisk/keys/ca.crt — k/etc/asterisk/keys/ca.key — O kontora — d/etc/asterisk/keys — o 5002. We receive the key for the client 5002 generated for the certificate of ca.crt and a key of ca.key of the kontora organization.

In folder/etc/asterisk/keys there will be following files: asterisk.key, asterisk.csr, asterisk.crt, asterisk.pem, 5002.pem, 5002.key, 5002.csr, 5002.crt, ca.key, ca.crt, ca.cfg, tmp.cfg.

Further we configure the server. All changes are made to the sip.conf file. Section general:

[general] tlsenable=yes tlsbindaddr=0.0.0.0:5061 tlscertfile=/etc/asterisk/keys/asterisk.pem tlscafile=/etc/asterisk/keys/ca.crt tlscipher=ALL tlsclientmethod=tlsv1 tlsdontverifyserver=yes bindaddr=192.168.0.106 externaddr=192.168.0.106 videosupport=yes

Here we set TLS support, we set the address and port, files of the certificate and a key, we include enciphering and in addition we enter a number of teams for Asterisk.

It is possible to check TLS work the openssl s_client team — connect 127.0.0.1:5061. Has to be are provided withdrawal of team with enciphering parameters, the certificate, a key.

We set up clients: [5002] type=friend secret=12345 host=dynamic context=local disallow=all allow=ulaw allow=h264 transport=tls encryption=yes

Here we set use of TLS and enciphering (we include SRTP). The following stage is the control of clients. Clients have to support TLS and obligatory inclusion of SRTP. We consider the control of clients.

For control of the mobile client for Zoiper it is necessary to make basic settings of the client, to include SRTP (at the same time the program will request inclusion of the TLS protocol what it is necessary to agree with). Besides, the address of the server needs to be added with number of port 5061 (after the address through a colon). Screenshots of settings are presented in the Figure 2:

】 🗅 🔹 🐌 奈: 📶 30% 🕞 11:39 Encryption Settings	[고 화 (중:) 30% SIP учетная запись	11:38		ኛ 🛜 : " 30% 🗈 11:38
Enable ZRTP Выкл.	Caller ID		SIP учетная запись Имя учетной зан 5002	писи
Enable SRTP	Мелодия звонка Enable Presence Вылл. Включить при запуске Вкл Audio Codec Settings		Authentication Сервер 192.168.0.106.5061 Имя пользовате 5002 Пароль Орtional	рля
	Video Codec Settings Encryption Settings Number Rewriting		Authentication u Исходящее про Caller ID	
	Сохранить Отмени	ть	Сохранить	Отменить

Figure 2. The VoIP by Antisip settings for TLS and SRTP

After saving of settings the client program has to be registered on the server. The Blink settings also demand inclusion of TLS and obligatory enciphering. At first obligatory enciphering joins in the Media menu (Fig. 3):

Blink Preferences Accounts Accounts Audio Video Chait Screen Sharing	Loging Advanced
○ :g=5002@192168.0106 ⓒ 5002@192168.0106	Accurat Information Media Server Settings Reburk Advanced Addo Codecs Veloc Codecs G oppo grave G SM G Opto LBC C Code
	Reset Drag codecs to change their order Reset RTP Options Image: Second inband DTMF Image: Second and video Second and video Encryptom: SDEE mandatary • •

Figure 3. Turning on the enciphering in Blink

Next in menu «Server Settings» we enter adress of the server, port number and choice of the TLS transporation (Fig. 4):

SIP Proxy

	Always use my proxy for outgoing sessions				
Outbound Proxy:	192.168.0.108	Port:	5061 🌻	Transport:	TLS 🔻
Auth Username:	5002]			

Figure 4. Settings of the server

In the Network menu the choice of TLS is also made, and the way to the file of the client certificate (Fig. 5) registers in the Advanced menu on the line «Certificate File»:

TLS Settings			
Certificate File:	C:\Program Files (x86)\Blink\resources\tls\5002.pem	\odot	Browse
	Verify server		

Figure 5. Choice of certification

In the Advanced menu of the program (the previous settings were made in the menu of accounts) it is left included only in the TLS protocol with the necessary port and the certificate is chosen.

And now at implementation of a call the organization of the protected session by means of the TLS protocol is carried out, and data are ciphered by SRTP. The intercepted stream is represented as UDP (User Datagram Protocol) stream. Now instead of the Wireshark Window with the intercepted packages are presented in the figure 6. In this case Wireshark doesn't identify streams of RTP and can't analyse them, data are ciphered. Protection of the user data against malefactors has been carried out.

Support of TLS and SRTP is declared practically in all modern client applications of IP-telephony. For this reason the linking of these protocols is widely applied to a traffic protection of telephony. It is especially urgent in complex compound networks in which is more difficult to trace and prevent interception of data. These technologies ensure safety of information, at the same time their application doesn't demand introduction of new hardware and is carried out at the program level.

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) [3].

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 (Fig. 6).

- 18 e	Applications I	Places Syster	m 🅘 🍕					1	} € ,]	🛃 🛛 Fri A	pr 29, 6:	44 PM	root
R		Capt	uring fro	om eth0	[Wiresha	rk 1.8.10 (SVN	Rev Unknowr	n from unkr	10wn)]			_ 1	×
File	Edit View	Go Capture	Analyze	Statistics	Telephony	Tools Internals	Help						
	öl 🛛 🌢	t 🕅 📼	∆ ×	c d	#	e ⇒ ∓		¥ 0	0, 6				~
Filte	r:				:	C Expression	Clear Apply	Save					
No.	Time	Source		Des	tination	Protoco	l Length Info						^
	44 17.10639	838 192.168.	0.101	192.	168.0.10	B STUN	70 Bin	ding Indica	tion				
	45 17.11033	998:192.168.	0.108	192.	168.0.10	5 TLSv1.	2 931 App	lication Da	ta				
	46 17.11089	297:192.168.	0.108	192.	168.0.10	1 TLSv1.	2 548 App	lication Da	ta				
	47 17.15294	8714192.168.	0.101	192.	168.0.108	B TCP	66 5533	33 > sip-tl	s [ACK	[] Seq=2299	Ack=18	15 Win=5	45
	48 17.18336	493! 192.168.	0.105	192.	168.0.10	в тср	66 3835	56 > sip-tl	s [ACK	[] Seq=3241	Ack=24	16 Win=1	73
*	49 17.20003	624(192.168.	0.105	192.	168.0.10	B TLSv1.	2 593 App	lication Da	ta				
	50 17.20075	542(192.168.	0.105	192.	168.0.108	B STUN	70 Bind	ding Indica	tion				
	51 17.24048	332192.168.	0.108	192	168.0.10	5 ТСР	66 sip	-tls > 3835	6 [ACK	[] Seq=2416	Ack=37	68 Win=9	57
	52 17.32750	423°192.168.	0.101	192.	168.0.108	8 UDP	224 Sou	rce port: 4	0100	Destinatio	n port:	11254	
	53 17.32796	299!192.168.	0.101	192.	168.0.108	8 UDP	224 Sou	rce port: 4	0100	Destinatio	n port:	11254	
	54 17.32818	5844192.168.	0.108	192.	168.0.10	5 UDP	224 Sour	rce port: 1	1216	Destinatio	n port:	40100	
_	55 17 37830	1/10:102 168	A 1A2	107	168 0 10		224 Sour	rce nort. 1	1216	Dectinatio	n nort.	40100	
<													>
						aptured (1792 b							
						e6), Dst: Cadmu	-	•					
						2.168.0.101), Ds		.108 (192.1	168.0.1	108)			
			rc Port:	40100 (40	100), Dst	: Port: 11254 (1	1254)						
Da Da	ta (182 byte	s)											
0000		o aa 22 f0 7				'".y Y.K.	E.						\cap
0010		5 40 00 40 1	1 e6 c3	c0 a8 00	65 c0 a8	U@.@	.e						=
0020		1 2b f6 00 b		80 00 00		.l+(···;·						
0030	8c 70 45 48	3 21 d5 a3 d	5 c2 ac	ed ea 88	b4 60 19	.pEH!	`.						~
0030	8c 70 45 48	3 21 d5 a3 d	5 c2 ac	ed ea 88	b4 60 19		`.	efault					~

Figure 6. The traffic protected from interception

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 WiFi 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 (Local Area Network) are also developed.

References

1 *Назаров И*. Пропускная способность в IP-сетях: расчет и выбор сетевого оборудования // Системы безопасности. — 2013. — № 6(10) / [ЭР]. Режим доступа: http://compsovet.info/magazine/security_systems.

2 Гольдитейн Б.С., Пинчук А.В. и др. IP-телефония. — М.: Радио и коммуникация, 2001. — 336 с.

3 *Якубова М.З.* Разработка топологии сетевой атаки на основе пакета программ Wireshark // ПОИСК Междунар. науч. журн.-приложение РК. Сер. естеств. и техн. наук. — 2013 — № 2 (2) / [ЭР]. Режим доступа: http://www.aipet.kz/article/facultet/frts/ikt/15/9.pdf.

4 Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Коммуникационные сети. — СПб.: БХВ-Санкт-Петербург, 2010. — 400 с.

5 *Якубова М.З.* Разработка критериев и требований по информационной безопасности // ПОИСК Междунар. науч. журн.-приложение РК. Сер. естеств. и техн. наук. — 2013. — № 2(2) / [ЭР]. Режим доступа: http://szgmu.ru/upload/files/Документы%20кафедр/СБОРНИК ОЗИЗ 2013.pdf.

М.З. Якубова, В.П. Разинкин, Т.Г. Сериков, А.К. Муратова

«Asterisk» базасының негізінде IP-телефония жүйесін деректерді ұстап қалудан қорғау

Қазіргі уақытта дауыс жіберу технологиясының дамуының жаңа кезеңін, соның ішінде IP-телефонияның қарқынды қолданыс тапқандығын байқауға болады. Жыл сайын IP-телефонияға корпоративтік коммуникациялық инфрақұрылымның негізі ретінде сұраныс және қолданыс деңгейі өсіп келе жатуынан, оның қауіпсіздігін қамтамасыз ету туралы сұрақ туындайды. IP-телефонияның интернет желісіне тікелей кірісі болғандықтан, абоненттердің аутентификациясы абоненттік IP-мекенжайлар бойынша жүргізіледі. Мақалада телефонияның қауіпсіздігін «Asterisk» программасының негізінде клиенттердің деректерін жаулап алудан қамтамасыз ету амалын сипаттайды. Байланыс анализаторы ретінде «Wireshark» программалық өнім алынған. Программалық телефон және клиенттік база ретінде сынақ жүргізілген ноутбуктар, компьютерлер және гаджеттар алынған. Сынақтар жасалған кезде алынған нәтижелер бойынша желінің төзімділік талдауы жасалған. Рұқсатсыз байланыстан қорғану мақсатында ұсыныстар берілген. Желіні қорғауға арналған ең ұтымды шешім ұсынылды.

М.З. Якубова, В.П. Разинкин, Т.Г. Сериков, А.К. Муратова

Защита сетей IP-телефонии на базе Asterisk от перехвата данных

В настоящее время наблюдается новый виток развития технологий передачи голоса, а именно IP-телефония. Ввиду растущих уровней спроса и популярности IP-телефонии как основы построения корпоративной коммуникационной инфраструктуры возникает вопрос обеспечения максимального уровня ее безопасности. Подчеркнуто, поскольку сервер IP-телефонии имеет прямой выход в сеть интернет, то и аутентификация абонентов происходит по IP-адресам. В данной статье показано решение вопроса обеспечения безопасности телефонии на базе Asterisk от перехвата данных клиентов. В качестве сетевого анализатора используется программное обеспечение Wireshark, в качестве софтфонов и клиентской базы рассмотрены ноутбуки, компьютеры и гаджеты, на которых проходит испытание. По результатам проведенных работ произведен анализ уязвимости сети. Даны рекомендации о мерах защиты данных клиентов от несанкционированного доступа. Предложен наиболее оптимальный вариант защиты сети.

References

1 Nazarov I. Security systems, 2013, 6(10), http://compsovet.info/magazine/security_systems.

2 Goldstein B.C., Pinchuk A.V. et al. IP-telephony, Moscow: Radio i kommunikatsiya, 2001, 336 p.

3 Yakubova M.Z. POISK: International sci. magazine-application of RK, Ser. of natural and techn. sci., 2013, 2(2), http://www.aipet.kz/article/facultet/firts/ikt/15/9.pdf

 Goldstein B.S., Sokolov N.A., Yanovsky G.G. Communication networks, Saint Petersburg: BHV-St. Petersburg, 2010, 400 p.
 Yakubova M.Z. POISK: International sci. magazine-application of RK, Ser. of natural and techn. sci., 2013, 2, http://szgmu.ru/upload/files/Документы%20кафедр/СБОРНИК_ОЗИЗ_2013.pdf