Қызмет диаграммалары реактивті жүйелерді модельдеу кезінде өте пайдалы оқиғалармен басқарылатын объект тәртібін айқындайды [4].

Бұл мақалада Web-қосымшаны жасау құралдарына талдау жасалды. Сайттың құрылымы және графикалық интерфейсін жасап, web-қосымша беттерінің арасында байланыс жасалды.

Web-қосымша қолданушыға түсінікті қарапайым және ыңғайлы навигациялық жүйе қарастырылды. Жүйені құру үшін XAMPP сервері, MySQL 5.0.24 мәліметтер базасын басқару жүйесі, Apche 2.4, JavaScript скриптерді жасау тілі, CSS 3 стилдерді сипаттау тілі, PHP 5.0.4 программалау тілдері қолданылды [4].

Ecademy жүйесі әкімшілік және клиенттік бөліктен тұрады. Әкімшілік өзінің жұмысын атқару үшін логин, құпиясөзді қолданады. Әкімшілік бөлімінде жүйедегі ақпаратты қосу, өшіру, өзгерту мүмкіндігі және сайттың құрылымын қайта жасау мүмкіндігі бар. Онда алты модуль қарастырылған: пәндер, студентер, хабарламалар, тесттік, әкімшілер және құпиясөзі ауыстыру. Тесттік модульде әкімші студенттерге тестілеуден өтуге рұқсат беріп, олардың нәтижелерін көреді және де кездейсоқ тест құрастырып оны .pgf форматында сақтап көре алады.

Қолданылған әдебиеттер тізімі

1. 2017 жылдың 31 қаңтарындағы Елбасы Н.Ә.Назарбаевтың Қазақстан халықна Жолдауы.
2. http://strategy2050.kz. А.Исекешев: «Сандық Қазақстан-2020» бағдарламасы халық жағдайы сапасын көтереді.
3. Сағымбаева А.Е. Тестілеу программасына қойылатын талаптар. // Білім беруді компьютерлендіру: проблемалары мен перспективасы республикалық конф. Материалдары. - Алматы, 1998. -Б. 186-187.
4. Сағымбаева А.Е. Білімді тексерудің тестілік әдістемесі. // Информатика негіздері. №2. 2002. Б. 15-17.

ОӘЖ 004

VOIP ЖЕЛІЛЕРІНДЕГІ АҚПАРАТТЫҢ ЖОҒАЛУ ЖОЛДАРЫН ЗЕРТТЕУ

Хибырат Е.
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Нұр-Сұлтан қ., Қазақстан
Жетекшісі - К. М. Сагиндыков

Кіріспе.

VoIP-дағы қауіпсіздік мәселелері бірегей және көп жағдайда күрделі емес. Бұл мақала VoIP қауіпсіздігінің негізгі мәселелерін, соның ішінде VoIP-дың негізгі архитектурасын, қорғаныс тетіктерін және қазіргі шабуылдарды, сонымен қатар SPIT сияқты ықтимал шабуылдар туралы және олардың шешімдері туралы шолуды қамтамасыз етуге бағытталған.

Келесі талқылауды жеңілдету үшін біз VoIP желісінің негізгі архитектурасын қысқаша сипаттаймыз. VoIP инфрақұрылымын үш қабат түрінде сипаттауға болады: түпкі пайдаланушы жабдықтары, желілік компоненттер және дәстүрлі телефон желісіне шлюз (1-суретті қараңыз).

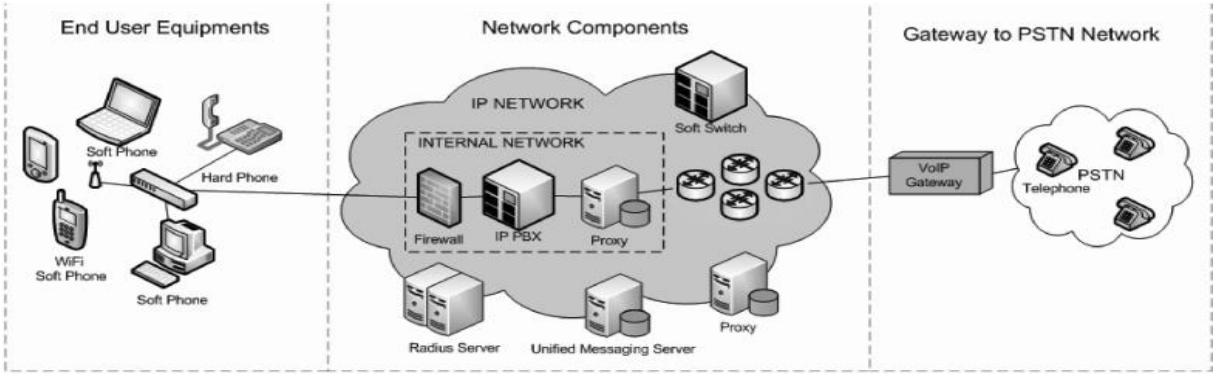
1. *Соңғы пайдаланушы жабдықтары:* соңғы пайдаланушы жабдықтары басқа қолданушылармен байланысу үшін пайдаланушыларға интерфейс ұсынады.

2. *Желілік компоненттер:* VoIP әдетте қолданыстағы IP желісін пайдаланады және осылайша оның осалдығын иеленеді. Желінің әрбір құрамдас бөлігінің соңғы бірнеше жыл ішінде пайда болған жеке қауіпсіздік мәселелері бар.

3. *VoIP шлюздері:* Шлюз IP желісін PSTN-мен интеграциялауда маңызды рөл атқарады, сондықтан оның қауіпсіздік саясатында осалдықтардың болмауын қамтамасыз ету қажет.

VoIP шлюзінің негізгі функциялары дауыстық жинақтау және сигналды басқару, қоңырауларды бағыттау және пакетизацияны қамтиды.

Бұл интерфейстерде әлсіздік болуы мүмкін, өйткені зиянкестер оларды тегін телефон қоңырауларын жасау үшін пайдалана алады. Кез келген қауіпсіздік жүйесі осы шабуылдарға тез және тиімді қарсы тұруға тиіс.



Сурет 1. VoIP желісі

VoIP хаттамалары

Телефонмен байланыс орнату үшін қоңырау шалу керек. Телефон қоңырауын дәстүрлі телефон жүйесінде орналастыру сандар тізбегін теруді қамтиды, содан кейін телефон компаниясы қоңырау соғылған адамға қоңырау шалу және қоңырауға жауап беру кезінде байланыс құру үшін өңделеді. VoIP көмегімен пайдаланушы қоңырау шалынатын нөмірге кіреді, ол телефон пернетақтасындағы нөмір немесе әмбебап ресурстық индикатор (URI) бола алады, содан кейін VoIP «сигнал беру протоколы» негізінде пакеттік алмасу реттілігі пайда болады. Шақырылған тарап жауап бергеннен кейін дауыстық сигнал цифрландырылады және «тасымалдау протоколы» негізінде тарату үшін пакеттер ағынына бөлінеді.

Signaling Protocols. Қазіргі кездегі VoIP жүйелері проприетарлық протоколды немесе екі стандарт H.323 және сеансты инициалдау протоколын (SIP) қолданады. SIP танымалдыққа ие болғанымен, осы хаттамалардың бірде-бірі нарықта әлі үстем бола қойған жоқ, сондықтан екі протоколды да түсіну маңызды.

H.323. H.323 - Халықаралық электробайланыс одағы - Телекоммуникацияны стандарттау секторы (ITU-T) ұсынған хаттамалардың жиынтығы және қоңырауды орнатуға, қоңырауды аяқтауға, тіркеуге, аутентификацияға және басқа да функцияларға қолданылатын протоколдар тобынан тұрады.

SIP. SIP - бұл интернет-инженерлік тапсырмалар тобы (IETF) біржақты немесе көп сессияларды құруға, өзгертуге және тоқтатуға арналған белгіленген протокол. SIP - бұл мәтінге негізделген хаттама және әр түрлі типтегі жүктемелерді әр түрлі кодтаумен тасымалдауға болады. SIP порт ретінде UDP және TCP қолдайды. SIP желісінің архитектурасы H.323 құрылымынан ерекшеленеді. SIP желісі соңғы нүктелерден, прокси-серверлерден, орналасу серверлерінен және тіркеуден тұрады.

Transport Protocols. VoIP орналастыруларының көпшілігі нақты медиа (мысалы, дауыстық немесе бейне) тасымалдау үшін RTP қолданады. Бұл UDP-ның жоғарғы жағында жұмыс істейтін қарапайым протокол, бірақ пакеттердің жеткізілуіне кепілдік бермейді, өйткені нақты уақыт режимінде ағындардың қасиеттері тасымалдау сенімділігіне қарағанда маңызды. Мультимедиа ағынының сапасы мен ақауларға төзімділігі нақты медиа-кодекпен анықталады, онда қателерді түзету алгоритмдері пакеттерді жоғалту арқылы туындаған мәселелерді шеше алады.

Құрылу механизмі.

VoIP-те қолданылатын негізгі протоколдар алдыңғы бөлімде сипатталған. Бұл бөлімнің негізгі бағыты VoIP протоколдарымен байланысқан қорғаныс механизмдерін, олардың күшті және әлсіз жақтарын талдауға арналған.

H.235. H.235 - H.323 негізіндегі жүйелер үшін таратылған байланыстарды қолдау үшін кілт алмасу протоколдарымен араласумен бірге түпнұсқалық растаманы, құпиялылықты және тұтастықты қамтамасыз ететін қауіпсіздік шеңбері. H.323 архитектурасы бойынша сигнал беру, басқару және медиа байланысының қауіпсіздік мәселелері үшін H.235 бірнеше хабарламалар, процедуралар, құрылымдар мен алгоритмдерді ұсынады

S/MIME. RFC 3851 Интернет-поштаның қауіпсіз/көп мақсатты кеңейтімдерін (S / MIME) анықтайды, олар SMTP және SIP сияқты қолданбалы протоколдарға құпиялылықты, бүтіндікті және аутентификацияны қамтамасыз етеді. S/MIME хабары MINE-ге негізделген, ол SMTP немесе басқа протоколдардағы мультимедиа мазмұны (мысалы, аудио, видео) және сыртқы таңбалар (мысалы, қытай, грек) сияқты күрделі хабарлама форматтарын кодтау мен ұсынудың механикалық жүйелерін анықтайды.

IPSec. Интернет протоколына арналған қауіпсіздік архитектурасы (IPSec) UDP немесе TCP көмегімен тасымалдайтын қосымшаларды қорғауды қамтамасыз етеді. IPSec соңғы нүктелер арасында қауіпсіз тоннельдер құру арқылы сигналдар мен медиа ағындарының құпиялылығына, тұтастығына және сәйкестігіне жауап береді.

Тасылмалдау қорғаныс механизмдері

Бұл бөлімде SRTP және SRTCP сияқты көліктік хаттамаларға қатысты қорғаныс механизмдері қарастырылған.

SRTP. Нақты уақыттағы қауіпсіз протокол (SRTP) - бұл RFC 3711 анықтаған RTP-ге арналған профиль медиа ағындардың хабарламалық жүктемесінің құпиялығын, тұтастығы мен аутентификациясын қамтамасыз етеді.

SRTP медиа мазмұн үшін құпиялылықты, бүтіндікті және аутентификацияны қамтамасыз ете алады, бірақ ол IP-желісінен PSTN-ге тасымалданатын медиа ағынының ақырғы және түпнұсқалығын қамтамасыз ете алмайды.

SRTCP. SRTCP хаттамасының формасы екі қосымша тақырыбымен SRTP-ге ұқсас: srtcp index және encrypt-flag аутентификация үшін. RTCP хабарламасында шығыс жағы және есептің мазмұны қорғауды қажет ететін құпия ақпарат болып табылады. Сондықтан бұл тақырыптар шифрланған.

Басқарудың негізгі механизмдері.

Кілттерді басқару VoIP сияқты мультимедиалық интернет қосымшаларын қорғаудың маңызды элементі болып табылады. Кілттерді келісу хаттамасы көп адресті және бір адресті байланыс үшін сенімді және кеңейтілген мүмкіндіктерді қамтамасыз ете алатын VoIP сияқты көп адресті коммуникациялар үшін қажет. Қазіргі уақытта бірнеше қолданыстағы және қалыптасқан негізгі басқару стандарттары бар. Бұл бөлім осы екі негізгі басқару хаттамаларына арналған.

MIKEY. Multimedia Internet KEYing - бұл нақты уақыт қолданбаларына арналған кілттерді басқару хаттамасы. MIKEY бір немесе бірнеше қауіпсіздік хаттамаларына арналған криптографиялық кілттер мен қауіпсіздік параметрлерінің келісуіне шыдайды. Ол сонымен қатар SIP және H.323 сияқты белгілі бір байланыс хаттамасының тәуелсіздігін қамтамасыз етеді. MIKEY-дің негізгі материалымен қосылудың екі жақты әдісі оны нақты уақыттағы мультимедиялық сценарийлер үшін қолайлы етеді.

ZRTP. ZRTP (Ziemmermann 2008) - қорғалған RTP қолдау үшін қолданылатын криптографиялық кілт туралы келісімнің тағы бір хаттамасы. Сигналдық маршруттың орнына RTP қолдануымен криптографиялық кілтті келісу ZRTP мен MIKEY арасындағы басты айырмашылық болып табылады, осылайша кілтті келісу негізгі компоненттерді бойлай беру үшін прокси SIP сияқты аралық терминалдарды тартусыз тікелей соңғы нүктелер арасында орындалады.

VOIP-ға шабуылдар және шешімдер.

Зиянкестер әдетте ең танымал және кең таралған жүйелер мен бағдарламаларға бағыттайды. Мұндай қосымшалардың бірі VoIP болды. Соңғы уақытта VoIP бірнеше әлсіз орындары анықталды, сондықтан хаттамаларды әзірлеушілер бұл проблеманы жаһандық ауқымда сәтті енгізбестен бұрын шешу қажет. Бұл бөлімде біз VoIP инфрақұрылымына

шабуылдарды зерттеуді ұсынамыз. Біз бұл шабуылдарды бес негізгі түрге жіктейміз, соның ішінде қызмет көрсетуден бас тарту (DoS), тыңдау, бүркемелеу, ақылы төлемдермен алаяқтық және интернет - телефония (SPIT) бойынша спам. Сонымен қатар, біз осы шабуылдарға қарсы тұру үшін қабылданған тәсілдерді талқылаймыз.

DOS. DoS-шабуылдар корпоративтік VoIP-жүйелер үшін ең үлкен қауіп төндіруі мүмкін. DoS-шабуылдар жүйенің функционалдығын немесе пайдаланушы құрылғылары, сигналдық компоненттер, медиа - компоненттер, басқару жүйелері, биллинг жүйелері және қауіпсіздік жүйелері сияқты тиісті компоненттің желілік мүмкіндіктерін бұзу үшін кез келген желілік элементке тікелей бағытталуы мүмкін.

DoS шабуылына арналған шешімдер. SIP, VoIP жүйелерінде DoS шабуылдарын басқаруға қарсы бірқатар шараларды ұсынды, соның ішінде:

• Мониторинг және сүзу - күмәнді пайдаланушылардың тізімдерін жүргізу және сол пайдаланушыларға сессияларды құрудан бас тарту.

• Аутентификация - хабарламаларды жібермес бұрын пайдаланушының жеке басын куәландыру.

• Апатридті прокси-сервер - жадтың таусылуы шабуылының (DoS) қаупін азайту үшін, азаматтығы жоқ прокси-сервері басқа қауіпсіздікті тексеруді, мысалы, пайдаланушылардың түпнұсқалығын растау, үшінші тұлғаларды тіркеу және спам көздерін тіркеу үшін пайдаланылуы мүмкін.

• Сервер дизайны (мысалы, процессор, жад және желі қосылымы) - DoS шабуылдарынан қорғанудың бірінші желісі. Sengar, Wijesekera, Jajodia (2008) сонымен қатар Hellinger қашықтығымен өлшенген трафик ағындарының қалыпты емес өзгеруіне негізделген статистикалық тәсілді қолдану арқылы DoS шабуылдарын анықтау әдісін ұсынды.

Eavesdropping. Eavesdropping - шабуылға дайындалу немесе байланысқа түсу үшін құпия ақпаратты жинау әрекеті. VoIP-те бұл болашақ шабуылдарға дайындалу үшін байланыстарды талдау үшін шабуылдаушы пайдаланушылар арасында алмасуды немесе медиа мазмұнын бақылай алатын сценарий.

Eavesdropping-ға арналған ұсынылған шешімдер. Eavesdropping болдырмау үшін төрт стратегия ұсынылады:

• мінсіз жабдықты пайдалану;

• монтаждау құралдарына қолжетімділікті тек уәкілетті қызметкерлер ғана шектеуі үшін қамтамасыз ету;

• кез-келген осал желі нүктесінде портқа негізделген MAC мекен-жай қауіпсіздігін енгізу; мысалы, қабылдау телефонында;

• жасанды режимде жұмыс істейтін құрылғылар үшін желіні үнемі қарап шығу процедурасын бастау.

Тағы бір шешім - бұл VoIP-трафикті шифрлау, бұл қауіпсіздіктің құлдырауын болдырмауға арналған жақсы әдіс; дегенмен, бұл қосымша шығындарды қосады.

Masquerading. Masquerading - бұл желіге, қызметке, желілік элементке немесе ақпаратқа қол жеткізу үшін пайдаланушы, құрылғы немесе қызмет үшін өзін қамтамасыз ету мүмкіндігі. VoIP қолдауын қамтамасыз ететін хаттамалармен манипуляциялау, сондай-ақ VoIP желілеріндегі бүркемелеу шабуыл ретінде іске асырылуы мүмкін.

Masquerading шабуылдар үшін ұсынылған шешімдер. Шифрлаумен біріктірілген аутентификацияның тиімді модулі маскарадинг және жалған шабуылдар үшін тиімді шешім болар еді.

Toll Fraud. Toll Fraud - бұл жеке немесе ақшалай пайда табу үшін VoIP қызметтеріне рұқсатсыз кіру мүмкіндігі. Телекоммуникация операторлары мен провайдерлері үшін бұл өте маңызды шабуылдардың бірі. Төлемді алаяқтықты сигналдық хабарламаларды немесе VoIP құрамдас бөліктерін, соның ішінде төлем жүйесін қоса конфигурациялау арқылы жүзеге асыруға болады.

Toll Fraud шабуылдары үшін ұсынылған шешімдер. VoIP провайдерлері желіаралық қалқанды дұрыс конфигурациялау және порттарды қорғау арқылы төлемдердің

алаяқтықтың алдын алады. VoIP провайдерлері желіге кімнің кіретінін, қандай жиілікпен және кімнің қандай траффик тудыратынын білуі үшін өз желілерін белсенді түрде бақылап отыруы керек.

SPIT. Байланыс шығындарының анағұрлым төмен болуына байланысты VoIP желісі қазіргі PSTN-ге балама ретінде және спамерлер үшін де тартымды бола бастады. VoIP-спам немесе Интернет-телекоммуникация бойынша спам деп аталатын SPIT, VoIP желілері үшін маңызды проблема болып табылады және нақты уақыт режимінде қорғаныс механизмін қажет ететін шабуыл сипатына байланысты электрондық поштаның спамынан да ауыр болады.

SPIT шабуылдары үшін ұсынылатын шешімдер. Қауіп жоқ болса да, SPIT -ке қарсы оның ықтимал қауіп-қатеріне байланысты көптеген шешімдер ұсынылуда. SPIT проблемасына шолу Rosenberg & Jenings (2007), Radermacher (2005), Niccolini(2006) және Baumann, Cavin, & Schmid бұл мәселені талдап, әртүрлі мүмкін шешімдерді талқылады. VoIP спамын анықтау және азайту мақсатында Jenings (2007) спам жасаушыларды (әсіресе DoS шабуылдаушыларын) ұстау үшін криптографиялық посттарды қолдануды ұсыну арқылы есепті қымбат тұратын кішігірім басқатырғышты шешуге байланыс орнатуға талпынған күдікті қоңырауды талап ету арқылы байланыс сұранысының құнын ұлғайту арқылы ұсынды. Бұл шешімнің жетіспеушілігі - жұмбақтың қиындықтары заңды қоңырау шалушының баяу машинасын басып озуы мүмкін, бұл қалаусыз кідірісті тудыруы мүмкін. Dantu және т.б. (2005) VoIP спам-сүзгісін ұсынды, ол қолданушы қоңырау қабылдауға дайын болған әлеуметтік желілерге негізделген беделге бейімделеді. Бұл тәсіл бірнеше түрлі домендердің жоғары бірлескен күш-жігерін қажет етеді және сүзгінің жоғары күрделілігі қосылуды қажетсіз кідіртуге әкелуі мүмкін. Hansen және т.б. (2006) қоңырау шалушының жеке басы және қоңырау шығу тегі сияқты қоңыраулардың мета-деректері негізінде қоңырауды бағалау арқылы беделі жүйесін қолданды.

Қорытынды.

VoIP IP желісінде мультимедиялық байланыстың негізгі технологиясына айналды. Сонымен қатар, Интернет ашық желі бола отырып, телефон қоңырауларына арналған географиялық шектеулерді жояды. Алайда, VoIP қолданыстағы IP желісін қолданады және осылайша оның осалдығын иелік етеді. VoIP-ға қатысты қауіпсіздік мәселелерін зерделеу үшін VoIP-дің негізгі архитектурасын және қолданыстағы қорғаныс механизмдерін, VoIP желілеріне қазіргі және ықтимал қауіптер мен шабуылдарды түсіну керек. Бұл мақалада біз VoIP-тің негізгі архитектурасын сипаттаймыз, ол соңғы пайдаланушы жабдықтарынан, желілік компоненттерден және шлюздерден, сонымен қатар PSTN-мен салыстырғанда түбегейлі айырмашылықтардан тұрады. VoIP жүйелерінде H.323 және SIP сияқты сигнал беру үшін және RTP және RTCP сияқты медиа-тасымалдау үшін қолданылатын протоколдар сипатталған. Қазіргі уақытта VoIP сигнализациясын (S / MIME, IPSec және H.235), медиа-тасымалдауды (SRTP және SRTCP) қорғауды және кілттерді басқаруды (MIKEY және ZRTP) қорғауға арналған қолданыстағы қорғаныс тетіктерін талқыладық. Ақырында, VoIP-тің қазіргі шабуылдары (мысалы, DoS, Eavesdropping, Masquerading) және олардың ықтимал шешімдері SPIT сияқты ықтимал VoIP шабуылдарын талқылау және ұсынылған шешімдерді зерттеу арқылы талқыланады. VoIP желілерін қауіпсіздендіру үшін бізде VoIP жүйелері және оның қол жетімді қауіпсіздік құралдары туралы негізгі білім болуы керек. Осылайша, бұл мақала VoIP-ті қолдану мен қауіпсіздігімен қызығушылығы бар оқырмандар үшін осындай білім мен пайдалы ақпарат береді деп үміттенемін.

Қолданылған әдебиеттер тізімі

1. Balasubramaniyan, V. A., Ahamad, M., & Park, H. (2007). CallRank: Combating SPIT using call duration, social networks, and global reputation, In Proceedings of the 4th Conference on Email and Anti-Spam, Mountain View, California, USA, August 2007.
2. Baugher, M., McGrew, Naslund, D., Carrara, E., & Norrman, K. (2004). The secure real-time transport protocol (SRTP). RFC 3711

3. Baumann, R., Cavin, S., & Schmid, S. (2006). Voice over IP – security and SPIT. Swiss Army FU Br 41, KryptDet Report, Zurich: University of Berne.
4. Sengar, H., Wijesekera, D., & Jajodia, S. (2008). Detecting VoIP floods using the Hellinger distance. IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 6, pp. 794–805.
5. Ziemmermann, P. (2008). ZRTP: Media path key agreement for secure RTP draft-zimmermann-avt-zrtp-06. IETF draft. Алынған http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-06
6. Thermos, P. & Takanen, A. (2008). Securing VoIP Networks. Pearson Education, Inc.

УДК 519.713

ОБ АЛГОРИТМАХ, ОПРЕДЕЛЯЮЩИХ ОБРАТИМЫЕ КОНЕЧНЫЕ АВТОМАТЫ С ПАМЯТЬЮ

Шахметова Гульмира Балтабаевна
sh_mira2004@mail.ru
Докторант 3 курса специальности «6D060200-Информатика»
Кафедра «Информатика и информационная безопасность»
Факультет «Информационные технологии»
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Ж.С.Сауханова

На сегодняшний день, информационные технологии являются неотъемлемой частью всех сфер жизнедеятельности общества, например, таких как, электронное правительство, банковские транзакции, связь, телевидение и многое другое, что ведет за собой крайне важную необходимость в эффективных средствах обеспечения защиты информации и данных. Такие средства относятся к криптографии, которая отвечает за конфиденциальность, проверку подлинности, целостности и неотрицания авторства [1]. Следует отметить, что рост использования компьютеров и мобильных устройств во всех аспектах жизни человечества, особенно в коммуникации, привел к возникновению новых форм криптографии. Одним из таких направлений является конечно-автоматная криптография.

Идея конечно-автоматной криптографии заключается в интегрировании теории автоматов в классическую криптографию [2]. В работах [3, 4] обсуждены основные моменты применения конечных автоматов в качестве криптографических алгоритмов и их компонент. Как известно в криптографии можно использовать как автоматы без выхода [5], так и автоматы с выходом. В данной статье будут рассмотрены конечные автоматы с памятью. Авторами была поставлена цель продемонстрировать потенциальную возможность использования данного вида конечных автоматов в криптографических системах.

Конечный автомат (КА) – это абстрактное математическое устройство, работающее в дискретном времени. В формальном виде КА представлен как пятерка $M = < X, Y, S, \delta, \lambda >$, где X $= \{x_1, x_2, \dots, x_n\}$ - конечное множество входных символов, $Y = \{y_1, y_2, \dots, y_m\}$ – конечное множество выходных символов, $S = \{s_1, s_2, \dots, s_l\}$ – конечное множество внутренних состояний, δ: $S \times X \rightarrow S$– функция переходов; λ: $S \times X \rightarrow Y$– функция выходов.

Для заданий автоматов удобнее всего использовать табличное представление (см. таб 1), где в строках записываются текущее состояние (ТС), в столбцах указываются входные символы, а на пересечении строки и столбца – следующее состояние (СС), и через запятую выходной символ.

Таблица 1. Таблица состояний КА

ТС	**СС,** y_m		
	x_1	…	x_n