ISSN 2226-6070
1 2
9 772226 607127

Ахмет Байтұрсынов атындағы
Қостанай мемлекеттік университеті

Костанайский государственный университет
имени Ахмета Байтурсынова

№ 4 2017 «3i: intellect, idea, innovation – интеллект, идея, инновация»

intellect, idea, innovation

3i

интеллект, идея, инновация

КӨПСАЛАЛЫ ҒЫЛЫМИ ЖУРНАЛЫ

МНОГОПРОФИЛЬНЫЙ НАУЧНЫЙ ЖУРНАЛ

№4 2017

ЧАСТЬ 2

Ахмет Байтұрсынов атындағы
Қостанай мемлекеттік университеті

КӨПСАЛАЛЫ ҒЫЛЫМИ ЖУРНАЛЫ

МНОГОПРОФИЛЬНЫЙ НАУЧНЫЙ ЖУРНАЛ

Желтоқсан (Декабрь)
№4 2017

МАЗМҰНЫ - СОДЕРЖАНИЕ

УДК 004.056.55

ЗАМАНАУИ ШИФРЛЕНГЕН ДЕРЕКТЕРДІ ЖІБЕРУ ЖҮЙЕЛЕРІ

Утемисова А.А. – ғылыми жетекшісі, А. Байтұрсынов атындағы Қостанай мемлекеттік университетінің педагогика ғылымдарының кандидаты, доцент.

Сагумбаева Ж.С. - А.Байтұрсынов атындағы Қостанай мемлекеттік университетінің магистранты.

Бұл мақала ақпараттарды жіберу кезінде кіруі қажететілмегендерден қорғаудың түрлерін ашады. Сізге қай әдіс қолайлы? Файлдарды интернет арқылы жіберу көп таралған, дегенмен көп кәсіпорындарға файлдардың қорғауда болуы, маңызды рөл атқарады. Файлдарды қорғау мен жіберудің бірнеше әдістері бар. Ол әдістердің қайсысын қолданып файлды жіберу мен шифрлайтынын әр ақпаратты жіберуші қажеттілігіне қарай өзі шешеді. Кейбір жағдайларда файлдарды тасымалдау кезінде қауіпсіздікті қамтамасыз ету жеткілікті. Басқаларда файлдарды алушыға жеткізгеннен кейін де қорғалған күйде етіп шифрлау маңызды. Бұл мақалада файлдарды қауіпсіз тасымалдау әдісі туралы ақпарат бар. Интернет арқылы қауіпсіздікті қамтамасыз ететін деректерді сақтауға арналған хаттамалардың мұрағаттық файлдарды жасаудың танымал әдістерін жасауы, файлдарды берудің оңтайлы түрін алуға мүмкіндік беретін негізгі деректерді шифрлау туралы айтылған. Файлдарды қауіпсіз сақтауға көмектеседі. Мақалада жазылғандарды мұқият зерттеп, жоғары қорғау деңгейімен кез келген жобаларды айтарлықтай іске асыруға болады. Сондай-ақ, мұнда негізгі арна пошталық серверді таңдау арқылы, көптеген негізгі функцияларды іске асыратыны туралы білуге болады және де қорғап қалуға болады.

Кілт сөздер: шифрлау, файлдарды қысу, файлдарды қорғау, заманауи жүйелер.

СОВРЕМЕННЫЕ СИСТЕМЫ ПЕРЕДАЧИ ЗАШИФРОВАННЫХ ДАННЫХ

Утемисова А.А. - научный руководитель, доцент, кандидат педагогических наук Костанайского государственного университета им. А. Байтурсынова, г.Костанай

Сагумбаева Ж.С. - магистрант Костанайского государственного университета им. А. Байтурсынова, г. Костанай

Данная статья раскрывает минимальный набор средств, обеспечивающих защиту данных при их передачи от несанкционированного доступа. Какой метод оптимален для ваших условий? Пересылка файлов по Internet - операция весьма распространенная, а защита передаваемых файлов имеет первостепенную важность для многих предприятий. Существует целый ряд способов передачи файлов и множество методов защиты этих файлов в процессе передачи. Выбор методов передачи и шифрования зависит от общих потребностей отправителя. В одних случаях достаточно просто обеспечить безопасность файлов в процессе передачи. В других важнее зашифровать файлы таким образом, чтобы они оставались защищенными и после доставки адресату. Данная статья подробно рассматривает способы безопасной передачи файлов. Описаны протоколы безопасной передачи данных по каналам Internet с приведением наиболее популярных методов создания архивов сжатых файлов, необходимости шифрования на основе данных об отправителе, позволяющей подобрать оптимальный способ передачи файлов.

Внимательно исследовав написанное в статье можно реализовать проекты с достаточно высоким уровнем защиты на любом из уровней. Здесь также можно узнать, что выбрав основным каналом почтовый сервер, реализуются большинство основополагающих функций.

Ключевые слова: шифрование, сжатие файлов, защита файлов, современные системы.

MODERN SYSTEM OF TRANSFERRING OF ENCHANTED DATA

Utemisova A.A. – Ph.D., Associate Professor, A.Baitursynov Kostanay state university.
Sagumbaeva Zh.S. – master student of A.Baitursynov Kostanay State University

This article discover the minimal set of tools that provide data protection while transferring from unsanctioned access. Which method is optimal for your conditions? File transferring over the Internet is very common, and the protection of transmitted files have paramount importance for many enterprises. There are a number of ways to transfer files and many methods to protect these files during the process of transferring. The choice of transmission methods and encryption depends on the overall needs of the sender. In some cases, it is quite simple to ensure the security of files during the transferring. In others, it is more important to encrypt the files in thereby that they remain protected after delivery to the recipient. This article details how to securely transfer files. Protocols for the safe transfer of data over the Internet channel are described with the reduction of the most popular methods for archives of compressed files, the necessity for encryption based on data of the sender, which allows you to choose the optimal method for file transferring.

Keywords: encryption, file compression, file protection, modern systems.

Егер сіздің ниеттеріңіз Интернетте таратылып жатқанда файлдарды қорғаумен шектелсе, қауіпсіз тасымалдау технологиясы қажет. Бір нұсқасы - оған жіберілген файлдарды ала алатын және мұндай файлдарды қауіпсіз жүктеу мүмкіндігін беретін веб-сайтты пайдалану. Файлдарды веб-сайтқа қауіпсіз тасымалдауды ұйымдастыру үшін ActiveX басқару элементін немесе Javascript сценарийін орналастыратын Secure Sockets Layer (SSL) бар веб-бетті жасауға болады. Мысалы, AspUpload басқару элементін Persitis бағдарламалық жасақтамасынан пайдалана аласыз; әзірлеушілер бұл «файлдарды орталық түйіндерге тасымалдау үшін нарық басқару құралдарында барынша жетілдірілген» деп бекітеді. Басқа нұсқасы - тегін ASP жүктеу сценарийін пайдалану, ол екілік құрамдас бөлікті пайдалануды қажет етпейді. Қосымша қорғауды қамтамасыз ету үшін сайтқа келген хостинг материалына веб-парақшаны және байланысты каталогты құпия сөзбен қорғауға болады. Веб-тораптан файлдарды жүктеуге келетін болсақ, тиісті веб-серверде, кем дегенде, файлдарды жүктеу үшін пайдаланылатын URL үшін SSL арқылы байланыс қамтамасыз етілгеніне көз жеткілікті.

Сонымен қатар, FTP қауіпсіз деректерді беруді қамтамасыз ететін FTP серверін пайдалануға болады. Шындығында, FTPS - қауіпсіз SSL қосылымы арқылы жұмыс істейтін FTP протоколы. FTPS протоколын пайдалану мүмкіндігі көптеген танымал FTP клиенттерінде берілген, бірақ, өкінішке орай, ол Microsoft корпорациясының FTP қызметінде іске асырылмайды. Сондықтан осы мүмкіндікті беретін FTP серверінің қолданысын (мысалы, танымал WFTPD өнімі) пайдалану қажет. FTPS-ді SSH файлды тасымалдау протоколымен шатастырмаңыз. SFTP - Secure Shell (SSH) қабығының үстінде жұмыс істейтін файлдарды тасымалдау протоколы; Сонымен қатар, ол файлдарды тасымалдау үшін пайдаланылуы мүмкін. Қорғалған терминал сервері (SSH Communications қауіпсіздік көзделген, мысалы, сервер) бірге, SFTP арнайы клиент (бұл клиент болуы мүмкін, PuTTY Telnet пакетінің бөлігі / қажет болады, сондықтан Алайда, біз, SFTP FTP дәстүрлі хаттама сыйыспайтын екенін есте ұстауымыз керек Secure Shell немесе графикалық интерфейсі бар WinSCP).

Сонымен қатар, файлдарды қауіпсіз тасымалдау виртуалды жеке VPN желілерінің негізінде ұйымдастырылуы мүмкін. Windows Server платформалары VRN технологиясымен RRAS арқылы үйлесімділікті қамтамасыз етеді. Дегенмен, бұл серіктестердің VPN шешімдерімен үйлесімділікке кепілдік бермейді. Мұндай үйлесімділік болмаса, ең көп пайдаланылатын шешімдердің бірін пайдалануға болады, мысалы Open Source-ашық-VPN. Ол тегін таратылады және Windows, Linux,

BSD және Macintosh OS X сияқты бірқатар платформаларда жұмыс істейді. OpenVPN интеграциясы туралы қосымша ақпарат алу үшін «OpenVPN-мен жұмыс істеу» бөлімін қараңыз.

VPN байланысын орнату арқылы каталогтарды бөліп, файлдарды екі бағытта да тасымалдауға болады. VPN трафигін кез-келген пайдалану арқылы шифрланған, сондықтан қосымша файлдарды шифрлауды қажет етпейді - файлдар қорғалған қалады және олар берілетін жүйеде қажет болған жағдайларды қоспағанда. Бұл принцип осы күнге дейін айтып өткенімнің барлық әдістеріне қолданылады.

Егер беру кезеңі сіздің қорқынышыңызды тудырмаса және сіздің негізгі мақсатыңыз файлдардың мазмұнына рұқсатсыз пайдаланушылардың қол жеткізуін болдырмау болса, онда файлдарды тасымалдау алдында ғана шифрлау ұсынылады. Бұл жағдайда электрондық пошта тиімді файлды беру арнасы болуы мүмкін. Электрондық поштаны өңдеу бағдарламалары іс жүзінде әрбір үстелдік жүйеде орнатылады, сондықтан егер файлдарды электрондық пошта арқылы жіберсеңіз, деректерді шифрлаудан басқа қосымша технологияларды пайдаланудың қажеті жоқ. Файлдарды электрондық пошта арқылы жіберу әдісі тиімді, себебі хабарлар мен тіркелген файлдар, әдетте, алушының пошта жәшігіне тікелей келеді, алайда жіберу кезінде бірнеше серверлерден өтуі мүмкін.

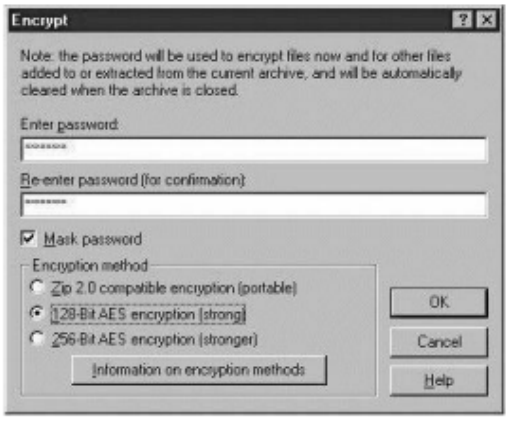
Егер электрондық пошта арқылы жіберу кезінде қосымша деректерді қорғау қажет болса, SMTP Secure (SMTPS) және POP3 Secure (POP3S) протоколдарын қолданыңыз. Шын мәнінде, SMTPS және POP3S әдеттегі SMTP және POP3 хаттамалары болып табылады, олар қауіпсіз SSL қосылымы арқылы орындалады. Microsoft Exchange Server, электрондық пошта клиенттерінің көпшілігі сияқты Microsoft Outlook, SMTPS және POP3S протоколдарын пайдалануға мүмкіндік береді. SMTPS протоколы пошта клиенті мен пошта сервері арасында файлдарды алмасу үшін пайдаланылған жағдайларда да, пошта сервері поштаны қалыпты қорғалмаған SMTP қосылымы арқылы соңғы орынға жеткізу мүмкіндігін сақтайтынын есте ұстаған жөн.

Электрондық поштаны өңдеу құралдары соншалықты кең таралғандықтан, осы мақалада ең алдымен файлдарды электрондық пошта арналары арқылы қауіпсіз тасымалдау туралы мәселелер талқыланады. Бұл ретте, жіберуші деректерді жеткізу кезеңінде де, жеткізілімнен кейін де оларды қорғау үшін деректерді шифрлау қажет екендігін ескереміз. Мысалы, электрондық пошта хабарларын шифрлаудың ең танымал технологияларын қарастырайық.

Файлды қысу құралдары

Бір мұрағат файлына файлдарды қысудың көптеген құралдары бар және ұсынылған көптеген шешімдер мұрағат мазмұнын қорғау үшін шифрлаудың кейбір түрлерін пайдалануды қамтиды. Әдетте, құпия сөз қысу процесінде орнатылады және мұрағатты ашқысы келетін кез-келген адам мұны тек осы құпия сөз арқылы жасай алады.

Сығылған файлдарды жасаудың ең танымал әдістерінің бірі zip-қысу әдісі болып табылады; барлық архивтер оны қолдайды. Бүгінгі күні zip қысудың ең көп таралған құралының бірі - WinZip қосымшасы. Ол қарапайым кіру үшін Windows Explorer-ге біріктірілген, сондай-ақ, осы өнімді Outlook клиентімен біріктіру үшін Outlook бағдарламасына арналған WinZip Companion бағдарламасын пайдалану арқылы жеке бағдарлама ретінде пайдаланылуы мүмкін. WinZip, көптеген zip-жабдықталған мұрағатшылар сияқты, Zip 2.0 шифрлау әдісін пайдалану арқылы шифрлау мүмкіндігін ұсынады. Бірақ бұл әдіспен файлдарды қорғау жеткіліксіз деп айтуға тиіспін. Енді WinZip 128 биттік немесе 256-бит шифрлау кілттерін қолданатын Advanced Encryption Standard (AES) спецификациясын қолдайды. AES салыстырмалы жаңа технология болып табылады, бірақ ол қазірдің өзінде салалық стандарт деп саналады.



1 Экран. WinZip AES спецификациясына қолдау көрсетеді

Көптеген архиваторлар AES көмегімен тұрақты шифрлау алгоритмдерін пайдалануын қамтамасыз ете алмайтындығын айта алмаймын, және мен осындай қосымшаны еске салу үшін өзімді шектеймін, бұл BAxBEx Software bxAutoZip әзірлеген өнім. Ол BAxBEx CryptoMite шифрлау бағдарламасымен өзара әрекеттесе алады және Outlook бағдарламасына біріктірілуі мүмкін. Егер WinZip деректерді шифрлауды Zip 2.0 және AES арқылы ғана пайдалануға мүмкіндік беретін болса, CryptoMite басқа танымал Twofish және Blowfish алгоритмдері, Cast 256, Gost, Mars және SCOP сияқты басқа шифрлау құралдарын қолдануға мүмкіндік береді.

ZIP-файлдарды шығару арқылы дерлік барлық компьютерлік жүйелер жабдықталған, бірақ zip-қосымшалары шифрлаудың әртүрлі алгоритмдерімен үйлесімділікті қамтамасыз етпейді. Сондықтан, шифрланған файлдарды жібермес бұрын, таңдалған алгоритмді «қабылдайды», «алушы» zip бағдарламасының «түсінеді».

Zip-негізделген қолданбаларды пайдаланып файлдарды шифрлау кезінде, құпия сөздер қорғалған. Мұрағат файлын шифрлау үшін алушы тиісті құпия сөзді де қолдануы керек. Құпия сөзді жеткізу әдісін таңдаған кезде қамқорлық қажет. Құпия сөзді жеткізудің ең қауіпсіз әдісі - телефон, факс немесе курьер. Сіз олардың кез-келгенін таңдай аласыз, бірақ ешбір жағдайда парольді электрондық пошта арқылы қарапайым мәтінмен жіберуге болмайды; Бұл жағдайда шифрланған файлға қол жеткізу рұқсатсыз пайдаланушымен алынатын қауіпті айтарлықтай арттырады.

Шифрлау құралдарымен жабдықталған мұрағатшылар файлдарды тек электрондық пошта арқылы ғана беруді ұмытпаңыз. Олар деректерді тасымалдау үшін және жоғарыда аталған басқа әдістер үшін тиімді пайдаланылуы мүмкін.

Pretty Good Privacy

PGP шифрлау кілттерін - ашық кілтті және құпия кілтті генерациялауды қамтитын ашық кілтті шифрлау жүйесін пайдаланады. Бұл екі перне математикалық түрде өзара байланысты, себебі ашық кілтпен шифрланған деректер тек жеке кілт арқылы шифрлануы мүмкін. PGP пайдаланушысы ашық құпия кілт жұпын жасайды, содан кейін ашық кілтті ашық кілт каталогында немесе веб-сайтында жариялайды. Құпия кілт, әрине, еш жерде жарияланбайды және құпия болып табылады; оны тек иесі ғана пайдаланады. Деректерді жасырын құпия сөз арқылы шифрлау кезінде пароль қажет, бірақ деректерді жалпыға қолжетімді кілтпен шифрлау кезінде, бұл барлық көрсетілмейді, себебі барлық пайдаланушылар жалпы кілттерді пайдалана алады.

PGP жүйесін пайдаланудың қарапайымдылығы үшін оның әзірлеушілері жалпыға қолжетімді кілт каталогтарын автоматты түрде сұрау функциясын жүзеге асырды. Бұл функция пайдаланушының электрондық пошта мекенжайын іздеу жолына енгізу арқылы оның ашық кілтін табуға мүмкіндік береді. PGP файлдарға негізделген арнайы «кілттерді» жүйеде өздерінің қол жетімділігін жеңілдету үшін жергілікті сақталатын ашық кілттерді автоматты түрде оқуға мүмкіндік береді. Ашық кілттер каталогын сұрау арқылы, PGP әрқашан ең соңғы нұсқаларын «түйінге» сақтап қоюға мүмкіндік береді. Пайдаланушы ашық кілтті өзгертсе, сізге қажет кез келген уақытта жаңартылған кілтке кіруге болады.

Ашық кілттердің шынайылығына сенімді болу үшін сіз басқа пайдаланушылар кілттерімен сандық қолтаңбаларды пайдалана аласыз. Басқа пайдаланушының кілтіне қол қою кілт шын мәнінде кілттің иесі деп аталатын адамға тиесілі екенін қосымша растау ретінде қызмет етеді. Кілтті электрондық цифрлық қолтаңбамен куәландыру үшін, PGP математикалық операцияны орындайды және оның ерекше нәтижесін қосады. Содан кейін қолтаңбаны жасау үшін пайдаланылған қолтаңба кілтімен салыстыру арқылы растауға болады. Бұл процесс адамның басқа біреудің жеке басын растайтын процесіне ұқсас.

PGP жүйесі көптеген адамдарға сенім артады, себебі ол ұзақ уақыт бойы ақпаратты қорғау үшін сенімді технология үшін салада беделге ие болды. Бірақ бәрібір, PGP немесе жалпыға қолжетімді кілттерді пайдалана отырып, деректерді шифрлаудың басқа әдісін қолдануға шешім қабылдасаңыз, файлдарыңыздың алушыларына сәйкес келетін шифрлау жүйесі болуы керек. PGP жүйесінің артықшылықтарының бірі электронды поштаны деректер байланысы ретінде пайдаланғанда оның өз шифрлау моделін, сондай-ақ X.509 және S / MIME технологияларын қолдайтынын білдіреді.

Сонымен қатар, тағы бір тармақты атап өту керек. Сіз PGP, WinZip немесе басқа шифрлау жүйесін пайдалануды жоспарлап отырсыз ба, қарамастан, егер сіз мазмұнның мазмұнын шифрлауды қоса, тіркелген файлдарды шифрлауды қаласаңыз, сіз оны жеке файлға жазуға және оны шифрлауға тура келеді. Қажет болса, бұл файлды басқа файлдармен бірге немесе мұрағатқа қосымша файл ретінде қоса орналастыруға болады.

Жіберуші деректеріне негізделген шифрлау

Вольтаж қауіпсіздігі жеке сәйкестендірілген шифрлау (IBE) негізінде жаңа технологияларды шифрлады. Жалпы айтқанда, ол PKI технологиясымен ұқсас, бірақ қызықты сипатқа ие. IBE-ге хабарламаларды шифрдан шығару үшін жеке кілт пайдаланылады, бірақ шифрлау процесінде ашық кілт қолданылмайды. Осындай негізгі IBE жіберушінің пошта мекенжайын пайдалануды қамтамасыз етеді. Осылайша, алушыға шифрланған хабарламаны жібергенде, оның кілтін алу мәселесі пайда болмайды. Бұл адамның электрондық пошта мекенжайын алу жеткілікті.

IBE технологиясы негізгі сервердегі алушының құпия кілтін сақтауды қамтиды. Алушы негізгі серверге кіру құқығын растайды және хабардың мазмұнын шифрлайтын құпия кілт алады. IBE технологиясын Outlook, Outlook Express, Lotus Notes, Pocket PC, сонымен қатар Research in Motion (RIM) BlackBerry пайдаланушылары пайдалана алады. Voltage Security өкілдерінің айтуынша, IBE кез-келген браузерге негізделген пошта жүйелерінде де кез-келген операциялық жүйе арқылы орындалады. Кернеу қауіпсіздігі сияқты әмбебап шешімдер - сізге қажет нәрсе.

Барлық жағдайларды ескере отырып

Интернеттегі файлдарды қауіпсіз түрде берудің көптеген жолдары бар және, сөзсіз, олардың ең қарапайым және ең тиімдісі электрондық пошта арқылы қамтамасыз етіледі. Әрине, үлкен көлемдегі деректерді құрайтын көптеген файлдарды айырбастауға тура келетіндер басқа әдістерді қолдануды қарастыра алады.

Сізге қанша файлды тасымалдайтындығыңыз, олардың көлемі қаншалықты үлкен екенін, осы файлдарды қаншалықты жиі беруіңіз керектігі, оларға қолжетімді болуы және оларды қалай алуға болатындығы туралы мұқият қарауыңыз керек. Осы факторларды ескере отырып, файлдарды тасымалдаудың ең жақсы әдісін таңдауға болады.

Егер сіз электрондық поштаның ең жақсы нұсқасы электрондық поштаның көптеген пошта серверлеріне және электрондық пошта клиенттеріне келгенде, сценарийлерді іске қосуға немесе ережелерге негізделген белгілі бір әрекеттерді орындауға болатындығын есте сақтаңыз. Осы функциялардың көмегімен пошталық серверлерде және файлдар пошта жәшігіне келген кезде маршруттағы файлдардың қозғалысын автоматтандыруға болады.

Әдебиеттер тізімі:

1. Водолазский В. Коммерческие системы шифрования: основные алгоритмы и их реализация. Часть 1. - 1999. –М.:2005. – 336 с.
2. Игнатенко Ю.И. Как сделать так, чтобы?.. // Мир ПК. – 1994. – 289 с.
3. Мафтик С.А. Механизмы защиты в сетях ЭВМ. - М.: Мир, 1993. – 158 с.
4. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь, 1992. – 215 с.
5. Гринберг А. Магический трюк MIT: вычисление по зашифрованным базам данных без их расшифровки. // MIT, 2011. – с. 5-9.
6. Арасу А., Эгуро К., Рамамути Р., Каушик Р. Запрос зашифрованных данных // Microsoft Research 2014. – с.10-17.
7. А. Болдырева, Н. Ченет, А. О'Нил. Запоминающее шифрование заказов: улучшенный анализ безопасности и альтернативные решения // Достижения в криптологии - CRYPTO 2011, – с. 18-19.
8. Р. А. Попа, С. М. Редфилд, Н. Зельдович, Х. Балакришнан PCryptDB: обработка запросов в зашифрованной базе данных // MIT CSAIL, 2012. – с. 28-33.
9. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; – М.: Радио и связь, 2001. – 376 с.
10. Шифрование данных [Электронный ресурс]. – Режим доступа: http://digest.subscribe.ru/inet/protection/n94412309.html

References:

1. Vodolazsky V. Commercial encryption systems: the main algorithms and their implementation. Part 1. // Monitor. – M.:2005. - N 6-7. – 336 p.
2. Ignatenko Yu.I. How to make it so that?// PC World. - 1994. - N 83. – 289 p.
3. Maftik S. Mechanisms of protection in computer networks. – M.: Mir, 1993. – 158 p.
4. Spesivtsev AV, Wegner VA, Krutyakov A.Yu. Protection of information in personal computers. - M .: Radio and Communication, 1992. – 215 p.
5. Greenberg A. An MIT Magic Trick: Computing On Encrypted Databases Without Ever Decrypting Them. // MIT, 2011. – p. 5-9.
6. Arasu A., Eguro K., Ramamuthy R., Kaushik R. Querying Encrypted Data // Microsoft Research 2014. – p. 10-17.
7. A. Boldyreva, N. Chenette, A. O'Neil Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions // Advances in Cryptology - CRYPTO 2011,– p 18-19.
8. R. A. Popa, C. M. S. Redfield, N. Zeldovic, H. Balakrishnan PCryptDB: Processing Queries on an Encrypted Database // MIT CSAIL, 2012. – p. 28-33.
9. Romanets Yu. V. Information protection in computer systems and networks / Yu. V. Romanets, PA Timofeev, VF Shanguin; - Moscow: Radio and Communication, 2001. - 376 p.
10. Encryption of data [Electronic resource]. - Access mode: http://digest.subscribe.ru/inet/protection/n94412309.html