

НАУКОВІ ЗАПИСКИ

УКРАЇНСЬКОГО НАУКОВО-ДОСЛІДНОГО ІНСТИТУТУ ЗВ'ЯЗКУ

- *Загальні питання розвитку телекомунікацій*
 - *Інформаційні технології і мережі наступного покоління*
 - *Телекомунікаційні транспортні мережі*
 - *Телекомунікаційні телефонні мережі*
 - *Радіомережі і радіотехнології*
 - *Управління мережами і послугами телекомунікацій*
 - *Технологічні засоби телекомунікацій*
 - *Інфокомунікаційні послуги і якість обслуговування*
 - *Надійність телекомунікаційних мереж і захист інформації*
 - *Проектування, впровадження, виробництво*
 - *Метрологія і стандартизація зв'язку*
 - *Поштовий зв'язок*
 - *Обчислювальна техніка та програмне забезпечення*
 - *Навчальний процес*
-
-

УНДІЗ

№1(9) • 2009

UNDIZ

МІНІСТЕРСТВО ТРАНСПОРТУ ТА ЗВ'ЯЗКУ УКРАЇНИ

ДЕРЖАВНЕ ПІДПРИЄМСТВО «УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ЗВ'ЯЗКУ»

НАУКОВІ ЗАПИСКИ УКРАЇНСЬКОГО НАУКОВО-ДОСЛІДНОГО ІНСТИТУТУ ЗВ'ЯЗКУ Науково-виробничий збірник

Свідоцтво про державну реєстрацію збірника – КВ №12133-1022Р від 26.12.2006 р.
Наукове фахове видання України – Постанова президії ВАК України № 1-05/2 від 13.02.2008 р.

Редакційна колегія:

Головний редактор: *Л.Н. Беркман*, доктор техн. наук, професор, академік Академії зв'язку України, почесний зв'язківець України

Заступники головного редактора: *П.Ф. Баховський*, член-кореспондент Академії зв'язку України; *Г.Ф. Колченко*, кандидат техн. наук, ст. наук. співроб., доцент; *І.В. Шестак*, кандидат техн. наук, доцент

Члени колегії: *Ю.Б. Балтер*, кандидат техн. наук, ст. наук. співроб., почесний радист СРСР, почесний зв'язківець України; *М.Л. Бірюков*, кандидат техн. наук, ст. наук. співроб.; *О.Г. Варфоломєєва*, кандидат техн. наук, ст. наук. співроб., доцент, почесний зв'язківець України; *М.А. Віноградов*, доктор техн. наук, професор, почесний радист СРСР; *В.О. Гребенніков*, кандидат техн. наук, ст. наук. співроб.; *Г.Ф. Зайцев*, доктор техн. наук, професор, Заслужений діяч науки УРСР, лауреат Державної премії України, почесний зв'язківець України; *М.В. Захарченко*, доктор техн. наук, професор, академік Міжнародної академії інформатизації, академік Всесвітньої академії наук комплексної безпеки, академік Академії зв'язку України, Заслужений працівник народної освіти України, майстер зв'язку СРСР, почесний зв'язківець України; *В.Б. Каток*, кандидат техн. наук, доцент; *О.В. Лемешко*, доктор техн. наук, професор; *А.М. Лучук*, доктор техн. наук, професор, Заслужений діяч науки УРСР, лауреат Державної премії України, почесний зв'язківець України; *В.В. Поповський*, доктор техн. наук, професор, академік Академії зв'язку України, академік Академії прикладної радіоелектроніки України; *В.М. Почерняєв*, доктор техн. наук, професор, академік Академії зв'язку України, академік Аерокосмічної академії України; *Ю.Г. Савченко*, доктор техн. наук, професор; *А.І. Семенко*, доктор техн. наук, професор, лауреат Державної премії СРСР; *В.П. Тарасенко*, доктор техн. наук, професор, академік Академії інженерних наук України, Заслужений діяч науки і техніки України, лауреат Державної премії України

Відповідальний редактор: *Я.І. Торошанко*, кандидат техн. наук, ст. наук. співроб.

Науково-технічний редактор з англійської мови: *С.Я. Несвітська*

Стилістичне редагування та коректура: *О.В. Логійко*

№1(9) • 2009

Рекомендовано до друку Науково-технічною радою УНДІЗ (протокол №1 від 17.02.2009 р.)

Адреса редакції: Український НДІ зв'язку. Вул. Солом'янська, 13, м. Київ, 03110
Тел. +38 (044) 248 87 15; Ел. пошта: toroshanko@ukr.net

©Український науково-дослідний інститут зв'язку, 2009

ЗМІСТ

Управління мережами і послугами телекомунікацій	
<i>Поповский В.В., Лемешко А.В., Евсева О.Ю.</i> Динамическое управление ресурсами ТКС: математические модели в пространстве состояний	3
Технологічні засоби і обладнання телекомунікацій	
<i>Яніцький І.Я.</i> Статистична оптимізація точності формувачів періодичних відліків часу з кільцем фазового автопідстроювання ВПС телекомунікаційних мереж.	27
<i>Зайцев Г.Ф., Булгач В.Л., Стась В.В.</i> Показатели качества комбинированной системы фазовой автоподстройки	36
Радиомережі і радіотехнології	
<i>Урывский Л.А., Прокопенко Е.А.</i> Зависимость пропускной способности дискретного канала связи от его энергетического потенциала при использовании многопозиционных сигналов	41
Надійність телекомунікаційних мереж і захист інформації	
<i>Холявкина Т.В.</i> Интегрированная система сбора и обработки информации в распределенной системе анализа безопасности полетов	51
Інфокомунікаційні послуги і якість обслуговування	
<i>Савченко А.С., Чанг Шу.</i> Адаптивное формирование трафика путем управления частотой генератора маркеров	58
<i>Павлов С.В.</i> Снижение размерности параметров предоставления инфокоммуникационных услуг методом факторного анализа	65
Загальні питання розвитку телекомунікацій	
<i>Шмелёва Т.Р.</i> Параметрическая модель IP-сетей в форме раскрашенных сетей Петри	70
Проектування, впровадження, виробництво	
<i>Сундучков К.С., Яландин П.Н., Шестак В.И.</i> Интеллектуальная составляющая интерактивной гетерогенной телекоммуникационной сети	78
<i>Маишталер И.Я.</i> Выбор архитектуры телекоммуникационной среды информационно-аналитической системы мониторинга динамических объектов.	86
<i>Алексеев М.О.</i> Створення єдиного інформаційного середовища вищого навчального закладу.	95
<i>Макаренко А.О.</i> Використання графічного програмування для створення керуючих програм	100
Автори випуску	106
К 100-летию со дня рождения Льва Исааковича Ярославского	108

УДК 629.735.051:004.7(043.3)

Холявкина Т.В., аспірант

ИНТЕГРИРОВАННАЯ СИСТЕМА СБОРА И ОБРАБОТКИ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ АНАЛИЗА БЕЗОПАСНОСТИ ПОЛЕТОВ

Холявкина Т.В. Интегрована система збору і обробки інформації в розподіленій системі аналізу безпеки польотів. У статті розглянуто задачу побудови розподіленої інформаційно-обчислювальної системи аналізу і обробки інформації про безпеку польотів державної авіаційної адміністрації (державіаслужби). Розглянуті взаємозв'язані аспекти досягнення необхідної якості функціонування системи: захист від несанкціонованого доступу і забезпечення умов функціонування в реальному масштабі часу. Для вирішення першої задачі запропоновано ешелоновану систему захисту з наростаючою складністю подолання кожного рубежу. Для вирішення другої задачі запропонований алгоритм послідовної багаторівневої оптимізації запитів в розподіленій базі даних.

Холявкина Т.В. Интегрированная система сбора и обработки информации в распределенной системе анализа безопасности полетов. В статье рассмотрена задача построения распределенной информационно-вычислительной системы анализа и обработки информации о безопасности полетов государственной авиационной администрации (госавиаслужбы). Рассмотрены взаимосвязанные аспекты достижения требуемого качества функционирования системы: защита от несанкционированного доступа и обеспечение условий функционирования в реальном масштабе времени. Для решения первой задачи предложена эшелонированная система защиты с нарастающей сложностью преодоления каждого рубежа. Для решения второй задачи предложен алгоритм последовательной многоуровневой оптимизации запросов в распределенной базе данных.

Kholyavkina T.V. Integrated data acquisition and processing system in the distributed flight safety analysis system. This paper considers the construction problem of distributed computing and information system for analysis and processing of information about flight safety of state aviation administration (state aviation service). It considers an interrelated aspects of obtaining the required quality of the system operation: non-authorized access protection and arrangement of conditions of real time operation. In order to solve the former problem it is proposed the separated protection system with the growing complexity of each border overcoming. To solve the latter problem it is proposea an algorithm of successive multilevel optimization of queries in the distributed data base.

Ключевые слова: ОБРАБОТКА ИНФОРМАЦИИ, БЕЗОПАСНОСТЬ ПОЛЕТОВ, ЗАЩИТА ИНФОРМАЦИИ, ОПТИМИЗАЦИЯ ЗАПРОСОВ, БАЗА ДАННЫХ

В соответствии с требованиями ИКАО, которые изложены в дополнении к Чикагской конвенции (Дополнение Е от 03.03.2006 р.), защита информации о безопасности полетов (БП) от ненадлежащего использования является важным элементом обеспечения постоянного доступа к ней. Использование этой информации в других целях, кроме обеспечения безопасности полетов, может осложнить получение такой информации в будущем с негативными последствиями для решения задач БП.

Запрещение ненадлежащего использования означает, что не допускается использование информации о БП для целей, отличающихся от тех, для которых она собиралась, таких, как использование информации для дисциплинарного, гражданского, административного и криминального разбора по отношению к эксплуатационному персоналу и/или предание гласности этой информации.

В соответствии с рекомендациями ИКАО основным принципом защиты информации является определение того, что:

а) единственной целью защиты информации о безопасности полетов от ненадлежащего использования является обеспечение доступа к ней, гарантирующего возможность принятия соответствующих и своевременных превентивных мер по повышению уровня безопасности полетов;

б) защита информации о безопасности полетов не ставит своей целью вмешательство в процесс должного осуществления правосудия;

в) защита конфиденциальной информации о безопасности полетов с учетом конкретных условий является составной частью обязательства государства относительно обеспечения безопасности полетов;

г) информацию о безопасности полетов не следует использовать в других целях, кроме тех, для которых она собиралась;

д) с целью дисциплинарного, гражданского, административного и уголовного разбора информация о безопасности полетов должна использоваться лишь при наличии соответствующих гарантий, предусмотренных действующим законодательством Украины.

Должностные лица, ответственные за хранение информации о безопасности полетов, обязаны обеспечивать все виды возможной защиты от раскрытия информации.

По требованиям директивы Европарламента 2003/42/ЕС от 13.06.2003г. приемлемый уровень БП не может быть достигнут при малой информативности системы сообщений, реализуемой каждым государством-членом в отдельности. Поэтому:

– Государства-члены назначают одну или несколько компетентных администраций для запуска механизма сбора, оценки, обработки и хранения поступающих от них сообщений об опасных событиях;

– компетентная администрация сохраняет собранные сообщения в базе данных;

– информация о серьезных инцидентах и авиационных событиях (происшествиях) должна также сохраняться в этой базе данных.

Основываясь на "Положении о системе управления безопасностью полетов на авиационном транспорте", госавиаслужба (ГАС) создает базу данных безопасности полетов (БД БП) с целью эффективного анализа полученной информации, в том числе по результатам расследования авиационных событий и добровольных извещений об опасных факторах, и разработках профилактических мероприятий (п.7.3.11).

Концептуальная схема БД БП изображена на рис. 1.

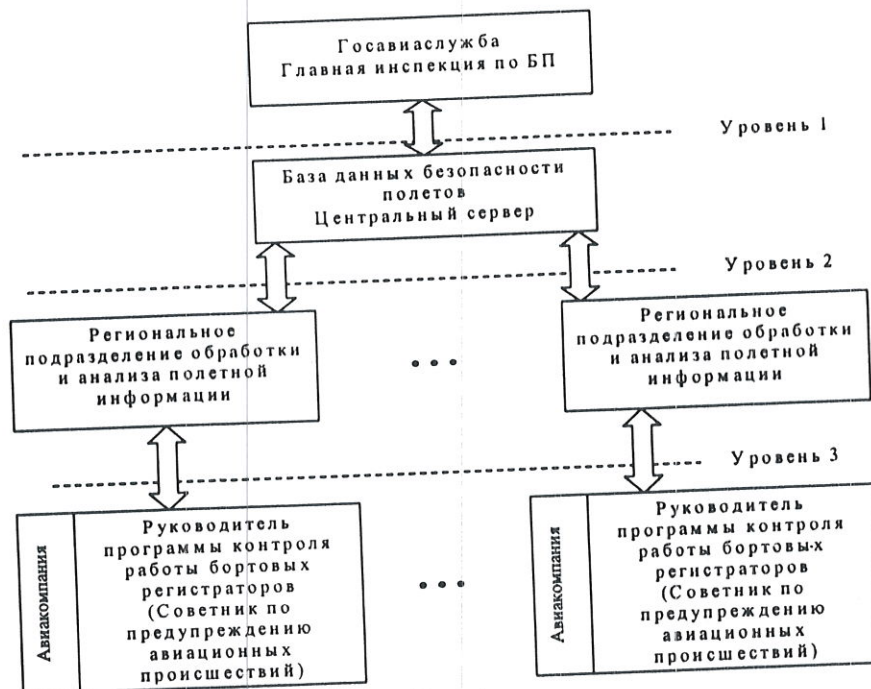


Рис. 1.

По своей организации она является многоуровневой (иерархической):

- БД госавиаслужбы (госавиаадминистрации);
- БД региональных подразделений;
- БД авиакомпаний.

Запросы в БД БП направляются как сверху вниз, так и снизу вверх. Запросы "сверху вниз" – это, как правило, запросы с целью получения информации о вновь происшедших событиях. Эти запросы поступают во все авиакомпании с периодичностью, которая

определяется ГАС. Ответы на запросы обрабатываются в центральном сервере БД БП.

Запросы “снизу вверх” – это, с одной стороны, запросы авиакомпаний о текущем состоянии проблемы безопасности полетов в регионе, стране и мире. С другой стороны – это запросы на размещение и обработку информации об экстремальных событиях: летных происшествиях и предпосылках к ним, серьезных инцидентах в воздухе и на земле, и, конечно, об авариях и катастрофах. Запросы на передачу данных об экстремальных событиях, по определению, передаются и обрабатываются с высшим приоритетом.

По своему типу БД БП является распределенной реляционной базой данных и знаний со всеми вытекающими из этого требованиями:

- оптимальное распределение информации между центральным сервером, региональными подразделениями и авиакомпаниями;
- оптимизация планов выполнения запросов;
- обеспечение требуемого качества сервиса (в первую очередь – достоверности передачи данных);
- обеспечение защиты сети от несанкционированного доступа (НСД).

Очевидно, две последние задачи являются взаимосвязанными. БД БП является структурой критичного применения по требованиям работы в реальном масштабе времени и по соображениям безопасности и защиты информации. Утрата, модификация или другие нарушения целостности информации могут повлечь серьезные и непредсказуемые последствия, вплоть до нарушения работы всей авиационной транспортной инфраструктуры.

Учитывая выше сказанное, для эффективного функционирования БД БП, помимо применения высоконадежного оборудования, необходимо обеспечить защиту сетей передачи данных (СПД) от угроз самой различной природы, как техногенных и природных, так и из-за человеческого фактора. Восстановление поврежденного оборудования сопряжено с большими материальными и временными затратами. Требуется с высокой точностью определить место и характер повреждения, внести соответствующие изменения в трафик, топологию и алгоритмы работы узлов сети на период ее восстановления, отремонтировать поврежденные участки и узлы сети. В некоторых случаях расходы на восстановление оборудования могут оказаться значительно меньше убытков из-за простоя участка сети.

Поэтому задача комплексной защиты информации о БП является чрезвычайно актуальной.

Нагрузка на сеть является случайной и меняется в широких пределах в зависимости от времени интенсивности обмена информацией в штатных и экстремальных ситуациях и других условий. Информация о состоянии сети, как правило, не обладает требуемой полнотой и достоверностью. Состав и характеристики оборудования сети также известны не полностью. Поэтому для анализа сети в целом и ее отдельных фрагментов необходимо использовать стохастический подход. При этом во многих задачах фильтрации и управления в системах со случайными параметрами и структурой можно ограничиться гауссовым приближением, что практически основывается на эффекте нормализации законов распределения в сложных (больших) системах [1]. Это также облегчает анализ.

Таким образом, сеть можно рассматривать как гетерогенную, нестационарную стохастическую структуру с гауссовскими распределениями параметров.

При наличии систем защиты процесс взаимодействия объекта сети и субъекта, делающего попытку проникновения (взлома, несанкционированного доступа - НСД), будем рассматривать как конфликт между двумя противниками:

первый – большая человеко-машинная система защиты, которая обслуживает множество защищаемых объектов сети;

второй – субъект-злоумышленник (в дальнейшем для краткости будем называть его просто субъектом или противником) достаточно высокой квалификации, вооруженный соответствующими техническими средствами.

В соответствии с классической теорией конфликта [2] взаимодействие между

рассматриваемыми сторонами можно классифицировать как антагонизм с возможным переходом в строгое соперничество, а если в процессе взаимодействия эффективность второй стороны уменьшается быстрее, чем эффективность первой, возможен переход в нестрогое соперничество.

Дадим краткую характеристику наиболее вероятных экстремальных состояний сети.

1. Попытка НСД с целью хищения или совершения акта вандализма. Эффект проявляется сразу; основные задачи – обнаружение и распознавание для исключения других состояний (отказ оборудования, природные факторы – молния, подтопление, сдвиг почвенных слоев, ураган и т.д.). Необходима немедленная реакция, требуется определенное время на нейтрализацию. На время локализации попытки НСД необходима перемаршрутизация транспортной подсистемы БД БП.

2. Попытка НСД с целью съема информации. Внешние эффекты могут отсутствовать. Основная задача – идентификация – вычисление противника по характеру последствий, на что требуется время, иногда длительное.

3. Внезапный отказ оборудования. Проявляется сразу – возникает задача локализации отказавшего устройства (узла, блока). Требуется определенное время на восстановление.

4. Постепенный отказ оборудования: плавное увеличение числа ошибок, сбоев вплоть до критического значения – полный отказ. Необходим постоянный анализ состояния сети. При стабильном росте числа ошибок – локализация критического устройства, перемаршрутизация трафика.

5. Перегрузка сети – увеличение задержки передачи информации выше допустимой, перемаршрутизация трафика.

6. Другие экстремальные ситуации, например, из-за человеческого фактора (низкая квалификация или утрата лояльности персонала), из-за стихийных бедствий, актов терроризма, не направленных специально против информационно-телекоммуникационных сетей, и т.д.

Рассмотрим задачу многоуровневой защиты СПД от попыток несанкционированного доступа того или иного типа.

Предположим, что защищаемый объект D_d находится внутри N защищенных сооружений (экранов). При этом выполняются следующие условия:

1. Каждый защитный экран является замкнутым. Его нельзя обойти, а можно только преодолеть (вскрыть).

2. Экраны вложены друг в друга по принципу матрешки. Защищаемый объект находится внутри последнего (внутреннего) экрана. Таким образом, для проникновения внутрь объекта необходимо последовательно вскрыть все N экранов, от первого (внешнего) до N -го (внутреннего).

Если рассматривать процесс преодоления i -го экрана как обслуживание некой заявки, то в соответствии с классической задачей теории массового обслуживания [3] длительность обслуживания t_{pi} есть случайная величина с показательным распределением плотности вероятности:

$$\begin{aligned} W_1(t_{pi}) &= \gamma_i \exp(-\gamma_i t_{pi}) \quad \text{при } t_{pi} > 0 \\ W_1(t_{pi}) &= 0 \quad \text{при } t_{pi} < 0 \end{aligned} \quad (1)$$

где $\gamma_i > 0$ – постоянная величина; или же с распределением плотности вероятности Эрланга:

$$\begin{aligned} W_1(t_{pi}) &= \gamma_i \frac{(\gamma_i t_{pi})^{k-1}}{(k-1)!} \exp(-\gamma_i t_{pi}) \quad \text{при } t_{pi} > 0 \\ W_1(t_{pi}) &= 0 \quad \text{при } t_{pi} < 0 \end{aligned} \quad (2)$$

где $\gamma_i > 0$ – постоянная величина; k – целое положительное число.

Обозначим среднее время преодоления i -го экрана через T_{pi} .

Для распределения (1)
$$T_{pi1} = \frac{1}{\gamma_i}, \quad (3)$$

а для распределения (2)
$$T_{pi2} = \frac{k}{\gamma_i}. \quad (4)$$

Постоянная γ_i есть функция стойкости i -го рубежа защиты и квалификации субъекта.

Выражения (3...4) можно использовать для оценки параметра γ_i по экспериментальным данным.

Поставим следующие условия:

$$T_{p1j} < T_{p2j} \dots < T_{p,N-1,j} < T_{pNj}, \quad j = 1, 2, \quad (5)$$

$$\sum_{i=1}^N T_{pij} > T_r \text{ с вероятностью } P_r \geq P_{r\min}, \quad (6)$$

где T_r - время реакции на попытку НСД;

$P_{r\min}$ - предельно допустимая (минимальная) вероятность выполнения условия (6).

Условием (5) определяется требование нарастающей сложности преодоления рубежей защиты от первого до последнего.

При выполнении условия (6) гарантируется своевременность реакции на попытку проникновения и ее нейтрализации с вероятностью не ниже предельно допустимой.

Эти условия фактически лежат в основе теории рубежей защиты объекта – транспортной сети, по которой осуществляется передача данных БД БП.

Управление БД БП, как и любой автоматизированной (большой) системой, невозможно без обратной связи. По каналам обратной связи поступают данные о внутреннем состоянии БД БП и ситуации, складывающейся на каждом периферийном объекте. Как отмечалось выше, эти данные регистрируются, анализируются и обрабатываются в корпоративной информационной системе - базе данных и знаний. Источники данных организационно и территориально распределены, а сами данные разнородны. В то же время правила доступа к данным должны быть единообразными, а процедуры доступа должны выполняться в реальном или квазиреальном масштабах времени. (Под квазиреальным масштабом времени мы понимаем работу при наличии задержек, не фиксируемых оператором и не приводящих к парализации БД БП.)

Для эффективного мониторинга состояния сети целесообразно использовать распределенную базу данных и защиты (БДЗ) с реляционной системой управления (СУБД).

На рис. 2 изображена обобщенная структурная схема системы сбора и обработки информации об экстремальных состояниях региональной сети. Важной особенностью ее является наличие подсистемы обработки – распознавание типов экстремальных ситуаций. Обработка осуществляется в региональной БДЗ. Периферийные БД играют роль промежуточных накопителей.

В работе [4] предлагается для упрощения модернизации и наращивания БД БП, подключение новых объектов использовать СУБД типа MS SQL Server с языком запросов SQL. В работах [4, 5] отмечаются преимущества использования SQL в качестве стандартного языка запросов, в первую очередь, его статус в качестве общепринятого стандарта. Кроме того, в настоящее время разработаны методы преобразования запросов на языке SQL и алгебраической форме. Это позволяет использовать реляционную алгебру в качестве унифицированного интерфейса реляционной СУБД и упростить задачу оптимизации плана выполнения запроса.

Как видно из рис. 2, система имеет структуру типа «виртуальной звезды» [5]: как центральная таблица БДЗ, так и периферийные таблицы БД каждого из фрагментов являются переменными. Они, во-первых, оперативно создаются и заполняются данными, поступающими от элементов БД БП.

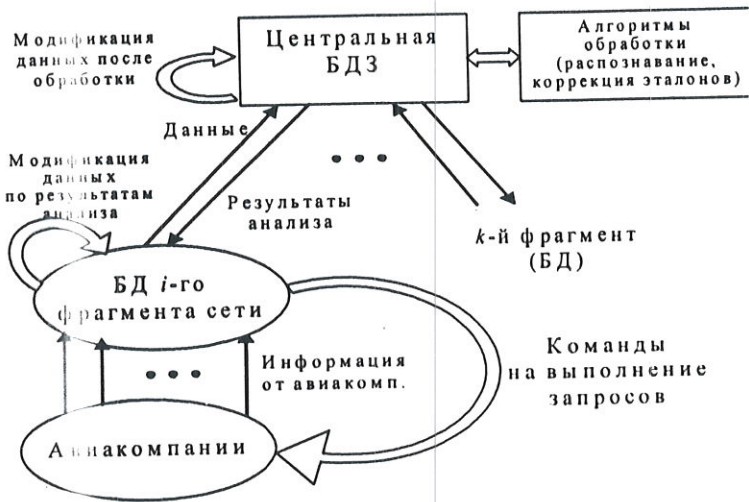


Рис.2.

В процессе доступа к БД запрос формируется на соответствующем языке (в нашем случае SQL). Затем он подвергается лексическому и синтаксическому анализу. В результате вырабатывается его внутреннее представление, и запрос преобразуется в алгебраическую форму. Дальнейшие этапы оптимизации плана и выполнения запроса уже выполняются с использованием алгебраической формы. Как отмечалось ранее, при этом упрощаются задачи оптимизации и вообще функционирования распределенной БД благодаря унификации и относительной простоте языка реляционной алгебры. Облегчается также решение задач построения оптимизаторов с гибкой структурой. Благодаря частичной децентрализации и модульной архитектуре БД системы сбора и анализа информации задача модификации БД БП также упрощается: при изменениях параметров и структуры данных БД i -го фрагмента не потребуется выносить изменения в БД j -го фрагмента.

Выводы. 1. При организации распределенной базы данных безопасности полетов возникают две связанные между собой задачи: обеспечение передачи данных с требуемым качеством и достоверностью и защита от несанкционированного доступа. Поэтому данные задачи необходимо решать в комплексе.

2. В работе предложена модифицированная модель рубежей защиты на основе вложенных экранов. Только после преодоления всех рубежей злоумышленник может проникнуть внутрь БД БП. При этом поставлено условие гарантированной локализации попытки НСД за время преодоления всех рубежей защиты.

3. Для построения защищенной и при этом достаточно быстродействующей системы обмена информацией на основе распределенной БД и З необходимо оптимизировать как структуру собственно БД, так и структуру запросов, циркулирующих сверху вниз и снизу вверх. Такой алгоритм предложен в работе.

4. В дальнейшем целесообразно рассмотреть задачу транспорта данных внутри БД БП на основе виртуальной частной сети. Нам представляется, что для системы критичного применения, каковой является государственная БД БП, такой подход обеспечит как требуемые быстродействие и достоверность, так и степень защиты данных.

Литература

1. Казаков И.Е. Статистическая динамика систем с переменной структурой. – М.: «Наука», 1977. – 416 с.

Во-вторых, по результатам обработки в соответствии с заложенными алгоритмами осуществляется модернизация этих таблиц. Команды на выполнение защитных действий могут генерироваться автоматически. Однако ЛПР – оператор центра сбора информации – всегда может принять свое решение и дать приоритетную команду на БД БП [4].

В соответствии с предложенными структурой и параметрами БДЗ составлен алгоритм обработки запросов с оптимизацией плана выполнения запроса (рис.3).

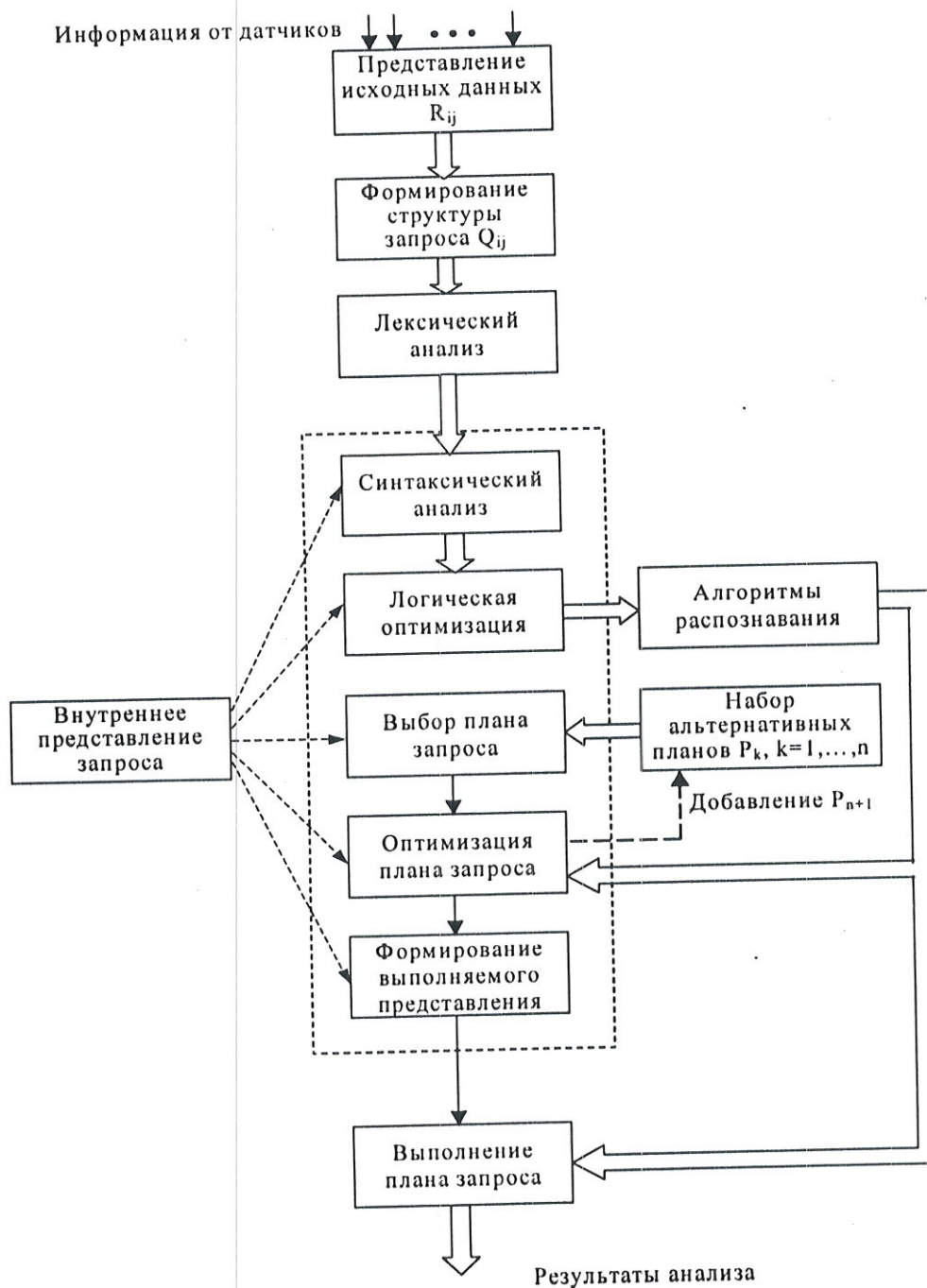


Рис.3.

2. Дружинин В.В., Конторов Д.С., Конторов М.Д. Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.
3. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания, 2-е изд. – М.: Наука, 1987. – 336 с.
4. Кузнецов С. Методы оптимизации выполнения запросов в реляционных СУБД // Центр Информационных Технологий, http://www.citforum.ru/database/articles/art_26.shtml
5. Коровкин С.Д., Левенец И.А., Ратманова И.Д., Старых В.А., Щавелёв Л.В. Решение проблемы комплексного оперативного анализа информации хранилищ данных // Центр Информационных Технологий, http://www.citforum.ru/database/articles/art_11.shtml

Стась Володимир Володимирович, ТОВ «Мікроком», аспірант каф. радіотехнологій
Держ. унів-ту інформ.-комунікац. технологій
Тел.: +380 67 401 99 14. E-mail: vadim@microcom.com.ua

Сундучков Костянтин Станіславович, проф., д.т.н., Лауреат Держ. премії УРСР з науки і
техніки, заст. директора з наукових питань інституту телекомунікац. систем Національного
технічного унів-ту України «Київський політехнічний інститут»
Тел.: +380 67 227 70 54. E-mail: sunduchkov@its.ntu-kpi.ua

Уривський Леонід Олександрович, к.т.н., доц., каф. телекомунікац. систем інституту
телекомунікац. систем Національного технічного унів-ту України «Київський політехнічний
інститут»
Тел.: +380 97 317 17 58; E-mail: leonid_uic@ukr.net

Холявкіна Тетяна Володимирівна, аспірант, асистент кафедри комп'ютерних
інформаційних технологій Національного авіаційного унів-ту
Тел. +380 67 939 01 12; E - mail : t.holyavkina@mail.ru

Шестак Василь Ігоревич, магістрант інституту телекомунікац. систем Національного
технічного унів-ту України «Київський політехнічний інститут»
Тел.: +380 68 709 5101

Шмельова Тетяна Рудольфівна, к.т.н., ст. викладач каф. мереж зв'язку Одеської
національної академії зв'язку ім. О.С. Попова
Тел.: +380 48 7158383, +380 482 348535. E - mail: tishtri@rambler.ru

Чанг Шу, аспірантка каф. комп'ютерних інформаційних технологій Національного
авіаційного унів-ту
Тел.: + 380 44 406-76-49

Яландін Павло Миколайович, аспірант Держ. унів-ту інформ.-комунікац. технологій
Тел.: +380 99 613 86 86. E-mail: DeveloperUA@ukr.net

Яніцький Іван Ярославович, аспірант Держ. унів-ту інформ.-комунікац. технологій
Тел. +380 44 249 25 35. E-mail: kafrfm@ukr.net