

**Министерство образования и науки Республики Казахстан**

**Казахстанский филиал Московского государственного университета  
имени М.В.Ломоносова**

**Евразийский национальный университет имени Л.Н. Гумилева**

**Ассамблея народа Казахстана**

**Международная научная конференция студентов,  
магистрантов и молодых ученых**

**«Ломоносов – 2009»**

**10-11 апреля 2009 года**

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

**ТЕЗИСЫ ДОКЛАДОВ**

**І часть**

**Астана, 2009**

УДК 378  
ББК 74.58я431  
Л 75

#### Организационный комитет

Сидорович А.В. (председатель), Берсимбаев Р.И., Бекмаганбетов К.А., Власова Г.И., Котлярова Т.Г., Коченов В.Г., Нурсултанов Е.Д., Отелбаев М., Нетесов В.В. (ответственный секретарь).

**Л 75 «Ломоносов - 2009»: Международная научная конференция студентов, магистрантов и молодых ученых: Тезисы докладов Международной научной конференции: В 2-х частях. - Астана: Казахстанский филиал МГУ имени М.В.Ломоносова, 2009. - 362с.**

ISBN 9965-31-234-6

В сборнике тезисов Международной научной конференции студентов, магистрантов и молодых ученых рассматриваются актуальные вопросы развития математики и информатики, экономики, языкознания и литературоведения, экологии и природопользования и молодежного сотрудничества.

Сборник представляет интерес для научных работников, преподавателей, аспирантов, магистрантов и студентов вузов.

**В подготовке сборника к печати принимали участие:**

Власова Г.И., Бекмаганбетов К.А., Нетесов В.В., Леонтьева С.В., Сарыбекова Л.О., Абельдинова П.Т., Блинова Г.А., Жайкенова Ж.Б.

4309000000  
Л 00(05)-09

УДК 378  
ББК 74.58 я431

**Тексты тезисов печатаются в авторской редакции**

© Казахстанский филиал  
МГУ имени М.В.Ломоносова

|                                                                                                               |    |
|---------------------------------------------------------------------------------------------------------------|----|
| Садыкова Р.С. О сопряжении подмножеств в группе.....                                                          | 54 |
| Сатышпова Ж.С., Абуова З.А. Кейбір алгебралық теңдеулер жүйесін шешуде стандарт емес тәсілдерді қолдану.....  | 55 |
| Сахова А.Б., Адилметова М.У. Теңбе-теңдіктерді дәлелдеуде туындының қолданылуы.....                           | 56 |
| Солтыбаева Л.С. О достаточных условиях двоичной дифференцируемости суммы рядов по системе Уолша.....          | 58 |
| Суттибаева Г.Д. Оценки приближения средними Чезаро в весовых пространствах....                                | 59 |
| Сыздыкова А.Т. Об одном аналоге теоремы Харди – Литтлвуда для кратных рядов по мультипликативной системе..... | 61 |
| Таукен А. Задачи на восстановление окружности Эйлера.....                                                     | 62 |
| Теняева Л.И. О центральной эквивалентности элементов смежных классов групп                                    | 64 |
| Тынымбаев Б.А. О сравнительной сложности вскрытия схем электронной подписи.....                               | 65 |
| Ыдырыс А. Аналог неравенства Карамата.....                                                                    | 68 |
| Ютовец Е.В., Ляшенко И.И., Павлюк И.И. Об индексной эквивалентности и FC – центре группы.....                 | 69 |

## МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

|                                                                                                                                                                        |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Абдрахманова Л.Г., Аубакир Д.А. Применение эстиматорных неравенств в адаптивном управлении в условиях неопределенности.....                                            | 71  |
| Абдышев Ж.М., Потеряева М.С. Прикладное значение теоремы об огибающей в экономическом анализе.....                                                                     | 73  |
| Абдуллаева Ж.А., Маукенова Ж.Е. Производственная функция.....                                                                                                          | 75  |
| Абенова Ж.С. Кусочно-линейная технология геометрической обработки.....                                                                                                 | 76  |
| Абжанова А.Е., Жалгасбекова Ж.К. Использование функций сглаживания в пакете Mathcad для обработки экспериментальных данных.....                                        | 78  |
| Агыбетова А.Е., Ахметова А.К., Джунусбеков А.С. Компьютерное моделирование образования радиационных дефектов в целочно-галлоидных кристаллах на базе пакета MORAS..... | 80  |
| Айгозин Б.К., Шаханова Г.А. Основные принципы разработки электронных изданий в вузе.....                                                                               | 82  |
| Айтжанов М.Е., Малибекова М.С. Основы разработки систем автоматизированного управления.....                                                                            | 84  |
| Антоненко А.А., Евграфова А.М. Фрактальный синтез графических изображений....                                                                                          | 86  |
| Аринова А.Б. Производственная функция с постоянной эластичностью замены ресурсов.....                                                                                  | 88  |
| Асылбекова Ж.Ш. Особенности обработки графической информации методами сжатия.....                                                                                      | 90  |
| Байжуманова А.Э. Анализ модернизации образования в странах СНГ. Интегрированные автоматизированные системы управления (ИАСУ).....                                      | 92  |
| Бейбитхан Е. Хаттамалардың дәріменсіздігі мен кеңейтілген шекті автоматты түрі.....                                                                                    | 93  |
| Галиев Д.С. Система электронного документооборота в ВУЗе.....                                                                                                          | 95  |
| Галиев Д.С. Автоматизированная система управления в ВУЗе.....                                                                                                          | 97  |
| Галиева Н.К. Оценки параметров распределения Стюдента.....                                                                                                             | 99  |
| Дарбаева Д.К. Особенности применения основных статистических методов в здравоохранении.....                                                                            | 100 |

функциональности за счет взаимодействия с программным обеспечением независимых поставщиков, а при необходимости и с собственными наработками пользователей;

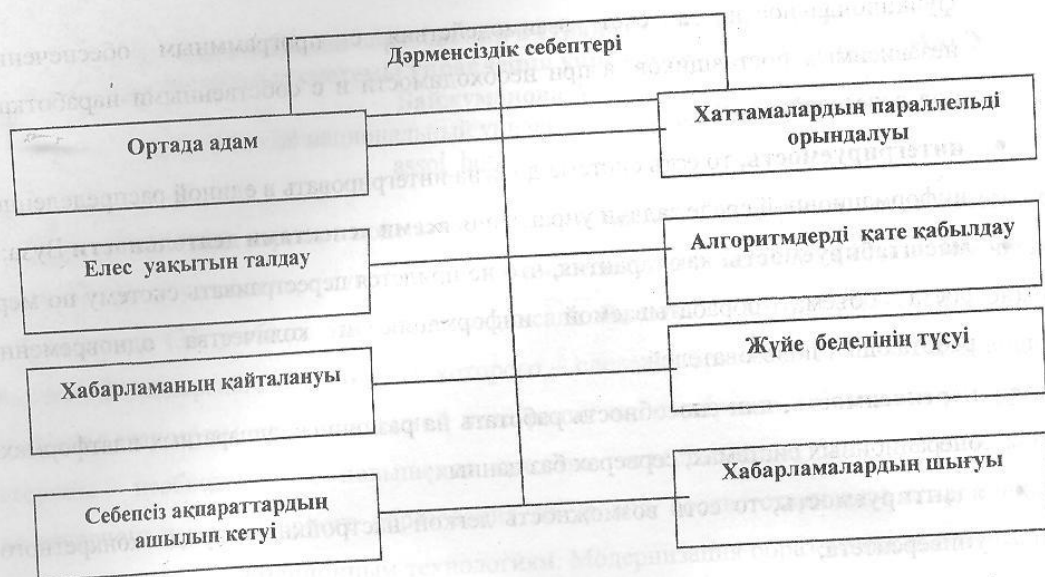
- **интегрируемость**, то есть система должна интегрировать в единой распределенной информационной среде задачи управления **всеми аспектами деятельности** Вуза;
- **масштабируемость**, как гарантия, что не придется перестраивать систему по мере роста объема обрабатываемой информации и количества одновременно работающих пользователей;
- **переносимость**, или способность работать на различных аппаратных платформах, операционных системах, серверах баз данных;
- **адаптируемость**, то есть возможность легкой настройки на нужды конкретного университета;
- **расширяемость** – возможность наращивания функциональных возможностей системы, не выходя за рамки принятой изначально концепции развития и технологической базы, в соответствии со специфическими потребностями пользователей;
- **локализация**, то есть поддержка национальных требований и стандартов в области бухучета, финансового контроля, документооборота, организации процесса обучения, особенностей системы образования.

В этом докладе я собираюсь осветить несколько ИАСУ из стран СНГ, выделить отличительные особенности и различия, предложить на основе проведенного анализа наиболее оптимальный вариант.

#### **Хаттамалардың дәріменсіздігі мен кеңейтілген шекті автоматты түрі** **Бейбітхан Е.**

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің магистранты,  
Yerkegul\_1@mail.ru

Ақпаратты қамтамасыз ету хаттамасының дәріменсіздігі - бұл абоненттердің қолданып жатқан криптографиялық алгоритмдерінің тікелей бұзылуынсыз зиян келтіруіне себепші. Хаттаманың жұмысына және оның талаптарына кедергі келтіру үшін қаскүнемдер қолданатын шабуылдар мен амалдарының түрлері (1-сурет).



### 1-сурет. Ақпаратты қамтамасыз ету дәрменсіздігін пайда болу себептері

**Ортада-адам.** Қаскүнем екі абоненттің арасындағы ақпарат алмасу процесіне еніп алады. Ортада адам әдісінің атауы ағылшынның **man-in-the-middle (MINM)** терминінен шыққан. Бұл ашық кілтті криптографиялық алгоритмдерді қолданатын хаттамаларға тиісті.

**Елес уақытын талдау.** Бұл шабуылдың класын себепсіз хабарламалардың ашылып кетуі (oracle) класының арнайы ішкі класына жатқызуға болады. Кейде бұл шабуылдар ақпаратты қамтамасыз ету хаттамаларына сәтті шабуыл жасауды жүзеге асыруға жеткілікті болады. SSL/TLS [1] хаттамаларына шабуыл жасау мүмкіндігі мысал бола алады. SSL (англ. Secure Sockets Layer — Сокеттердің қорғалған деңгейі) хаттамасы [2, 3] формальді талдау әдіс көмегімен бірнеше рет талданғанын ескеру керек.

**Хабарламалардың шығуы.** Бұл әдіс қаскүнемнің абонентке өзінің хабарламасын қайталап жіберуіне негізделген. Шетел әдебиеттерінде осы топқа кіретін шабуылдарды **reflection** деп атайды.

**Хабарламаның қайталануы.** Қаскүнем бұрын хаттама орындалуы кезінде жіберілген кейбір хабарламалардың жіберілуін қайталауы мүмкін.

**Себепсіз хабарламалардың ашылып кетуі.** Бұл әдістің мәні қаскүнем кейбір автоматты құрылғыларды немесе абонентті белгілі бір әрекеттің тізбегін орындауға мәжбүр ететіндігі болып табылады. Шетел әдебиеттерінде мұндай құрылғылар мен абоненттерді **oracle** деп атайды.

**Хаттаманың параллельді орындалуы.** Формальді хаттамалар талдауы бірнеше сессияда параллельді орындалуының рұқсат етілу мүмкіндігі шешілмейтін көптеген хаттамалар типтері үшін күрделі мәселе болып калады [4].

**Математикалық амалдардың ерекшелігін қолдану.** Шабуылдың бұл типі ақпаратты қамтамасыз ету хаттамаларында қолданылатын криптографиялық алгоритмдердегі нақты математикалық өзгертулерге байланысты.

**Жүйе беделінің түсуі.** Уақыт өте келе барлық жүйенің беделі түсетіндігін болжауға болады. Мұның себебі тек қана техникалық жұмыстың жетілмегендігі емес.

**Кеңейтілген шекті автомат** деп келесі объектілердің жиынтығын айтады [5]  $A = (S, S_0, X, Y, O, \delta, \lambda)$ , мұнда  $S$  – жағдайдың шекті бос емес жиыны;  $S_0 \subset S$  – бастапқы жағдайдағы шекті бос емес жиын;  $X$  – кіріс мәніндегі шекті бос емес жиын;  $Y$  – шығыс мәніндегі шекті бос емес жиын;  $O \subset X, Y$  – синхронды мәнінің бірлік жиыны;  $\delta: S \times X \rightarrow S$  – өту функциясы;  $\lambda: S \times X \rightarrow Y$  – шығу функциясы; Автоматтың әрбір жағдайы белгілі бір жұмыс кезеңінде ақпараттық алмасуды сипаттайды.

#### Әдебиет

1. Klima V, Pokoruy O, Rosa T. Attacking RSA – based Session in SSL/TLS. // Presented at CHRS 2003, September 7-11, Cologne, Germany.
2. Mitchell J, Shmatikov V, Stettin U. Finite-State Analysis of SSL 3.0. In Proc. 7th USENIX Security Symposium, pages 201-215, 1998.
3. Paulson L.C. Inductive analysis of the Internet protocol TLS. // ACM Transactions on Information and System Security, Volume 2, Issue 3, 1999, pp. 332-351.
4. Rabinowitch M, Turant M. Protocol insecurity with finite number of session is NP-complete // in 14 IEEE Computer Security Foundations Workshop, pp. 174-190. IEEE Computer Society, 2001.
5. Карпов Ю.Г. Теория автоматов.- СПб., 2002.

#### Система электронного документооборота в вузе

Галиев Д.С.

Евразийский национальный университет имени Л.Н.Гумилева  
daniyar145@rambler.ru

В современном мире новые технологии поражают нас невероятными изобретениями и возможностями. Каждый новый день мы слышим и читаем, видим и пробуем средства, которые еще вчера казались нереальными. Целый мир лихорадочно изобретает новые решения для автоматизации и эффективности рабочих процессов. Повальный ряд предложений ставит нас в затруднительное положение в выборе оптимального программного обеспечения (ПО).

Моя работа посвящена разработке автоматизированной системы управления документами и данными, которая максимально отвечает требованиям современного ВУЗа.

Неоспорима важность сохранности и умелого использования информационных ресурсов для успешного ведения процесса обучения. Способность принять верное решение и вовремя отреагировать на ситуацию, гибко реагировать на все изменения