Қазақстан Республикасы білім және ғылым министрлігі
Л.Н. Гумилев атындағы ЕҰУ
Студенттердің ғылыми қоғамы

Министерство образования и науки Республики Казахстан
ЕНУ им. Л.Н. Гумилева
Студенческое научное общество

«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2009»

ЖАС ҒАЛЫМДАРДЫҢ VI ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯСЫ

ЖАС ҒАЛЫМДАРДЫҢ ХАЛЫҚАРАЛЫҚ КОНФЕРЕНЦИЯСЫНЫҢ ЕҢБЕКТЕРІ
29-30 сәуір 2009 жыл.

VI МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ МОЛОДЫХ УЧЕНЫХ

«НАУКА И ОБРАЗОВАНИЕ – 2009»

ТРУДЫ МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ МОЛОДЫХ УЧЕНЫХ
29-30 апреля 2009 года.

Конференция посвящается 15-летию инициативы Президента Республики Казахстан Н.А. Назарбаева о создании Евразийского союза

I бөлім
часть I

АСТАНА – 2009

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н.ГУМИЛЕВ атындағы ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ им. Л.Н.ГУМИЛЕВА

ЖАС ҒАЛЫМДАРДЫҢ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯСЫ «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2009»

МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ МОЛОДЫХ УЧЕНЫХ «НАУКА И ОБРАЗОВАНИЕ - 2009»

ЖАС ҒАЛЫМДАРДЫҢ ХАЛЫҚАРАЛЫҚ КОНФЕРЕНЦИЯСЫНЫҢ ЕҢБЕКТЕРІ
29-30 сәуір 2009 жыл.

ТРУДЫ МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ МОЛОДЫХ УЧЕНЫХ
29-30 апреля 2009 года.

І БӨЛІМ
ЧАСТЬ І

Астана, 2009

ББК

Жалпы редакцияны басқарған з.ғ.д., профессор Б.Ж. Әбдірайымов
Под редакцией д.ю.н., профессора Б.Ж. Абдраимова

«Ғылым және білім - 2009» халықаралық жас ғалымдар конференциясының материалдар жинағы. – Астана, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2009. 1 бөлім, - 470 б.

Сборник материалов международной научной конференции молодых ученых «Наука и образование - 2009».– Астана, Евразийский национальный университет им. Л.Н. Гумилева, 2009. 1 часть, - 470 с.

Жинаққа студенттердің, магистранттардың, аспиранттардың және PhD докоранттардың жаратылыстану-техникалық және гуманитарлық салаларындағы өзекті мәселелері бойынша еңбектері енгізілген.

В сборник вошли материалы студентов, магистрантов, аспирантов и докторантов PhD по актуальным вопросам естественно-технических и гуманитарных наук.

ББК

ISBN

Жинақты баспаға шығару жұмысына қатысқандар:
В подготовке сборника к печати принимали участие:
Аджиханова А.(ФТФ), Аскарбекова А.(ФТФ), Байбосынова Л.(ИСФ), Жаксыгулова А.(ФТФ), Махашева А.(ФМИТ), Мухышбаева А.(ФТФ), Рахметова Г.(ФМИТ), Сырлыбаева Г.(ФТФ), Шалимова Н.(ФМО).

Тексты тезисов печатаются в авторской редакции
Тезис тексттері авторлық редакцияда баспаға шығарылады

Дорогие гости!
Уважаемые участники конференции!!

Я сердечно рад приветствовать всех участников международной научной конференции молодых ученых «Наука и образование-2009».

Проведение международной конференции молодых ученых, аспирантов, докторантов и студентов стало ежегодной традицией Евразийского национального университета им. Л.Н. Гумилева.

И в этом году число участников конференции (более 500 человек) еще раз показывает уровень нашего университета, как ведущего образовательного и научного центра новой столицы Казахстана.

Данная конференция молодых ученых посвящена 15-летию инициативы Президента Республики Казахстан Н.А. Назарбаева о создании Евразийского союза. И Евразийский университет, основанный в 1996 году, является логическим продолжением идеи евразийской интеграции, суть которой заключена в самом названии университета. Символично, что университету по инициативе Президента Н.А. Назарбаева было дано имя выдающегося ученого – евразийца Льва Николаевича Гумилева. В лекции «К экономике знаний через инновации и образование», которую Президент прочитал перед многотысячной студенческой аудиторией в Евразийском национальном университете имени Л.Н. Гумилева 26 мая 2006 г., в год десятилетия университета, говорится: «Не случайно Ваш университет называется Евразийским. Евразийская Идея как теория была рождена в прошлом веке. Но, уверен, что Евразийская Идея, как практика организации новой жизни, будет воплощена в этом веке. Евразийство – одна из главных идей XXI-го века. И вы это скоро поймёте и увидите. И духовной столицей, сердцем Евразии может стать Астана, а самым сокровенным центром этого сердца - наш Евразийский Университет в Астане». Этими словами, Президент Республики Казахстан, возложил на Евразийский университет историческую миссию, которая заключается в становлении и развитии университета как образовательного и исследовательского центра по подготовке высококвалифицированных кадров для государственной службы, образования и науки, которые внесут свой вклад в развитие и процветание Казахстана в новом веке. В этом и заключается основная стратегическая цель развития университета, лидирующие позиции которого ежегодно подтверждаются официальным рейтингом Министерства образования и науки Республики Казахстан.

Наше молодое и динамично развивающееся государство имеет все основания ожидать от нашей талантливой молодежи новых научных открытий во благо процветания нашей Родины, Республики Казахстан.

Желаю успехов и плодотворной работы конференции!

Б.Ж. Абдраимов
Ректор Евразийского национального университета имени Л.Н. Гумилева, доктор юридических наук, профессор

СЕКЦИЯ 1
ЕСТЕСТВЕННО-ТЕХНИЧЕСКИЕ НАУКИ

УДК 525.2: 681.3.06

КОМПЬЮТЕРНАЯ МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ЗЕМЛИ ОТ СТОЛКНОВЕНИЯ С КРУПНЫМИ КОСМИЧЕСКИМИ ТЕЛАМИ

А.У.Абиев
Студент ЕНУ им. Л.Н.Гумилева, Астана
Научный руководитель – А.Т.Канаев

Вследствие разных причин время от времени по направлению к Земле могут двигаться достаточно крупные небесные объекты. Столкновение их с Землей приведет к катастрофическим последствиям. В 1999 году на конференции ООН Международный астрономический союз представил систему оценки угрозы возможных столкновений Земли с астероидами и кометами. Туринская шкала позволяет классифицировать астероиды и другие небесные тела по 10 уровням степени их опасности. Шкала содержит только качественные критерии, количественная оценкой является Палермская шкала. В ней используется непрерывный индекс *PS* (от Pa1erto Sca1e).

$$PS = \lg \frac{P_1}{f \Delta t} \qquad (1)$$

где P_1 – вероятность столкновения в момент сближения объекта с Землей, Δt — время, оставшееся до вероятного столкновения, фоновая частота столкновения с объектами.

Один из вариантов решения проблемы – фрагментация опасного астероида мощной ударной волной. Для этого необходимо предварительно произвести запуск ракеты с мощным взрывчатым зарядом и направить к астероиду. Для этого мы разработали систему обеспечивающая защиту Земли от столкновения, которая состоит из трех подсистем:

1. **Система обнаружения и маниторинга крупных космических тел;**
2. **Система оповещения и запуска ракет;**
3. **Система выбора типа траектории наведения ракеты на движущиюся цель и расчет точки столкновения.**

Итак, астрономы обнаружили астероид, движущий к Земле. Его массы и размеры превышают критические. Расчеты показывают, что столкновение с Землей неизбежно. Астрономы передают данные об астероиде ракетным воискам, которые решают по какой траектории запустить ракету. А теперь это моделирует программа. Задачами данной программы являются:

1. **Моделирование опасной для Земли ситуации;**
2. **Расчет траектории астероида;**
3. **Расчет начальных условий для запуска ракеты;**
4. **Моделирование и визуализация всех процессов.**

При моделировании принимается, что астероид и ракета движутся в поле тяготения Земли. Гравитационные влияния других небесных тел не учитываются. Интегрирование движения ракеты и астероида осуществляется методом Эйлера.

Моделирование опасной для Земли ситуации. Программа, используя генератор случайных чисел, из разных точек, находящейся на расстоянии приблизительно 600 000 км, по направлению к Земле «пускает» астероид со случайной массой. Модуль скорости астероида и ее направление варьируются в определенных пределах.

Расчет начальных условий для запуска ракеты. Это наиболее трудная часть программы. Обнаружен опасный астероид. Уже просчитана его траектория. Задача – вывести

ракету на разгонную орбиту и придать ей такой импульс, чтобы в дальнейшем, двигаясь в поле тяжести Земли, она попала в астероид. В общем виде, это достаточно сложная задача. Но мы сделаем ряд упрощений. Во-первых, будем считать, время необходимое для вывода ракеты на разгонную орбиту мало по сравнению со временем, которое нужно, чтобы долететь ракете до астероида. Во-вторых, будем считать, что плоскости орбит астероида и ракеты совпадают. Траекторией тела, движущегося в поле гравитационной силы, является: парабола, гипербола.
и эллипс. Ракета, запущенная с Земли, может двигаться по одной из них. Это будет зависеть от полной энергии ракеты.

Запуск ракеты по параболической траектории. Если полная энергия ракеты равна нулю, то она будет двигаться по параболе. Полная энергия складывается из кинетической и потенциальной энергий. $E = \frac{mv^2}{2} - \frac{GMm}{r} = 0$ (3)

Из закона сохранения энергии можно определить скорость ракеты в точке 2: $v = \sqrt{\frac{2GM}{r}}$

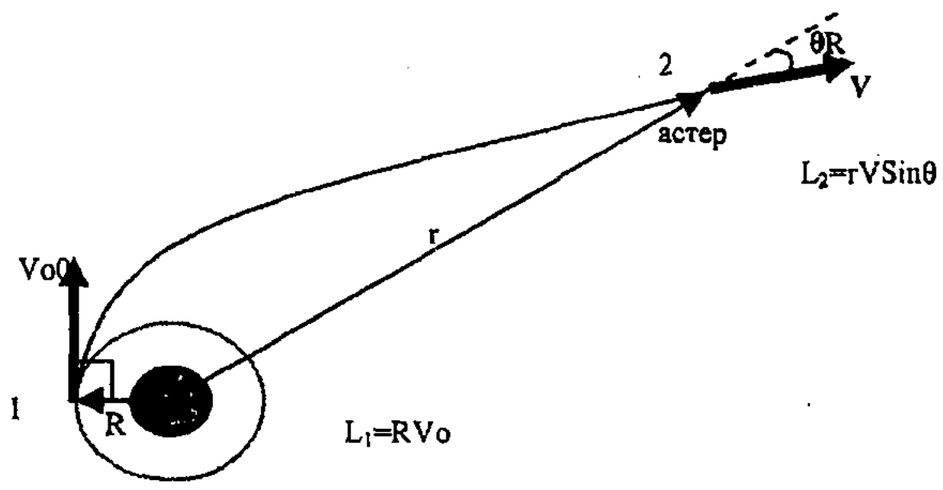


Рис. 2. Движение ракеты по параболической траектории.

Воспользуемся также законом сохранения момента импульса $L_0 = L$. Откуда

$$Rv_0 = rv\sin\theta, \tag{4}$$

где

$$v_0 = \sqrt{\frac{2GM}{R}}, \quad v = \sqrt{\frac{2GM}{r}}.$$

Из формулы (4) определим угол θ, а точнее синус и косинус этого угла. После несложных преобразований получим: $\sin\theta = \sqrt{\frac{R}{r}}$, $\cos\theta = \sqrt{\frac{r-R}{r}}$

Теперь, мы знаем с какой скоростью и в каком направлении запустить ракету из точки 2, чтобы она двигалась по параболе. Пусть x и y – координаты астероида. Тогда, пользуясь тригонометрическими формулами, нетрудно получить следующие выражения для составляющих скоростей ракеты.

$$v_x = \frac{v}{r}(x\cos\theta - y\sin\theta), \qquad v_y = \frac{v}{r}(x\sin\theta - y\cos\theta).$$

Запуск ракеты по гиперболической траектории. В этом случае полная механическая энергия ракеты будет больше нуля. Скорость ракеты определяется по формуле (5) :

$$v = \sqrt{\frac{2GM}{r} + \frac{2E}{m}}, \qquad \frac{2E}{m} = v_\infty^2, \tag{5}$$

где v_∞ – скорость ракеты на бесконечности. Синус и косинус угла θ определяются по формулам (6), (7):

$$\sin\theta = \frac{R}{r}\sqrt{\frac{\frac{GM}{R}+v_\infty^2}{\frac{GM}{r}+v_\infty^2}} \quad (6); \qquad \cos\theta = \sqrt{1-\sin^2\theta}\,. \quad (7)$$

Запуск ракеты по эллиптической траектории. Полная энергия ракеты меньше нуля, движение финитное и траектория представляет собой эллипс, большая полуось которого

$$a = \frac{p}{1+e^2}, \quad (8)$$

где p – параметр эллипса, а e – эксцентриситет, причем $p = \frac{v_0^2 R}{GM}$. Известно также, что

$$\frac{r}{R} = \frac{e+1}{e-1}$$

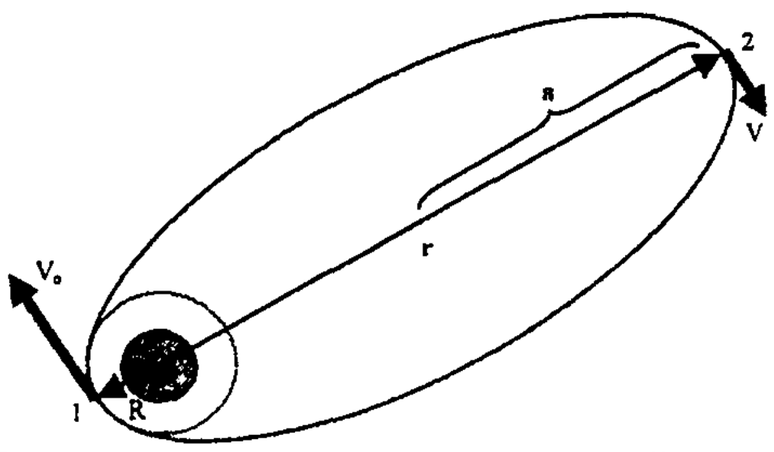


Рис. 3. Движение ракеты по эллиптической траектории.

Из рисунка 6 видно, что $2a = R + r$. Воспользовавшись законом сохранения момента импульса, получим $v = \sqrt{\frac{2GM}{r} * \frac{R}{r+R}}$

Если координаты астероида фиксированы, то можно численно рассчитать начальные условия для ракеты. Осталось учесть, что астероид постоянно движется и, следовательно, его координаты и скорость постоянно меняются.

Расчет точки столкновения. Для этого необходимо прогнозировать положение астероида. Точку столкновения можно определить из условия равенства времени полета ракеты от Земли до точки М и времени полета астероида от точки А до точки М. Положение точки столкновения можно по следующему алгоритму.

1. Фиксируются начальные координаты астероида

2. Находятся новые координаты астероида в следующий момент времени (через малый промежуток времени *dt*)

3. Рассчитывается время полета астероида от начального положения (т. А) до нового положения T_a

4. Рассчитывается время полета ракеты до нового положения астероида T_p

5. Если $T_a < T_p$, вернуться к пункту 2

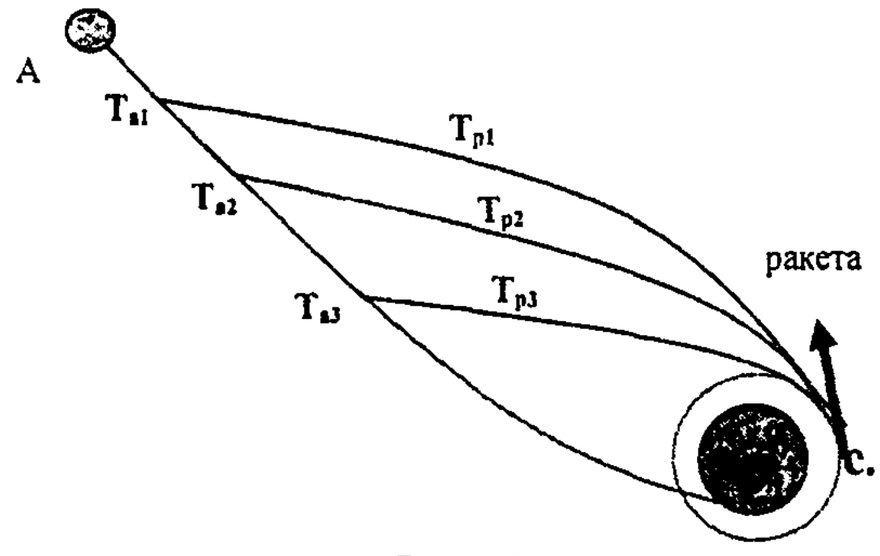


Рис4. Расчет момента запуска ракеты.

Во всех приведенных процедурах используется алгоритм Эйлера:
accelXr:=-GM*Xr/Rr/Rr/Rr; Vxr:=Vxr+accelXr*dt; Xr:=Xr+Vxr*dt; Rr:=sqrt(Xr*Xr+Yr*Yr);

accelYr:=-GM*Yr/Rr/Rr/Rr; Vyr:=Vyr+accelYr*dt; Yr:=Yr+Vyr*dt;

Таким образом, мы видим, что человечество достигло такого уровня развития науки и техники, что мы можем предотвратить столкновение Земли с крупными небесными телами.

Литература:

1. Е.Л. Кринов «Планеты карлики». Государственное издательство технико-теоретической литературы. Москва 1956 г
2. Гулд Х., Тобочник Я. Компьютерное моделирование в физике. Часть первая – М.: Мир, 1990. – 227 с.
3. Туркин О.В. Расчет движения небесных тел // Информатика. - № 18, 2002. – С. 27–30.

УДК51758

О СХОДИМОСТИ ДВОЙНЫХ РЯДОВ, СОСТАВЛЕННЫХ ИЗ КОЭФФИЦИЕНТОВ ФУРЬЕ-УОЛША ФУНКЦИИ ОГРАНИЧЕННОЙ S-ВАРИАЦИИ

Т.Б.Ахажанов, Е.Н.Бокаев
Докторанты ЕНУ им. Л.Н.Гумилева, Астана
Научный руководитель – Н.А. Бокаев

Пусть $S \in R_+.$, $[0.1]^2 = [0,1) \times [0,1)$. Пусть $\tau : 0 = x_0 < x_1 < x_2 < ... < x_n = 1$, $0 = y_0 < y_1 < y_2 < ... < y_n = 1$ произвольное разбиение отрезков $[0,1]$. Функция $f = f(x;y)$ называется ограниченной s-вариацией если

$$V_s = \sup_{\tau} \sum_{k=1}^{m} \sum_{l=1}^{m} \left| f(x_k, y_l) - f(x_{k-1}, y_l) - f(x_k, y_{l-1}) + f(x_{k-1}, y_{l-1}) \right|^s < \infty .$$

В этом случае будем писать, что $f \in BV_s(0,1)^2$

Говорят, что двойная последовательность $\gamma = \{\gamma_{mn} : (m,n) \in N_+^2\}$ принадлежит классу A_α при некотором $\alpha \geq 1$ когда имеет место неравенство:

$$\left(\sum_{m \in D_\mu} \sum_{n \in D_\gamma} \gamma_{mn}^{\alpha} \right)^{1/\alpha} \leq k 2^{(\mu+\gamma)(1-\alpha)/\alpha} \sum_{m \in D_{\mu-1}} \sum_{n \in D_{\gamma-1}} \gamma_{mn}$$

для всех $\mu, \gamma \geq 0$, где $D_\mu := \{2^{\mu-1}+1, 2^{\mu-1}+2, ..., 2^\mu\}, \mu \in N_+$

Через $\omega^{(2-s)r/2}(f; \frac{1}{m}; \frac{1}{n})$ будем обозначать модуль непрерывности функции f. Через $\hat{f}(m,n)$ обозначим коэффициенты Фурье-Уолша [1].

Теорема. *Пусть* $f \in C(0,1)^2 \cap BV_s(0,1)^2$ *и пусть* $\{\gamma_m\} \in A_{2/(2-r)}$ *для некоторого* $r \in (0,2)$. *Тогда выполняется неравенство:*

$$\left(\sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \gamma_{mn}^{\alpha} \left| \hat{f}(m,n) \right| \right)^r \leq k C V_s^{r/2}(f) \sum_{\mu=0}^{\infty} \sum_{\gamma=0}^{\infty} 2^{-(\mu+\gamma)r} \Gamma_{\mu-1,\gamma-1} \omega^{(2-s)r/2}(f; \frac{1}{m}; \frac{1}{n}),$$

где $\Gamma_{\mu\nu} := \sum_{m \in D_\mu} \sum_{n \in D_\nu} \gamma_{mn}$ *для* $\mu, \gamma \geq 1$

Следствие. *При условии теоремы имеет место неравенство*

$$\left(\sum_{m=D}^{\infty}\sum_{n=D}^{\infty}\gamma_{mn}\left|\hat{f}(m,n)\right|\right)^{r} \le kCV_s^{r/2}(f)\sum\sum(m,n)^{-r}\gamma_{mn}\omega^{(2-s)r/2}(f;\frac{1}{m};\frac{1}{n}).$$

Для случая тригонометрических рядов подобный результат получен в работе [2].

Литература:

[1] Б.И.Голубов, А.В.Ефимов, В.А.Скворцов, Ряды и преобразования Уолша: теория и применения, Москва «Наука», 1987 г.

[2] F. Moicz and A. Veres, On the absolute convergense of multiple Furier series, Acta Math. Hungar. 117(2007), 275-292.

УДК 681.3.05

АҚПАРАТ АЛМАСУ ХАТТАМАЛАРЫНДА ҚОЛДАНЫЛАТЫН КРИПТОГРАФИЯЛЫҚ ӘДІСТЕРДІҢ КЕЙБІРІН САЛЫСТЫРУ

Бейбітхан Е.

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің магистранты, Астана

Ғылыми жетекші: ШАРИПБАЕВ А.А., т.ғ.д. профессор

Ақпарат алмасу хаттамалары дегеніміз – барлық абоненттерге алдын–ала белгілі **реглементтік** тізбекті хабарламаны жіберумен сәйкес абонеттердің өзара әрекеттесуі. Хабарламаны өңдеу және дайындау үшін ақпарат алмасу хаттамаларының жол шеңберінде абоненттер деректерді өңдеудің әр түрлі криптографиялық технологияларын қолданады.

Қолданылатын алгоритмдердің екі типі бар: симметриялық және асимметриялық. Симметриялық деп бір ғана кілт қолданылатын алгоритмді айтады. Ашық кілтті алгоритмдерде әр түрлі кілттер қолданылады. Осы себепті әр түрлі процестерде әр түрлі кілттер қолданылады, ашық кілтті алгоритмді асимметриялық алгоритмдер деп атайды. Симметриялық алгоритмдерді қолданған жағдайда байланыс арнасының екі типі кездеседі. Оның бірі ашық, екіншісі қорғалған болады.

Әр абонент бастапқыда өзінде қос кілтті байланысқан *E* ашық кілтті және құпия *D* кілтін генерирлейді. Ашық кілттерді кейбір сенімді ***кілттерді бөлу орталығында*** жариялайды. Бұл орталық ақыры барлығына ашық кілттердің көшірмелерін береді. Шифрлеу алушының ашық E кілтінде жасалынады. Шифрленген құпиялы D кілтінде оқылады. Қастық ойлаушы адам желідегі әрбір екі абонент арқасында деректер жөнелту каналдарына, сондай-ақ абоненттер арасында және сенімді *кілттерді бөлу орталығында* ене алады. Сызбада құпиялы қорғаулы байланыс каналдары болмайды. *A* қолданушы *B* қолданушыға құпиялы хабар жіберсін. Хабарды шифрлегенде ашық кілтті криптографиялық жүйе қолданылады. *B* қолданушыда өзінің ашық E_n кілті және құпиялы D_n кілті бар. Ашық *EB* кілті барлық қолданушыларға белгілі және жарияланған, сонымен қатар *A* қолданушыға белгілі және ол E_n ашық кілтті хабарды шифрлеу үшін қолданады. *A* қолданушы шифрлеу алгоритмдерін қолданады. Оның негізінде кейбір *F* функциясының екі аргументтері: бастапқы хабар және алушының ашық кілті болады. Функцияның мәні *C* криптограммасы болып табылады. Оны қорғаусыз ашық байланыс каналдары арқылы жіберуге болады. *A* қолданушы $C=F(M, E_n)$ кодтау операциясын орындайды да, *B* қолданушыға криптограмманы жібереді. *B* қолданушы *C* криптограммасын алып, өзінің құпиялы кілті арқылы $M=F(C, D_n)$ дикодтауды орындайды. Нәтижесінде *B* қолданушы құпиялы хабардың бастапқы мәтінін алады.

Криптографиялық алгоритмнің негізінде жатқан сол бір *F* функциясы арқылы хабарды кодтауға және дикодтауға болады. Жалпы жағдайда әр түрлі функцияларды қолдануға болады.

Қазіргі заманның деректер кодтауы симметриялық криптографиялық алгоритмдер класына жатады. Нақтырақ айтқанда симметриялық блоктық итерациондық кодтау тобына жатады. Бұларға, мысалы, ГОСТ 28147-89, FIPS PUB 46-3 (DES), FIPS PUB 197 (AES) стандарттар жатады. Электронды цифрлы қол стандарты және кілттерді орналастыру ашық кілті криптографиялық алгоритмдер класына жатады. Тәжірибе жүзінде математикалық әдістің екі кластары таратушылық алды. Осы кластар арқылы қазіргі заманғы ашық кілтті криптографиялық жүйелер жасалынады. Бұларға Эль-Гамальдың электронды цифрлы қолдар алгоритмі және Диффи-Хеллманның протоколы жатады және қазіргі заманғы стандартты электронды цифрлы қолдар ГОСТ Р 34, 10-94 және ГОСТ Р 34, 10-2001, хэш алгоритмін қолданылуымен, американдық DSA және ECDSA алгоритмдермен және көптеген криптографиялық протоколдар арқылы ГОСТ Р 34, 11-94 жазылған.

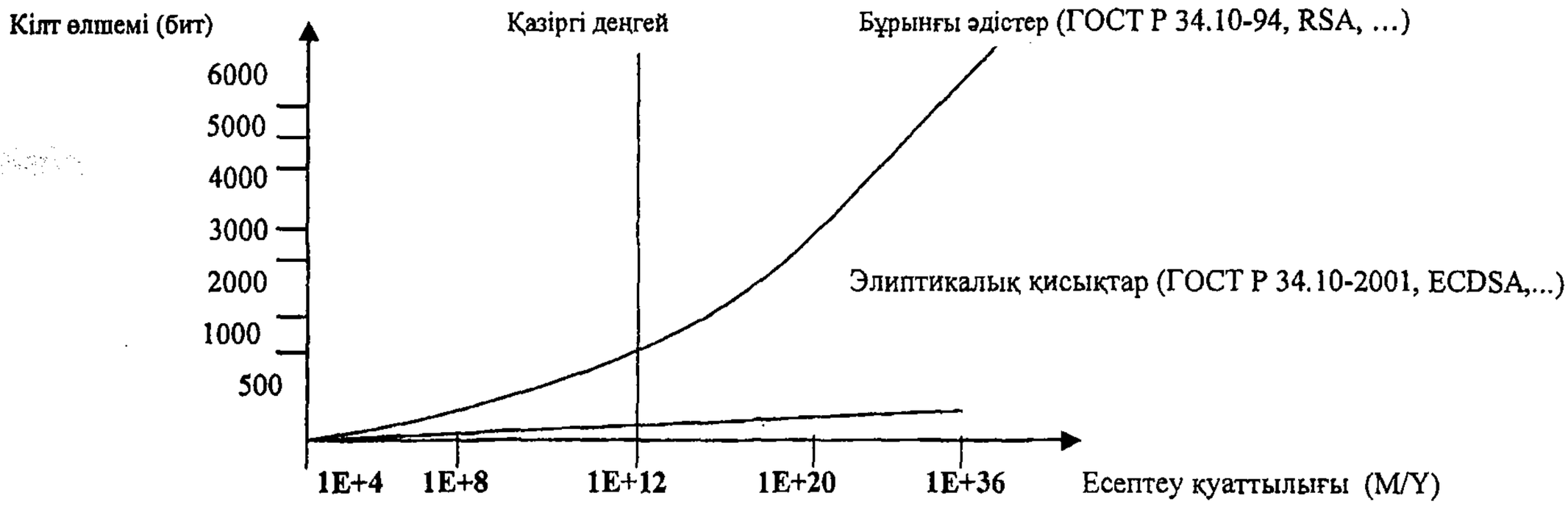
Шифрлеу алушының ***E*** кілтінде жасалынады. Шифрлеуді ашып алушының ***D*** кілтінде жүзеге асырылады.

Сурет-1. Криптографиялық алгоритмдер

Егер S жиынында коммутативтік, ассоциативтік, дистрибуттік, тұйық, бірлік және кері элементтері болатын қасиеттерді қанағаттандыратындай қосу, көбейту амалдары анықталған болса, онда S жиынын F өрісі деп атаймыз. Шекті элементі бар өріс **шекті өріс** деп аталады және жалпы жағдайда Fq деп белгіленеді. $q = p^r$, p – жай сан, ал r-бүтін оң сан. Егер r=1 болса, онда өріс қысқалығы Fp мәнін береді. Кей кезде мұндай өрістер Галуа өрістері деп те аталады және $GF(p)$ деп белгіленеді. Есептеу p модулі бойынша модульдік алгебра ережесімен жүзеге асырылады, яғни есептің нәтижесі $[0, p-1]$

интервалында жатады деп есептейміз. Егер p – жай сан болса, онда бұдан шығатыны, кез келген $\alpha \in (0, p-1]$ элементі үшін мультипликатты кері элемент болып табылады. Мұндай элементтердің жиындары [1] мультипликатты топтар құрайды. Қазіргі кездегі ақпарат алмасу хаттамаларында қолданылатын асимметриялы криптографиялық алгоритмдердің көпшілік басым бөлігі экспоненттеу амалдарын қолданады.

Кейбір алгоритмдерде, мысалы, Эль-Гамальдің электронды-цифрлі қолтаңбасының сызбаларында, ГОСТ Р 34.10- 94 стандарттарында, DSA және басқаларда құпия кілт қолтаңбасында [2, 3] модулі бойынша дәрежеге көтеру нәтижесі ретінде қабылданады. Басқа алгоритмдердің, мысалы, RSA сызбасында модуль бойынша r дәрежесіне көтеру нәтижесінің шығуы хабарламаны шифрлеу және дешифрлеу процедураларында қолданылады [4]. Алғашқы жарыққа шыққан Диффи-Хеллманның экспоненттті кілт алмасу асимметриялық алгоритмі жалпы құпия мәнді генерациялау үшін осы амалдарды қолданған еді. $b = a^n \bmod p$ экспоненттеу операциясының кең таралуы шекті өрісте дискреттік логарифмдеу есептері деген атқа ие болған операциясы есепті кері шығару күрделігімен байланысты [6]. a, b және p мәндері белгілі болатын болса, онда n мәнін есептеуі күрделі мәселені шешу есебі болып табылады [7]. Эллиптикалық қисық криптожүйесі бұрын шыққан криптожүйелермен салыстыра отырып кіші мәнді сандарды қолдану кезіндегі беріктілік деңгейін қамтамасыз етеді, ал беріктілік шекті өрістегі дискреттік логарифмде немесе есептің факторлық күрделілігінде қортындыланады. 2-суретте есептеу қуаттылығының өсуіне тәуелді беріктіктің адекваттық деңгейін қамтамасыз ету үшін қолданылған сандар мөлшерінің өсуі салыстырмалы графикте келтірілген.



Сурет-2. Бұрынғы және элиптикалық әдістерді салыстыру

MIPS/YEAR - де келтірілген қуат көрсетілген, яғни M/Y - элиптикалық қисықты криптография қолданылған жағдайда секундына бір миллион операцияны орындайтын компьютердің шыққан жылы. Салыстыру үшін элиптикалық қисықтарда криптографияны қолдану кезінде 160 бит мөлшерлі сандарды, тең алгоритмдерді қолдану кезінде 1024 бит қатардағы сандармен салыстырғандағы эквивалентті тіреуіш деңгеймен қамтамасыз етеді. Келтірілген графиктен көрініп тұрғандай элиптік қисықтарға криптографияларды қолдануға көшу жақын болашақта көрнекті жетістіктер беретіні көрініп тұр.

Әдебиет

1. Акритас А. Основы компьтерной алгебры с приложениями. М.: Мир, 1994.
2. Зима В., Молдовян А., Молдовян Н .Безопасность глобольных сетевых технологий. СПб ;BHV Санкт- Петербург ; 2002
3. Иванов М .А Криптографичские методы защиты информации в компьютерных системах в сетях. М: КУДИЦ – ОБРАЗ, 2001

4. Коутинхо С .Введение в теорию чисел . Алгоритм RSA , Постмаркет, 2001

5. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информаций. Функция хэширования
6. Гошков С.Б., Чубариков В.Н. Арифметика. Алгоритмы. Сложность вычислений. –М.: Наука, 1984
7. Верещагия П.К., Шен А. Лекция по математической логики и теория алгоримтов Часть 2. Языки и исчисления.-М.: МЦИМО, 2002

УДК 338.2:658.1

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ МЕНЕДЖМЕНТА ПРЕДПРИЯТИЯ НА ОСНОВЕ МАТРИЧНОЙ СТРУКТУРЫ УПРАВЛЕНИЯ

Н.А. Грицова
Студентка им. Л.Н.Гумилева, Астана
Научный руководитель – А.Т. Какимова

Важнейшим вопросом, подлежащим рассмотрению при создании любых систем менеджмента, является организационное структурирование деятельности предприятия. Организационная структура должна отвечать конкретным потребностям каждого предприятия, с учетом условий и целей деятельности, имеющихся в его распоряжении трудовых, материальных и финансовых ресурсов, а также требований предъявляемых предприятию всеми заинтересованными сторонами.

Система менеджмента предприятия традиционно строится на основе функциональной модели, предполагающей выделение и группировку различных видов управленческого труда с последующим формированием специализированных подразделений. Функциональная структура в сочетании с линейной образует структуру управления предприятием.

Основными недостатками эффективной реализации стандартов ИСО 9000 на предприятиях являются:

- ✓ система менеджмента предприятия и СМК строятся на различных принципах;
- ✓ при отсутствии механизма взаимоувязывания систем большинство предприятий не справляется с проблемой интеграции СМК в систему менеджмента предприятия;
- ✓ отсутствует согласованное функционирование СМК с действующей системой управления предприятием;
- ✓ отсутствие возможности реализации на практике в полном объеме процессного подхода к организации производства и менеджмент качества.

Как наладить гармоничное сочетание линейно-функционального и процессного управления, их взаимную интеграцию? Современная практика показывает, что реальным механизмом решения этой задачи является применение матричной структуры управления предприятием.

Для обеспечения рационального разделения и кооперации труда в сфере управления предприятием реализуется функциональный подход, сущность которого состоит в выделении совокупности функций управления как обособленных видов управленческого труда. Их типовой состав включает: перспективное и текущее технико-экономическое планирование, организацию финансовой деятельности, разработку и постановку продукции на производство, организацию работ по стандартизации, материально-техническое обеспечение, организацию производства (основного, обеспечивающего), организацию метрологического

обеспечения, технический контроль и испытания, сбыт продукции, учет и отчетность, управление организацией труда и заработной платы, организацию работы с кадрами, экономический и финансовый анализ. Для осуществления названных функций на постоянной основе формируются функциональные подразделения (например, в области проектирования, планирования, финансовой деятельности, стандартизации, снабжения и т.д.). Для обеспечения единства руководства предприятием и его подразделениями, согласованности действий руководителей и специалистов реализуется линейный подход к управлению. В каждое подразделение назначается руководитель, который подчиняется вышестоящему руководителю [2].

Матричная структура предусматривает также программно-целевой подход для повышения целенаправленности управления предприятием, ориентации его на конкретные конечные результаты. Целевые программы могут быть как временными, так и постоянными. Для каждой такой программы назначается руководитель, разрабатывается специальная организация деятельности руководителей и специалистов функциональных подразделений в интересах достижения поставленных целей [2].

Матричная структура представляет собой тип структуры управления, построенный на принципе двойного подчинения исполнителей: с одной стороны – непосредственному руководителю функциональной службы, которая предоставляет персонал и техническую помощь, с другой – руководителю целевой программы, который наделен необходимыми полномочиями для осуществления процесса управления в соответствии с запланированными сроками, ресурсами и качеством (рис.1).

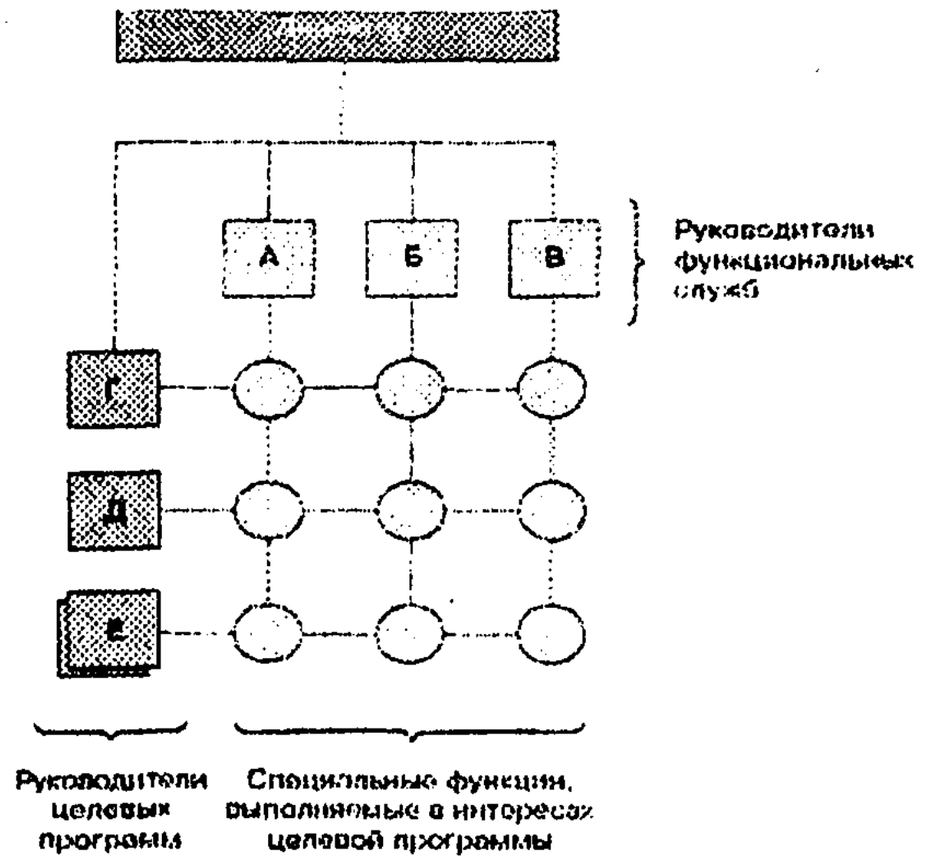


Рис. 1 Принципиальная схема матричной структуры

Руководитель целевой программы взаимодействует с двумя группами подчиненных: с постоянными членами проектной группы и работниками функциональных отделов, которые подчиняются ему в ограниченном круге вопросов.

Ключевым элементом матричной структуры являются специальные функции целевой программы, представляющие собой регулярно повторяющиеся действия линейных руководителей и специалистов функциональных подразделений для достижения целей программы. Образуются они путем «привязки» функции управления к целям программы. Например, если речь идет о функции планирования деятельности предприятия, то специальная функция применительно к менеджменту качества может быть сформулирована как «планирование достижения целей в области качества». В общем случае при определении специальных функций целевой программы необходимо исходить из того, что они в

совокупности должны предусматривать реализацию типовых элементов управленческого цикла (планирование, организация, контроль, учет, регулирование и анализ).

Таким образом, последовательность действий при интеграции СМК в систему менеджмента предприятия включает определение состава специальных функций СМК, обеспечивающих достижение поставленных целей, и их закрепление за линейными руководителями и функциональными службами предприятия. Соответствующие изменения вносятся в регламент их деятельности и должностные инструкции специалистов [2].

Интеграция СМК в систему менеджмента предприятия на базе матричной структуры может быть применена в условиях уже заданной структуры требований стандартов ИСО серии 9000. Ожидается, что это позволит повысить результативность создаваемых систем менеджмента качества. Вместе с тем на практике действия, связанные с интерпретацией требований этих стандартов в состав задач линейно-функциональной структуры, предоставляют определенную сложность, в том числе методическую, и не всегда могут привести к желаемому результату.

Перспективным решением является стандартизация системы менеджмента предприятия в целом с акцентом на качество. Это позволит в полной мере реализовать потенциальные возможности матричной структуры управления в организации взаимодействия линейных руководителей, руководителей и специалистов функциональных подразделений и руководителей целевых программ.

При практическом применении на конкретном предприятии модель должна быть адаптирована под реально существующие на нем функциональные структуры или состав управленческого персонала, идентифицированные объекты управления и значимые для предприятия группы заинтересованных сторон.

Проанализировав все факты, можно выделить несколько преимуществ данной системы:

- ✓ интеграция различных видов деятельности компании в рамках реализуемых проектов, программ;
- ✓ получение высококачественных результатов по большому количеству проектов, программ, продуктов;
- ✓ вовлечение руководителей всех уровней и специалистов в сферу активной творческой деятельности по реализации организационных проектов;
- ✓ сокращение нагрузки на руководителей высшего уровня управления путем передачи полномочий принятия решений на средний уровень при сохранении единства координации и контроля за ключевыми решениями на высшем уровне;
- ✓ усиление личной ответственности конкретного руководителя как за проект (программу) в целом, так и за его элементы;

Несмотря на перечисленные выше достоинства анализируемого вида структур управления, следует подчеркнуть и некоторые недостатки системы:

- ✓ сложность матричной структуры для практической реализации;
- ✓ структура сложна, громоздка и дорога не только во внедрении, но и в эксплуатации;
- ✓ в связи с системой двойного подчинения подрывается принцип единоначалия, что часто приводит к конфликтам;
- ✓ при использовании матричной структуры возникают трудности с перспективным использованием специалистов в данной компании;
- ✓ структура считается абсолютно неэффективной в кризисные периоды.

Но, тем не менее, наличие детально проработанной структуры должно облегчить руководителям и специалистам задачу грамотного позиционирования в рамках общей системы управления предприятием всех элементов систем менеджмента на основе международных стандартов и способствовать их результативности в достижении всех поставленных предприятием целей.

Литература

1. Версан В.Г. Стандарты ИСО серии 9000: закономерности развития // Стандарты и качество. – 2008. - № 1. – С.56-59.
2. Версан В.Г. Менеджмент качества // Стандарты и качество. – 2008. - № 5. – С.56-59.

УДК 681.3.05

БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

Д.С. Галиев
Магистрант ЕНУ им. Л.Н. Гумилева, Астана

Кто владеет информацией,
тот владеет ситуацией.
Народная мудрость.

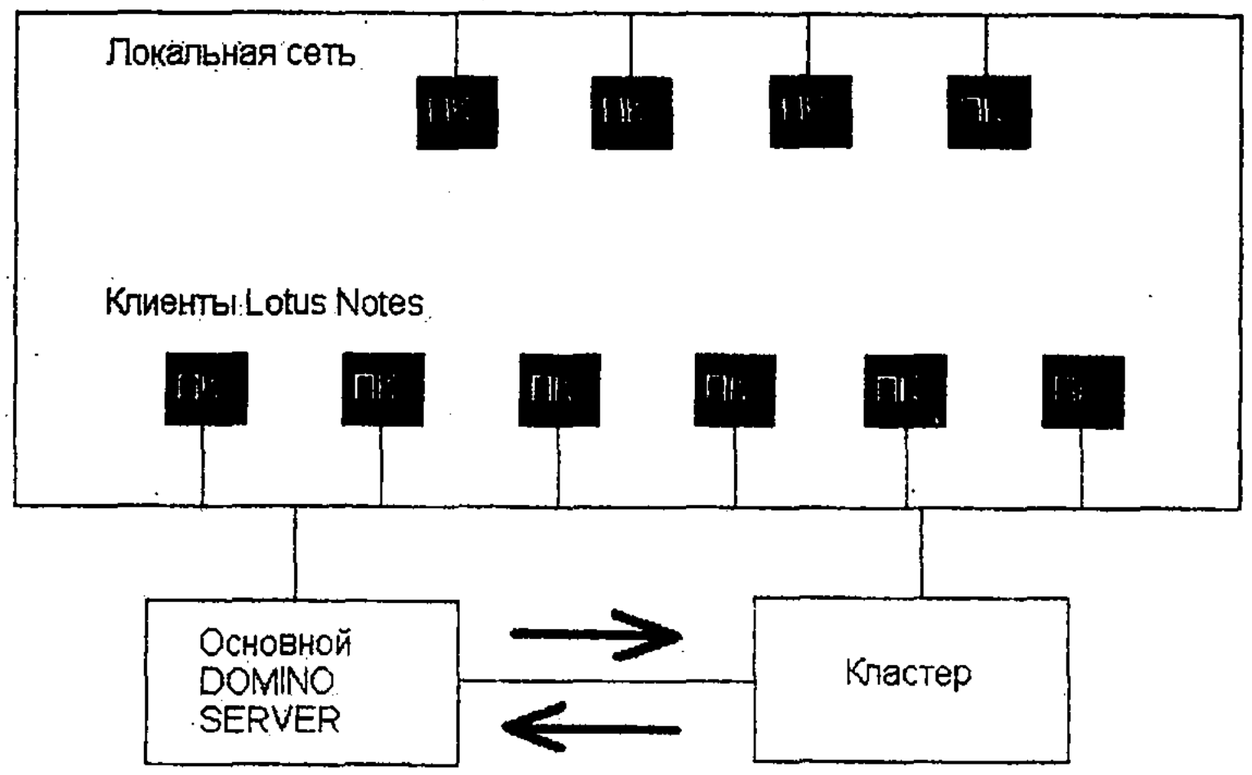
Большой акцент был поставлен вопросам безопасности, надежности и мобильности при создании автоматизированной системы управления учебным процессом (ASU VUZ), написанной в среде Lotus Domino/Notes.

Под безопасностью системы понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на систему [1].

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств. Среди угроз безопасности следует выделить два вида: случайные и умышленные. Источником случайных угроз могут быть выход из строя аппаратных средств, неправильные действия пользователей системы, непреднамеренные ошибки в программном обеспечении и т.д. Умышленные угрозы преследуют цель нанесения ущерба управляющей системе или пользователям.

Одной из самых частых проблем, с которой сталкивается любой администратор систем, – это сбой работы сервера. Причинами ее может быть отключение света, ошибка системы при запуске, неожиданный сбой системы. Для надежной и беспрерывной работы серверов используются зеркальные серверы (кластеры). Они настраиваются таким образом, что каждое изменение в любой базе реплицируется (копируется) в дополнительный сервер. При временном отключении сервера его зеркало полностью заменяет его, работая в 100-процентном режиме (рис.1).

Рис.1. Кластер



Система Lotus обеспечивает эффективную поддержку мобильных пользователей. Во-первых, эти пользователи имеют возможность связаться с серверами Domino по сети или по модемному подключению. С помощью модема они в состоянии соединиться непосредственно с серверами Domino, предусматривающими коммутируемый телефонный доступ, или же с удаленными сетями, после чего обратиться к серверу Domino по этой сети. Во-вторых, пользователи могут подключаться к нужному серверу Domino через промежуточные серверы. Это позволяет им набирать номер одного сервера и использовать его для связи с другими серверами Domino. И наконец, клиенты системы Notes способны поддерживать местные копии баз данных и реплицировать изменения в них на другие серверы, что обеспечивает мобильным пользователям нормальную работу даже в тех условиях, когда они непосредственно не соединены с сервером [2].

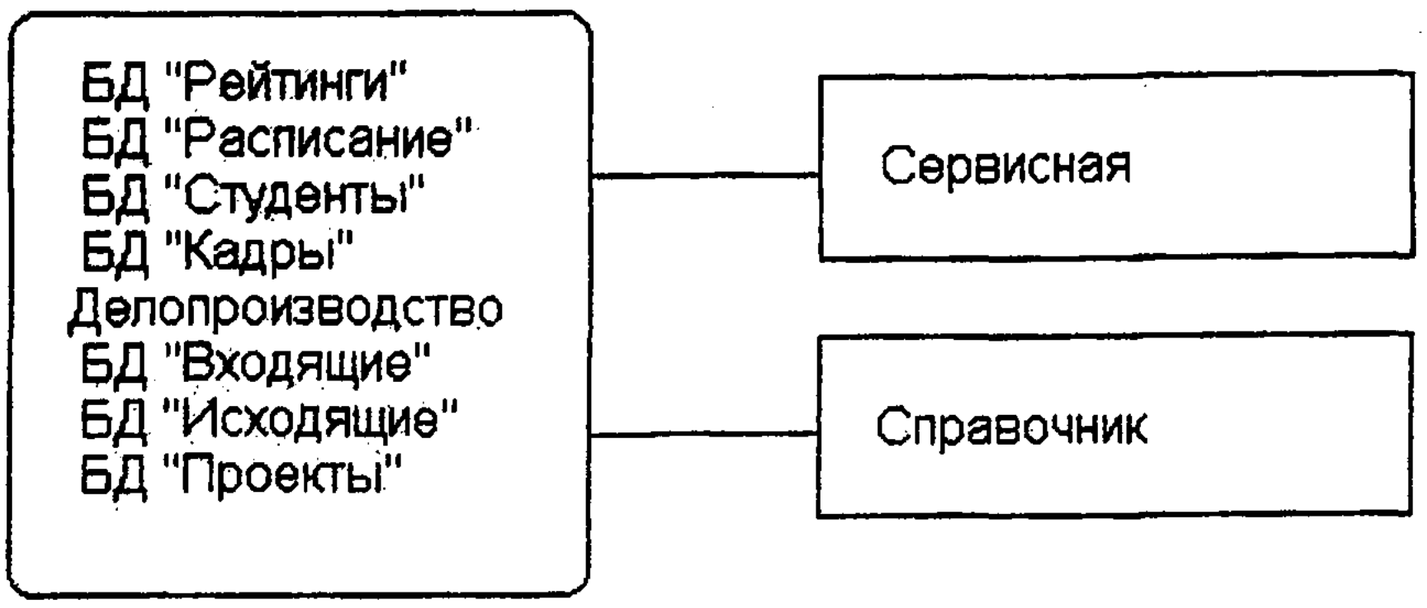
Для предотвращения случайных угроз системе детально была разработана политика раздачи прав для работы с информацией на всех уровнях.

1) Прежде всего, это уровень доступа к базам данных. При входе в базу система определяет данные пользователя, в том числе права на доступ, затем создает Profile – пользователя с необходимыми данными (например, роль пользователя и роль департамента).
2) Второй уровень, это доступ к документам в базе. Существуют два приоритетных атрибута документа:
   - ✓ Доступ на чтение
   - ✓ Доступ на редактирование
3) Третий уровень – это видимость полей в документе.
4) Четвертый уровень – это видимость кнопок и права на их использование.

Детальное распределение ролей для работы пользователей в системе минимизирует риск случайных ошибок. Также любое изменение в документе фиксируется в отдельной базе, в которой даже сам администратор системы не сможет совершить какие-либо правки.

Модульная архитектура ASU VUZ – это лучшее решение для универсальной системы, предназначенной для использования в различных ВУЗах. Различные Базы данных (БД) управляются двумя основными, в которых регистрируются основные данные и настройки системы (рис.2).

Рис.2. Настройки БД.



В «Сервисной» вводятся основные данные сервера (название сервера, кластеров, баз данных, пути расположения и т.д.). Они вписываются в базы в виде профилей БД, куда ссылаются все коды программы. Следовательно, процесс установки системы на новый сервер с новыми характеристиками не займет массу времени, благодаря этой функции.
Также это облегчит огромнейший труд архивирования БД и позволит сохранить все ссылки документов, сэкономив администратору или оператору месяцы работ.

Каждый эксперт по своему оценит существующую систему, но можно с точностью сказать, что политика безопасности, надежности работы и мобильности системы не оставит равнодушным никого.

Литература

[1]. Титоренко Г.А. «Информационные технологии управления». Второе издание, дополненное. Москва, 2003 год. (стр. 192-193)

[2]. Кирклэнд Р. «Администрирование сервера». ДМК – Пресс, 2003 год. (стр. 26-28)

УДК 681.3.05

СМАРТ КАРТАЛАР

Л.Н. Гумилев атындағы Еуразия Ұлттық Университетінің
ИШ-31 тобының білімгері
Калибекова Д.Ш.
Ғылыми жетекшісі: Л.Н. Гумилев атындағы Еуразия Ұлттық Университетінің
«Информатика» кафедрасының аға оқытушысы Зұлпыхар Ж.Е.

Смарт-карта енгізілген микросызбасы бар пластикалық карта. Көптеген жағдайда смарт карта құрылғыны бақылайтын және оның жадысының объектілеріне рұқсат беретін микропроцессордан, операциялық жүйеден тұрады. Сонымен қатар, ереже бойынша смарт карта криптографиялық есептеулерді жүргізетін мүмкіндіктерге ие. Банктік жүйеде смарт карталармен жұмыс әлдеқайда ыңғайлы және пайдалы. Соңғы кездері смарт карталарадың бағасы төмендеуде, сондықтан да смарт карталардың ортасы кеңейтілетін болады. Микросхемалардың орналасуына байланысты барлық смарт карталар бірнеше типтерге бөлінеді. Атап айтқанда, ішкі құрылғыларына және орындау функциясына қарай смарт карталар үш түрге бөлінеді:

*Есептеуіш(тіркегіш, санағыш) карталар.*Смарт картаның осындай түрі әрбір төлемді операцияның тіркелген сомасын есептеу кезінде қолданылады. Мұндай карталарды кей кезде алдын ала төленген карталар деп атайды. Осындай карта есептегіштер автотұраққа, жолға төлемді теледидарға жазылу кезінде қолданылады. Сонымен қатар, телефон автоматтары мен

телефонмен сөйлесуді төлеу кезінде қолданылады. Әдетте телефон автоматтарында сөйлесу уақытының бірлігі минимальды тіркелген бағаға ие болады. Сойлесу үрдісінде картадан әр бір бірлікке қажетті бит саны сызылып отырады. Бастапқыда мұндай карталар бір рет қолдану үшін жасалған. Қазіргі кезде смарт карталардың арнайы код арқылы болған соманы қалпына келтіріп қайта сөйлесе беретін типі шықты. Сонымен қатар, қазіргі уақыттағы карталар идентификациялық мәліметтерден де тұрады, яғни қолданушы туралы мәліметтен тұрады және ол клиенттің қалауы бойынша өзгертіліп отырады.

Жадысы бар карта. Барлық смарт карталар жадымен қамтамасыз етілгендіктен, смарткартаның бұл типі карталар арасында аралық болып табылады. Картаның осы түрі қолданушы туралы ақпаратты сақтау үшін қолданылады. Мұндай карталардың қорғалған және қорғалмаған жады деп аталатын екі түрлі ішкі типі бар. Олар бір бірінен рұқсат етілмеген енуден қорғауымен ерекшеленеді. Қорғалмаған карталарды, сонымен қатар толығымен рұқсат етілген жадысы бар карталар деп те атайды. Осындай карталардың жадысын арнайы командалар көмегімен бағдарламалауға, жаңартуға, көшіруге болады. Қорғалмаған жадысы бар карталарады төлемді карталар негізінде қолдану өте қауіпті. Картаның қауіпсіздігіне байланысты тағы бір айта кететін жайт картаның мәліметтеріне шектеу қою болып табылады. Банк картаға ақшаны тіркеуі, дүкеннің картадан ақшаны алуы және т.б. операциялардың барлығы клиенттің қатысымен жүзеге асуы керек. Сондықтан да картаның жадысы екі бөлікке бөлінеді: дебетті және кредитті. Смарт картаға ие адам өзінің құпия кілтіне ие болады. Ақпараттық кілтке тек банк ие болады.

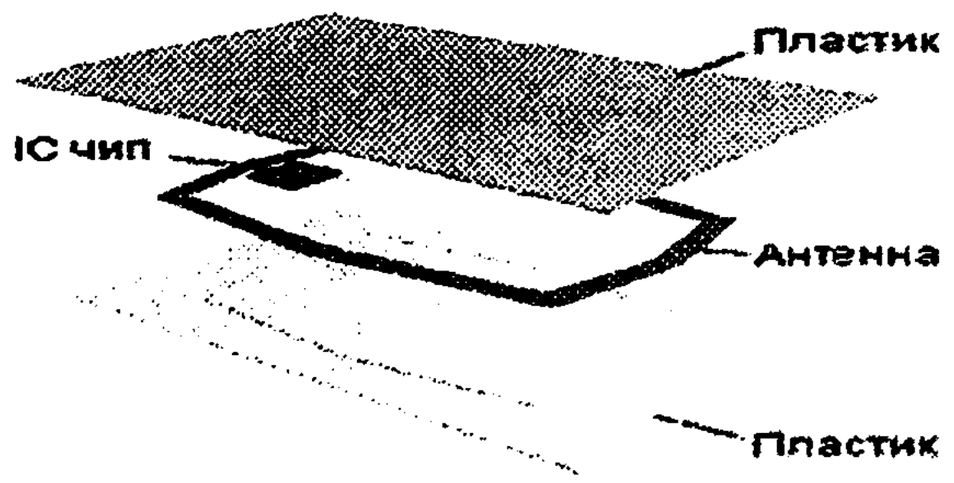
Микропроцессорлы карталар. Бұл смарт карталардың ішінде ең дамыған түрі. Олар ақпараттың күрделі талаптарын өңдеу үшін қолданылады. Микропроцессорлы карта микроконтроллерден, орталық процессордан тұрады. Микропроцессорлы смарт карта қажетті сервисті операцияны орындайтын енгізілген операциялық жүйеден тұрады. Барлық ақпарат көп деңгейлі құрылым түрінде келтірілген. Осындай типті карталарға DES дәстүрлі криптографиялық алгоритмдер орнатылады. Ол ақпараттың шифрленуін және цифрлы жазбаның сұранысын қамтамасыз етеді. Сонымен қатар, карталар сервисті функцияның әр түрлі спектрін орындай алады. Банктік операцияларды орындау үшін, мысалы карточкадан жұмыстың блокқа түсу мүмкіндігімен электронды төлемдерді енгізу құралдарын қарастырады. Блокқа түсудің екі түрін қарастырады: дұрыс емес транспортты кодты енгізу кезінде және рұқсат етілмеген ену кезінде.

Смарт карталарды қолданудың артықшылықтары:

- Біріншіден, смарт карталардың карталардың басқа түрлерінен негізгі айырмашылығы - жоғары интеллектуалды микросхемадан тұруында;
- Екіншіден, магнитті немесе штрихті карталар көмегімен төлемдерді тек on-line режимінде ғана жүреді. Төлемді операциялар үшін банкпен байланыстыру керек және рұқсат алу керек. Осындай жағдайда негізгі мәселе болып байланыстың жылдам, арзан, сенімді түрін қамтамасыз ету болып табылады;
- Үшіншіден, смарт карталар жоғары сенімділігі мен қауіпсіздігімен ерекшеленеді. Микросхема өзіндік шешім қабылдау үшін жеткілікті интеллектпен қамтамасыз етеді;
- Смарт картаның ең негізгі артықшылығы болып ақпаратты талдау, математикалық есептерді жүргізу және логикалық шешімдер қабылдау болып табылады;
- Төмен төлемді және қызмет көрсету ортасына байланыссыз;
- Коммуникациялармен тұрақты байланысты қолдану қажеттігі жоқтығында, яғни қолданушының қалауы бойынша қолдану;
- Ақша құралдарын тез арада ауыстыру кезінде инфляцияның төмендетілуі;
- Сапасының жоғары деңгейде болуы және картаның қауіпсіздігі күрделі өнеркәсіппен қорғалады.

Экономиканың дамуы смарт карталарды қолдануда жаңа белестерді ашады. Ірі қаржы компаниялары интеллектуалдық смарт картаның қолданылуының осындай технологияға көшуін жариялады. Сонымен қатар, смарт карталарды контактілі және контактілісіз деп

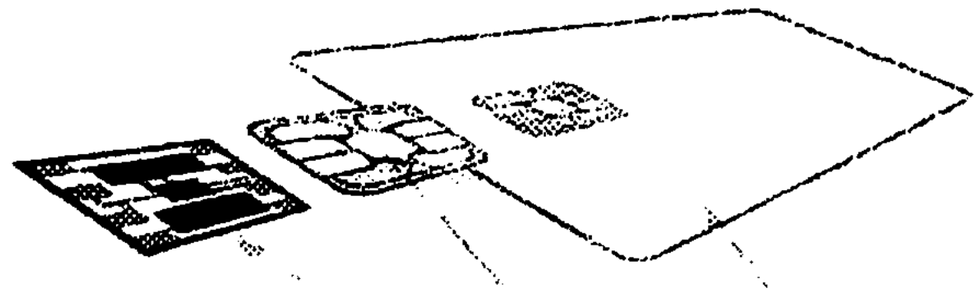
бөледі. Контактілісіз смарт карталар объектілердің радиожиілікті жүйе элементтері болып табылады. Объектінің идентификациясы смарт картаның чипінде сақталған уникальды цифрлі кодында жүзеге асады. ЧИП смарт картаның денесінде орналасады, осы жерде сонымен қатар радиотолқындардың қабылдауы мен шағылуы жүзеге асатын антенна орналасады.



1-сурет.Контактілісіз смарт-карта.

Смарт картадан ақпаратты оқу әдісіне қарай:контактілі,контактілісіз,екілік интерфейсті болып бөлінеді. Контактілі карта есептегішпен картаның металды контактілі ауданына тәуелісіз әсерлеседі. Контактілі смарт карта үш бөліктен тұрады (2-суретте):

1. Контактілі облыс.
- төртбұрышты немесе овальды формадан тұратын 6 немесе 8 контакт;
- ISO-7816 стандартымен сәйкес орындалатын контакті позициялары
2. Чип(картаның микропроцессоры)
3. Пластикалық негіз



2-сурет. Контактілі смарт карта құрылысы

Соңғы кездері смарт карталардың танымалдығы жоғарылап келе жатыр. Оның себебі смарт карталардың қарапайым карталардан қарағанда күрделі айырмашылықтарының болуы, жұмыс үшін қажетті ақпараттардың көп көлемін сақтауға болатын жадыдан тұруы. Банкоматтар мен кассаларда қолданылатын карталарды төлем жүйелерінде магнитті карталарды қолдану кезінде банкпен немесе басқа қызмет көрсету орталығымен байланыста болады. Смарт карталармен жұмыс кезінде есеп туралы мәліметтер тәуелсіз карта жадысында сақталады. Сондықтан да берілген смарт картаны қасиеті арнайы каналдарда үнемдеуге мүмкіндік береді. Смарт карталарда ақпаратты оқудан қорғау жүйесі бар. Осы қасиеті картаны қорғаусыз көшіруден сақтайды. Смарт картамен ақпаратты алмастыру шифрленген түрде жүреді, сондықтан да картаны өзгерту және алмастыру қиынға соғады. Осы мүмкіндік ақпартыңыздың біреу оқымайтынына жүз пайыз сенімділік береді және сіздің мәліметіңіз кассирге немесе сатушыға белгісіз болады. Смарт карталар көп уақытқа жарамды болады. Ол электромагниттік сәулелендіру мен су, химикаттардан аз бұзылады. Смарт карталардың жарамдығы үш жылдан он жылға дейін, ал магнитті карталар тек бір-екі жылға ғана жарайды. Біз мысалы ретінде Қазақстан Республикасының екінші деңгейлі «Цеснабанк» АҚ банкінде қолданылатын картаға сипаттама берсек: «Цеснабанк» АҚ клиенттеріне және төлем карточкалар иелеріне *«Card to Card» қызметі* – ақша қаражатын аударудың өте ыңғайлы, әрі жылдам тәсілін ұсынады.

- «Card to Card» – банкомат арқылы карточкадан карточкаға ақша аудару жүйесі:
- Цеснабанк карточкасынан Цеснабанк карточкасына;
- Цеснабанк карточкасынан Халық Банк карточкасына;
- Халық Банк карточкасынан Visa Electron Цеснабанк карточкасына;
- «Card to Card» қызметін ақша алушының төлем карточкасының нөмірін білетін «Цеснабанк» АҚ төлем карточкаларының кез келген иесі пайдалана алады;
- Банкомат арқылы ақша аудару карт–шоттың енгізілген валютасы – теңгемен «Цеснабанк» АҚ карточка иелерінің карт–шоттары бойынша жүзеге асырылады;
- Банк комисиясы – аударым сомасына қарамастан бір аударымға 90 теңге ақша жіберушінің карт–шотынан автоматты түрде ұстап қалынады;
- Ақша алушының карт–шотына банкомат арқылы аударылған ақша операциясы жасалып болғаннан кейін бірден аударылады. *Осы қызметтің артықшылықтары:*

1. Жылдам, әрі ыңғайлы. Сіз карточкадан карточкаға ақша аударымын сізге ыңғайлы уақытта және қолайлы орында жасай аласыз. Сондай–ақ аударымды жасау және артық қағаз толтыру үшін банкте кезекте тұрудың қажеті жоқ. Құжаттарды ұсыну талап етілмейді;
2. Қызметтің қолайлығы тәуліктің кез келген уақытында, демалыссыз жұмыс істеуінде. Ақша алушы Қазақстанда, сондай–ақ басқа шетелдерде жүрседе да ақшаны ала алады;
3. Операцияны жүзеге асырудың жеңілдігі – банкоматтың мониторындағы менюдің жеңіл, әрі түсінікті болуында;
4. Аударым сомасына қатысты емес төмен тарифтер. Сондай–ақ банкомат арқылы клиент қандай сома аударғандығына комиссия қатысты емес;
5. Card to card қызметі тек «Цеснабанк» АҚ карт–шоттың енгізілген валютасы – теңгемен жеке тұлғалар карточкасы бойынша ғана пайдалана алады. Жеке тұлғалардың валюталық карточкалары, сондай–ақ заңды тұлғалардың корпоративтік карточкалар бойынша осы қызмет түрі ұсынылмайды;
6. Бар болғаны – «Цеснабанк» АҚ төлем карточкасының иесі болсаңыз және ақша алушының төлем карточкасының нөмірін білсеңіз болды;
7. Ақша карт–шотқа операция жасалған соң бірден түседі;
8. Банкоматтағы қажетті шараларды жасау арқылы ақша аударымын жіберетін адамның карточка нөмірін және аударым сомасын тересіз.

Сонымен, қорыта келгенде қазіргі заманда қолданылатын смарт карталар дегеніміз: Микропроцессоры бар төлем карточкасы (*smart-карточка, smart card*) - жасалатын кезде модуль және процессордан тұратын микросхема орнатылатын пластикалық карта. Микросхеманың жадысы арнайы қосымшалар үшін ажыратылған рұқсатпен сегменттерге бөлінеді. Жеке сегменттер карточканың эмитентімен қолданылады.

Әдебиет

1. А. Каменкова. Рост в ожидании спада // Эксперт, 2003, №1.
2. Р. Фостер. Обновление производства: атакующие выигрывают. - М.: Прогресс, 1988. - 286
3. Скрипкин К. Г. Экономическая эффективность информационных систем. - М.: ДМК пресс, 2002.

УДК 621.395.6.003.63

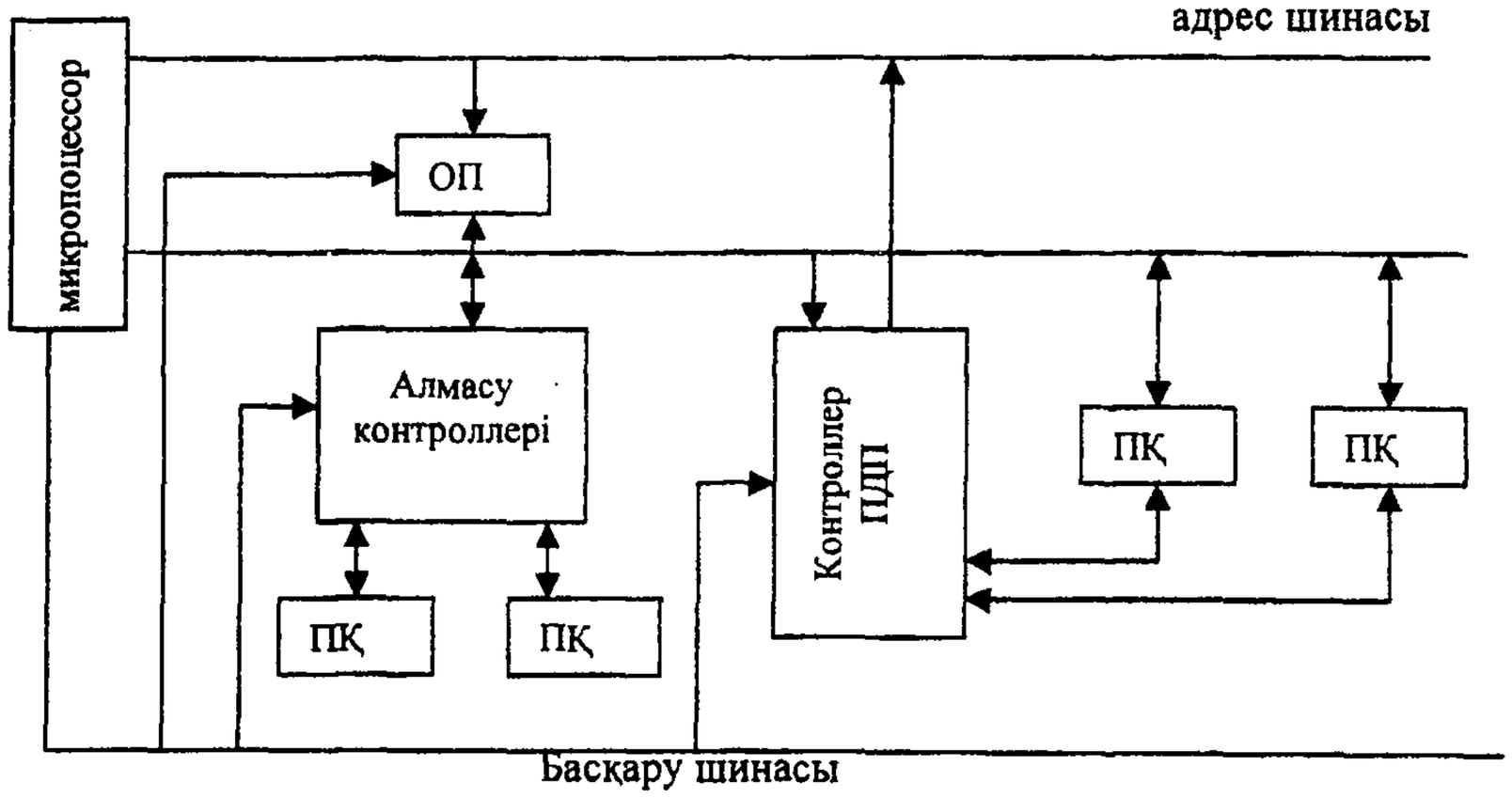
МИКРОПРОЦЕССОРЛЫҚ ТЕХНИКАДА ҚОЛДАНЫЛАТЫН ПЕРИФЕРИЯЛЫҚ ҚҰРЫЛҒЫЛАР

Салиева Ж.О.
Л.Н.Гумилев атындағы ЕҰУ магистранты, Астана
Ғылыми жетекшісі – д.т.н.,профессор А.А.Садыков

Қазіргі микроконтроллерлер микропроцессорлық жүйенің барлық негізгі элементтерін: жады, енгізу-шығару құрылғылары, үзу жүйесі, таймерлер және т.б. құрайтын әмбебап микросхемаларын көрсететіндей интеграция деңгейіне жетті. Микросхемалар шегінде қалатын негізгі элементтер кварцтық резонатор және қоректендіруді қосқандағы алғашқы алып тастауға арналған бірнеше элементтер ең қажетті элементтер болып табылады. Микропроцессорлық техниканың қазіргі даму тенденциясы ішкі элементтердің барлығы микроконтроллерлерідің ішінде орналасатынына бағытталады. Сондықтан микроконтроллерлер өзіндік жеткілікті жүйе болып табылады. Қарапайым тапсырмаларды ішкі қосымша элементтердің көмегінсіз шеше алады. Мысалы, телефондық розеткеде орындалған телефондық қосымшалардың бүтін жиыны. Өзінің қарапайымдылығына қарамастан мұндай қосымшалар күрделі қызметтерді орындайды. Қарапайым жағдайда сіздің телефон желісін рұқсатсыз қолдануды, сіздің бақылауыңсыз болатын қала аралық қоңырауларды бұғаттауы мүмкін. Екі абонентке бір телефондық линияны қолдануға мүмкіндік беретін телефондық розеткедегі АТС линиясын жоғарғы мүмкіндіктегі жағдай деп есептеуге болады.

Бірақ көп жағдайда тәжірибелік тапсырмаларды шешу үшін ішкі элементтерді қоспау мүмкін емес. Микроконтроллерлерге міндетті түрде ішкі есеп берулерді, әр түрлі орындауларды басқаратын батырмаларды және индикаторлық құрылғыларды қосу керек. Бұл барлық құрылғыларды перифериялық құрылғылар деп атау қабылданған. Мұнда сызбаларды өңдеу, сонымен қатар, басқарылатын бағдарламаларды өңдеу ұғымдарыда түсіндіріледі. Атап айтқанда перифериялық құрылғыларды сауатты және рационалды түрде қосуды білу мен схемотехника өнерінен тұрады.

1-суретте көрсетілген микропроцессорлық жүйенің құрылымдық сызбасын қарастырайық.



1-сурет. Микропроцессорлық жүйенің сызбасы.

Микропроцессорлық жүйенің қызметі келесідей жағдайлардың реттіліктерімен анықталады: әртүрлі перифериялық құрылғылардан түскен ақпараттар, деректерді өңдеу мен перифериялық құрылғыларға өңдеу нәтижелерін беру. Бұл жағдайда өңдеуге тапсырылған перифериялық құрылғылардан түскен деректер оларды өңдеу процесінде де түсуі мүмкін.

Микропроцессорлық сызбадағы бұл әрекеттерді орындау үшін микропроцессордан басқа мынадай құрылғылар қарастырылады:

- сақтауға және бағдарлама командаларына сұраныс бойынша тапсыруды, микропроцессордың жұмысын, әртүрлі деректерді анықтауға арналған оперативті жады;

- микропроцессормен және оперативтік жадымен берілген әртүрлі периферияльық құрылғылардың деректерін алмастыруды қамтамасыз ететін құрылғылар контроллерлері.

Микропропроцессор кезекті команда сақталатын оперативті жадының ұяшық номерін адрес шинасына жібереді, оперативті жадыдағы басқару шинасынан жады ұяшығының адрес шинасын көрсететін құрамдағы есептеуді қамтамасыз ететін сигналдар келеді. Оперативті жады деректер шинасына тыйым салынған микропроцессорға қабылданатын команданы жібереді. Мұнда команда ашылады. Егер деректер, команда қарайтын әрекеттер микропроцессор регистірінде болса, онда микропроцессор командада көрсетілген операцияны орындауға көшеді. Егер команда ашылғанда операцияға қатысатын деректер оперативті жадыда болса, онда микропроцессор осы деректерді сақтайтын ұяшық адресінің шина адресіне қояды; оперативті жадыдан түскен ақпараттарды жіберуде микропроцессор оларды деректер шинасы арқылы қабылдайды да, содан соң деректер операциясы арқылы орындалады. Шина адресіне ағымдық команданы жіберу аяқталғаннан кейін келесі команда адресі жіберіледі, берілген процесс қайталанады.

Периферияльық құрылғылармен деректер алмасу келесідей жағдайлармен жүзеге асырылуы мүмкін. Периферияльық құрылғылардың тобы микропроцессорлық жүйе деректерінің шинасына деректер алмасу процесін басқаратын алмасу контроллерлері арқылы қосылады. Периферияльық құрылғылармен деректер алмасу алдында микропроцессор шина арқылы контроллерлерге жіберуде қолданылатын тәртіп туралы ақпаратты, периферияльық құрылғылар контроллерлеріне қосылған әрбір деректер алмасуда қолданылатын деректерді жіберу бағыттары туралы деректерді беруі қажет. Содан соң, мысалы периферияльық құрылғыдан жіберілетін деректер оперативті жадыға беру талап етілсе, микропроцессор енгізу командасын орындап, контроллерге сәйкес басқарушы сигналдарды жібереді; периферияльық құрылғылардан деректер контроллерлер регистірінде қабылданады. Содан кейін бұл деректер мәліметтер шинасымен микропроцессорға қабылданып, сәйкес командаларды орындау процесінде олар оперативті жадыға жіберіледі.

Сыпайы түрде кері бағыттағы деректермен алмасу оперативті жадыдан периферияльық құрылғыға алмасу жүреді. Сәйкес команда бойынша бағдарламалар оперативті жадыдай деректер микропроцессорына қабылдау жүзеге асырылады, келесі команданың біреуі бойынша бұл деректер деректер шинасына көрсетіледі, контроллер арқылы периферияльық құрылғыға жіберіледі.

Суреттелген алмасу деректер алмасу жағдайлары алдын ала бағдарламалау этапында белгілі, бағдарламада алмасуды қамтамасыз ететін командалар анықталған орындарда қарастырылады. Алмасу жағдайлары периферияльық құрылғылардың өзімен де анықталуы мүмкін сонда бұл жағдайлар бағдарламалаушыға белгісіз болып саналады, ол бағдарламадағы сәйкес командалардың алмасуды қарай алмайды. Бұл жағдайда периферияльық құрылғылар анықталған сигналдарды микропроцессорға жіберуде оның жағдайындағы үзуді жібереді. Бұл жағдайда микропроцессор негізгі бағдарламаны орындауды тоқтатып, периферияльық құрылғымен талап етілген деректер алмасуды қамтамасыз ететін бағдарламалардың оперативті жадыда сақталатын басқа командаларды орындауға ауысады. Мұндай үзілу бағдарламасы аяқталғаннан кейін микропоцессор негізгі бағдарламаны орындауға көшеді.

Суреттелген тәсілдер алмасудың төменгі жылдамдығын қамтамасыз етеді және төмен жылдамдықты периферияльық құрылғылармен деректер алмасуда мақсатқа сай қолданады. Жоғарғы жылдамдықты периферияльық құрылғылармен жұмыс жасауда жадыға тікелей қатынау режимі қолданылады. Бұл режимде микропроцессор адрес шинасы мен деректерден үзіледі, оперативті жадымен деректер алмасу үшін периферияльық құрылғылардың орналасуын көрсетеді. Алмасу бұл жағдайда жадыға тікелей қатынаудың арнайы контроллерлермен ұйымдастырылады.

Периферияльық құрылғылардың жадысына тікелей қатынау режимінде оперативті жадымен біркелкі деректер емес, үлкен деректер жинағы алмасады. Жадыға тікелей

қатынау контроллерлеріне микропроцессор алмасуға басқаруға қажетті ақпаратты орналастырады. Алмасу үрдісінде жадыға тікелей қатынау контроллері адрес шинасына оперативті жадының ұяшық адресін берелі, жіберу аяқталғаннан соң оперативті жады мен перифериялық құрылғы арасындағы сөздер жадыға тікелей қатынау контроллері деректер шинасы арқылы адрес шинасына берілетін адрес мәнінің берілгеніне үлкейеді. Берілген сөздер санын жіберу аяқталған соң жадыға тікелей қатынау контроллері микропроцессорға хабарлау арқылы алмасуды тоқтатады. Нәтижесінде адрес шинасы мен және деректермен байланыс қайта қарастырылады және бағдарламаны орындау жалғасады.

Әдебиет

1.А.В.Белов. Конструирование устройств на микроконтроллерах. Санк-Петербург 2005 г.
2.Б.А.Калабеков. Цифровые устройства и микропроцессорные системы. Москва 2007 г.
3.А.Е.Васильев. Микроконтроллеры. Москва 2008 г.

УДК 681.32:37

ЗАМАНАУИ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР (ПОДКАСТИНГ) МҮМКІНДІКТЕРІН ПАЙДАЛАНА ОТЫРЫП ӘЛЕМДІК БІЛІМ БЕРУ ЖҮЙЕСІНІҢ АЛДЫҢҒЫ ҚАТАРЫНАН ОРЫН АЛУ

Салиева Ж.О.
Л.Н.Гумилев атындағы ЕҰУ магистранты, Астана
Салиева Д.О.
Л.Н.Гумилев атындағы ЕҰУ оқытушысы, Астана

Бұл мақала Президентіміз ұсынған «Санаткер ұлт – 2020» бағдарламасын жүзеге асыруды қолдаудың жазбаша көрінісі болып табылады.

Аталмыш бағдарламаның 3 өзекті мәселесін оқытушылардың алдына қойылған бүгінгі басты талаптар деп білеміз. Олар:

1. Оқытудың инновациялық әдістемесін дамыту;
2. **Ақпараттық эволюция**;
3. Жастарға рухани тәлім-тәрбие беру.

Елбасының білім және ғылым саласына аса көңіл бөлуінің үлкен мәні бар. Себебі, мемлекеттің даму көрсеткіші болып сол елдің ЖОО мен ғылымдағы жетістіктері табылады. Л.Н. Гумилев атындағы Еуразия ұлттық университеті еліміздің алдыңғы қатарлы ЖОО-ның бірі, алайда ол әлемдік білім жүйесінің алдыңғы қатарлы мүшесі болуға тиісті. Ол үшін, біріншіден, біз, оқытушылар және білім алушылар кауымы қажырлы еңбек етуге міндеттіміз. Екіншіден, университет ақпараттық эволюциядан кейін қалмай, инновациялық өнімдер мен әдістерді өз жүйесінде пайдалуға тиісті. Мәселен, қазіргі таңда алыс және жақын шетел білім жүйесінде төмендегі заманауи ақпараттық технологиялар мүмкіндіктері кең ауқымды игерілуде: блоггинг, веб-блоггинг, әлеуметтік желі, iTunes, подкастинг және т.б. Бұл жұмыста соңғы жетістікті білім беру саласында қолдану мәселесіне тоқталамыз. «Подкастинг» Оксфорд сөздігіне (New Oxford American Dictionary) 2004 жылы енгізіліп, бір жылдан соң «Жыл Сөзі» атағына ие болды. Блоггер Док Серлс зерттеуі бойынша 2004

жылдың 28 қыркүйегінде подкастинг сөзін Google-дан 24 адам қараса, бүгінде олардың саны 2 миллионнан асып кеткен [1].

Қазіргі таңда Қазақстанда подкастинг енгізілмеген, көршілес Ресейде бұл техникалық жетістік қолданыста болғалы көп уақыт өте қоймағанымен Батыста ол ақпарат таратудың тиімді түріне айналған.

Бұл сөздің этимологиясына тоқталатын болсақ, подкастинг ағылшынның iPod (Apple компаниясы ұсынған mp3-плеері) және broadcasting (кең ауқымды хабар тарату) деген сөздерінен құралған. Подкастинг аудио және видеоконтентті интернет арқылы таратудың жаңа форматы болып табылады. Ол мультимедиа-контентті жай ғана rss-каналға (Really Simple Syndication – өзгеріп тұратын веб-контентті тарату каналы) енгізу арқылы жүзеге асырылады.

Алайда ұсынатын мүмкіндіктері бойынша подкастинг – интернет пен радио артықшылықтарының синтезі болып табылады.

Подкаст деп – аудио және видеофайл түрінде жазылған кез келген ақпаратты айтамыз: дәрістер, шетел тілі сабағы немесе компьютердің құрылымы туралы сабақ, т.с.с Оқытушылар өздері жүргізетін курстар бойынша үй тапсырмаларына немесе дәрістерге подкаст жасап, оны барша халықтың қолданысына жариялай алады. Ал студенттер тек аудиториялық сабақтармен ғана шектеліп қоймай, берілген сабақты және сол сабаққа қатысты шетел профессорларының подкасттарын өзіне ыңғайлы уақытта және жерде көре не тыңдай алады [2]. Сонымен қатар олар өз подкасттарын оқытушылар назарына жариялай алады. Бұл әдіс студенттердің өзіндік жұмысы мен ізденіс қабілетін дамытады.

Университет кітапханасында миллионнан астам кітап түрі бар. Алайда қазіргі «электронды әлем» ғасырында дәстүрлі кітапханамен бірге электронды кітапхана дамуға тиісті. Бұл, әсіресе, университеттің алдағы қашықтықтан оқыту жоспарын жүзеге асыруда аса маңызды мәселе болып табылады. Әр факультет сайттағы өз парақшаларында подкасттар жарияласа, аудио және видео форматтағы дәрістерін білім алушылармен қоса кез келген азамат пайдалана алады. Өз кезегінде подкастинг, сонымен бірге, келешек студенттер мен олардың ата-аналарына таңдалынған университет туралы ақпарат алуына үлкен көмек береді. Бұл орайда подкастингтің негізгі мақсаты – «интеллектуалды байлықты» бүкіл әлеммен бөлісу болып табылады.

Подкастқа арналған софт (бағдарламалық қамтамасыздандыру). Бүгінде подкастингге арналған бағдарламалар көп. Осы тұрғыда Apple компаниясының өнімдеріне аса көңіл бөлу керек. Мәселен, iTunes медиаплеері аудио және видеоконтенттерді көрсетуді қамтамасыздандырады. iTunes бағдарламасын қолдануда ең қолайлы құрал iPod болып табылады.

Подкастқа арналған тағы бір бағдарлама – Juice (бұрынғы атауы – iPodder). Ол қолданыста қарапайым, сонымен қатар басқа да аудио файлға арналған бағдарламаларды қабылдайды: iTunes, Windows Media Player және WinAmp.