РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2018

электронды күнделік жүргізу, электронды баға журналы және сабаққа келу, білім берудегі қызықты бағдарламалар, онлайн тестілеу мүмкіндіктері бар интерактивті порталдар болып табылады. Ақпараттық технологиялардың дамуына байланысты онлайн тестілеуден бастап қашықтықтық оқытуға дейінгі жаңа көптеген мүмкіндіктерге жол ашылды. Еліміздің көптеген мектептері өз сайттары мен қазақстандық домендік атау мен хостингтерге ие болды.

Бүгінгі күні білім беру саласында көптеген өзгерістер енгізіліп, материалдардың жаңартылуы, жаңа білім жүйесіне көшу реформалары қарқынды жүріп жатыр. Бұл үлкен өзгерістер алдындағы қорқынышты жеңуге тұрақты түрде олимпиада және конкурстарға қатысып білім деңгейін тексеріп отыру арқылы жеңуге болады. Оқушылар туындап жататын әр түрлі жағдайларға бейімделуді үйренеді. Оған қоса олимпиадаларға қатысу оқушы портфолиосына да жақсы әсер етеді.

Қолданылған әдебиеттер тізімі

1. Алматы облысының Білім берудегі ақпараттық технологиялар орталығы, http://aocit.kz/indicators/cat-1/3/
2. Киреева Е. П. Польза предметных олимпиад. – Научно-методический журнал «Концепт», 2017
3. Старова Т. С., Могилев А. В. Типология образовательных веб-сайтов
4. Бородовский Г. А, Извозчиков В. А – Новые технологии обучения: вопросы терминологии – 1993.

ӘОЖ 00326

БІЛІМ БЕРУ ҰЙЫМДАРЫНДА ЭЛЕКТРОНДЫ АҚПАРАТ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ

Мақшатова Раида
makshatova.raida@mail.ru
Л.Н.Гумилев атындағы ЕҰУ, Ақпараттық технологиялар факультеті,
4 курс студенті, Астана, Қазақстан
Ғылыми жетекші – Н.Т.Шындалиев, п.ғ.к. доцент

Ақпарат сөзі күнделікті өмірден бастап техникалық салада қолданылып келе жатқан көп мағына беретін ұғым болып табылады. Латын тілінен аударғанда «informatio» сөзі-түсіндіру,мазмұндау деген мағынаны білдіреді. Жалпы алғанда, бұл ұғым шектеу, байланыс, бақылау, форма, иинструкция, білім, мағына,бейнелеу, сезіну түсініктерімен тығыз байланысты болып келеді. Ақпарат-адамнан ерте туған құбылыс. Табиғат өзінің даму барысында жұмбақталған ақпаратты өсімдіктер мен тірі ағзалар арқылы беріп оытрған. Қазіргі уақытта бұл «Білім дәуірі» немесе «Ақпарат заманы» деп аталып, «ақпараттық қоғам», «ақпараттық технологиялар» сияқты терминдер жиі айтылып жүр.Сонымен «ақпарат» деп- қоршаған орта мен онда болып жатқан әр түрлі құбылыстар туралы мәліметтер жиынын айтамыз.

Мәліметтердің автоматтандырылған жүйесін кеңінен пайдалану басталғанға дейін ақпараттардың қауіпсіздігіне ерекше түрде физикалық және әкімшілік шаралармен қол жеткізілді. Компьютерлердің пайда болуымен мәліметтердің файлдары мен бағдарламалық құралдарды қорғаудың автоматты құралдарын қолданудың қажеттілігі арта түсті. Ақпаратты тауар ретінде қарастыра отырып, тұтастай алғанда, ақпараттарға нұқсан келтіру материалдық шығындарға ұшыратады деп айтуға болады. Мысалы, бірегей өнім жасаудың технологиялық сырын ашу осыған ұқсас өнімнің пайда болуына әкеледі, бірақ оны өзге өндіруші өндіреді және соның салдарынан иесі нарықтың бір бөлігін жоғалтады. Осындай жағдайларда ақпаратты оған рұқсат етілмеген қатынаудан қорғауға маңызды орын берілуі тиіс.Ақпарат

қауіпсіздігін қамсыздандыру архитектурасын құруда ақпартты қорғау жүйесін жасау қадамы ең маңызды болып табылады. Бұл қадамда:

– ұйымдастырушылық-басқарушылық
– ұйымдастырушылық-техникалық
– программалық-ақпараттық
– технологиялық
– құқықтық және моральдық- этикалық сипаттағы түрлі іс-шаралардың ұйымдастыруын қарастырады[1].

Қорғаудың ұйымдастырушылық-басқарушылық құралдары, мәліметтерді өңдеу жүйесінің ақпараттық және есептеуіш ресурстары мен функционалдық процестерін қолдануды шектеуге, қызметкерлердің орындайтын әрекетін шектеуге бағытталады.Олардың мақсаты-қауіпсіздіктің бұзылу мүмкіндігін барынша қиындату не мүлдем болдырмау. Кең қолданылатын ұйымдастырушылық- басқарушылық құралдар ретінде мыналарды атауға болады:

– ЭЕМ және басқа да мәліметтерді өңдеу жүйелері орналасқан аумаққа енуге бақылауды орнату;
– Арнайы рұқсат қағаздарын даярлау және қолдану;
– Мәліметтерді өңдеумен және тасымалдауға тек тексерілген қызметкерлерді ғана жіберу;
– Құпия ақпарат сақталатын магниттік және басқа да ақпарат тасымалдаушылары мен тіркеу журналдарды арнайы орындарда сақтау;
– Мәліметтержі өңдеумен байланысатын орындарда тыңдаушы жасырын құралдардың орнатылуын болдырмау;
– Жасырын ақпаратқа негізделген құжаттардың қолданылуы мен жойылуын есепке алу;
– Ақпараттарды автономды қорғау құралдары ретінде , ақпаратты ашуға бақылау орнатылатын құралдарды қолдану.

«Ақпарат» терминімен қатар АЖ-ға жиі түрде «деректер» терминін пайдаланады. ҚР «Ақпараттандыру туралы» заңына сәйкес ақпараттық жүйелердегі (кітпханалардағы, мұрағаттардағы, қорлардағы, деректер банкіндегі және өзге ақпараттық жүйелердегі) жекелеген құжаттар мен құжаттардың жекелеген массивтері ақпараттық қорлар(ресурстар) болып түсіндіріледі.

АЖ ұғымы өте кең және ол:

– ЭЕМ бүкіл сыныптары мен тағайындауларын;
– Есептеу кешендері мен жүйелерін;
– Есептеу желілерін(жергілікті,өңірлік,ауқымды) қамтиды.

Ақпарат, АЖ-ны қоғау заты болып саналады. Электрондық және электрондық-механикалық құрылғылар,сондай-ақ машиналық тасымалдаушылар ақпараттық жүйеде ақпараттардың өмір сүруінің материалдық негізі болып саналады. Енгізу құрылғысының немесе деректерді беру жүйесінің (ДБЖ) көмегімен ақпарат АЖ-ге түседі. Жүйеде ақпарат әртүрлі деңгейлердегі есте сақтайтын құрылғыларда сақталады және процессорлармен түрлендіріледі, шығару құрылғыларының немесе деректерді беру жүйесінің көмегімен жүйеден шығарылады. Қағаз, магниттік таспалар, әртүрлі дискілер машиналықтасымалдауыштар ретінде қолданылады. Бұрын ақпараттардың машиналық тасымалдауыштары ретінде қағаз перфокарталары және перфотаспалар, магниттік барабандар және карталар пайдаланылған болатын. Ақпараттарды машиналық тасымалдауыштар типтерінің көпшілігі алалы-салмалы болып саналады, яғни құрылғыдан алынуы және құрылғыдан бөлек пайдаланылуы немесе сақталуы(таспалар,дискілер,қағаз) мүмкін. Осылай, АЖ-де ақпараттарды қорғау(ақпараттардың қауіпсіздігін қамтамасыз ету) үшін, құрылғыны (ішкі жүйелерді) және машиналық тасымалдаушыларды оған рұқсатсыз тиісуден қорғау қажет [2].

Ақпаратты түрлендіру арқылы қорғау мәселесімен криптология (kryptos-жасырын, logos- ғылым) айналысады.Криптология екі түрге бөлінеді: криптография және криптоталдау. Бұл бағыттар бір-біріне тікелей қарама-қарсы болып табылады. Криптография ақпаратты түрлендірудің математикалық әдіс-тәсілдерін іздеумен және оны зерттеумен айналысады.Криптоталдау шифрленген мәтінді кмпьютердің көмегінсіз бастапқы қалпына келтіру мүмкіндігін зерттейді. Ақпаратты қорғаудың криптографиялық әдістері- бұл ақпаратты шифрладың, кодтаудың немесе өзге түрлендірудің арнайы әдістері, соның нәтижесінде оның мазмұны кейбір арнайы ақпараттарды(кілтті) көрсетусіз қатынай алмайтынға айналады.

Криптограмма- арна бойынша беруге не кейбір таратушыға ақпаратты жазу үшін дайын хабарды жеке кодтау.

Криптограммалардағы кілт- бұл криптограмма бойынша бастапқы ақпаратты қалпына келтіруге болатынын біліп, кейбір параметрдің нақты құпия жай-күйін криптографиялық түрлендірулер алгоритмі.

Шифрлау,дешифрлау- бастапқы ақпаратты криптограммаға түрлендіру үдерісі және сәкесінше, керісінше, алгоритммен берілген криптографиялық түрлендіру.

Шифрлау, дешифрлау теңдеуі- бастапқы ақпараттан криптограмманың пайда болуын сипаттайтын арақатынас .

Криптосызба немесе криптографиялық алгоритм деп өзіндік шифрларыд, дешифрлеуді және өзге криптографиялық түрлендірулерді айтатын боламыз.

Криптографиялық хаттама- қандай да бір криптограммаларды пайдаланумен ақпарааттармен алмасу үдерісінде ақпараттық жүйелердің қызметтік элементтерінің жұмысын анықтайтын емантикалық және синтаксистік ережелер мен процедуралар жиынтығы.

Ақпаратты қорғау мақсатында орындалатын шифрлеудің тиімді болуы кілттің құпиялылығына және шифрдің криптотұрақтылығына тәуелді болады. Мәдіметтерді криптографиялық шифрлеу программалық түрде де, ақпараттық түрде де орындалуы мүмкін.Ақпараттық түрде орындалуы көп шығындылығымен ерекшеленеді, дегенмен оның қарапайымдылық, сенімділік және жоғары өнімділік секілді жетістіктері де бар. Ал программалық түрде орындалуы неғұрлым ыңғайлы әрі тиімді болып табылады. Жақсы шифр ақпараттың жіктелуі үшін оны пайдаланудың пайдалылығын анықтайтын бірқатар арнайы қасиеттерге ие болуы керек. Біріншіден, шифрлау және дешифрлауда қолданылатын жағдайларда шифр тез жеткілікті түрде орындалуы керек.Компьютермен пайдалануға арналған жақсы шифр қарындаш пен қағазды пайдалану арқылы шифрлауға жарамсыз болуы мүмкін. Екіншіден, шифр дешифрлауға төзімді болуы керек, яғни, тек шифрланған хабарламамен және шифр өзі белгілі болса да, ашық шифрді білу өте қиын болуы керек.

Алмастыру және қарапайым орын ауыстыру әдістерінде ұзындығы қысқа кілттер қолданылады, ал әдістің сенімділігі түрлендіру алгоритмінің күрделілігімен анықталады. Ал аддитивті әдістер үшін, керісінше, ұзын кілттер және қарапайым алгоритмдер қолданылады.Аталған криптографиялық түрлендіру әдістері симметриялық шифрлеу әдістеріне жатады,яғни шифрлеу үшін де дешифрлеу үшін де бір кілт, ал дешифрлеу үшін жабық кілт деп аталатын басқа кілт қолданылады.[3]

RSA ашық кілттік жүйесі

Бұл криптожүйені 1978 жылы Р.Л.Райвест, А.Шамир және Л.Адлеман деген үш математик ғалымдардың құрметіне RSA- деп аталған криптожүйе- өте кеңінен қолданылатын ашық кілтті криптожүйе болып табылады. Ол санды жай сандарға жіктеу негізінде хат алмасудың құпиялылығын қамтамасыз етеді.Ақпараттарды қорғау үшін криптографиялық жүйеде ең тиімді және жиі қолданылатын жүйелердің бірі болып саналады. Өте қарапайым және «ашық кілтті криптожүйенің» тамаша үлгісі болғандықтан қазіргі таңда бүкіл әлемде кеңінен таралған.Бұл криптожүйенің негізгі қиындығы- модулінің жай сандарға жіктелуі болып табылады. RSA криптожүйесі үлкен сандарды факторизациялау күрделілігіне негізделген жақсы криптоберіктілікпен ерекшеленеді. Бұл алгоритм

мәліметтерді шифрлеу режимінде және электронды сандық қолтаңба режимінде жұмыс істей алатын ең бірінші толыққанды алгоритм болып саналады. Ол ашық жүйелер үшін дүниежүзілік стандартқа айналды.Бұл алгоритм жеке криптографиялық өнімі ретінде, сонымен қатар қосымшаларға ендірілген құрал ретінде қолданылады [4].

Ақпаратты қорғау мәселесі бұрыннан көтеріліп келеді. Әрқайсысы білуі керек емес ақпарат әрқашан болған. Бұл мәліметтерді алған адамдар оны қорғаудың әртүрлі әдістеріне жүгінеді.Белгілі мысалдардан криптография, шифрлау сияқты әдістер.Қазіргі уақытта көптеген адамдардың өмірі мен тұрмысын компьютерлендіру көптеген компьютерлік ақпараттық өңдеу мен сақтаудың құпия және құпия ақпарат жүйелерін қамтиды.Ғаламдық ғаламторды кеңінен қолдану ақпараттың әлдеқайда осал болуына әкеледі.Бұған өңделген деректердің үнемі ұлғаюы, шектеулі орындардағы деректерді жинау және сақтау,ресурстарға, бағдарламаларға және деректерге қол жеткізе алатын пайдаланушылар шеңберін үнемі кеңейтуге, компьютер мен байланыс жүйелерінің аппараттық және бағдарламалық қамсыздандыруының жеткіліксіз деңгейіне және т.б. сияқты факторлар ықпал етеді. Осы фактілерді ескере отырып, ақпаратты жинау, сақтау,өңдеу және беру процесінде ақпаратты қорғау аса маңызды болып табылады.

Қолданылған әдебиеттер тізімі:

1. Қ.С.Аяжанов, А.С.Есенова. Ақпараттық қауіпсіздік және ақпаратты қорғау.- Алматы,2011.
2. А.У.Актаева, Р.С.Ниязова, А.Ә.Шәріпбай. Ақпараттық қауіпсіздік және қорғау.1-бөлім.-Алматы:Эверо,2015.
3. В.П.Мельников, А.И.Куприянов,А.Г.Схиртладзе.Защита информации.- Москва,2014.
4. Өтелбаев М,Зәуірбеков С,Адамов Ә. Ақпарат қорғау мен криптография негіздері(Оқу құралы).- Алматы,2012

ӘОЖ 004.051

ЖОҒАРЫ ЖЫЛДАМДЫҚТЫ ЕСЕПТЕУЛЕРДІҢ АППАРАТТЫҚ ПРОГРАММАЛЫҚ НЕГІЗДЕРІ ЖӘНЕ ОҚУ ПРОЦЕСІНДЕ ҚОЛДАНУ

Манақбаев Әділхан Ұлықбекұлы
Л.Н.Гумилев атындағы ЕҰУ, Ақпараттық технологиялар факультеті
Информатика кафедрасы магистранты, Астана, Қазақстан
Ғылыми жетекшісі – Серік Меруерт

Қазіргі таңдаңдағы көптеген заманауи микропроцессорлардың сәулеті өнімділікті жоғарылату үшін параллелдеу үрдісін қолданылады, себебі параллелдеудің бұл түрі программалардың барлық класстарында бар.

Суперкомпьютерлер қысқа уақыт мерзімінде үлкен көлемді ақпараттарды өңдеуге арналған күрделі мәселелерді шешуге арналған. Суперкомпьютерлердің пайда болуы мен қолданылуы ғылым мен білімнің, техниканың стратегиялық даму факторына жатады және дамыған мемлекеттердің алғашқы ондық приориттетті технологияларына жатады. Суперкомпьютерлердің көмегімен экономикалық және әлеуметтік жүйелерді модельдеуге, басқа да әр түрлі құбылыстарды болжауға болады. Микроэлектрониканың дамуы мен жоғары жылдамдықты есептеулерді құру бағыттары көп процессорлы есептеу жүйелері болып табылады.

Бүгінгі таңда операцияларды параллелдеудің суперскалярлы қағидасы ең көп тараған. Осы қағидаға сәйкес сәулеттерде программаны компиляциядан өткізгеннен кейін алынған тізбекті кодтар аппаратты түрде параллельденеді. Соның нәтижесінде аппаратура күрделі кодталған операцияларды қайта кодтайды, осы операциялар арасында байланыстарды талдайды, регистрлердің аттарын қайта өзгертеді, параллельді құрылғыларды операцияларды