ОБЕСПЕЧЕНИЕ ПРАВ ДОСТУПА К СИСТЕМАМ С МАНДАТНОЙ ПОЛИТИКОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С. П. Соколова[1], **Е. В. Г**ОРКОВЕНКО[2]

[1]Санкт-Петербургский институт информатики и автоматизации РАН,
[2]Институт проблем информатики и управления МОН РК

[1]СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178;
[2]ИПИУМОНРК, ул. Богенбай батыра, 221, Алматы, Республика Казахстан, 050026

[1]<sokolova_sv@mail.ru>, [2]< gev@ipic.kz>

УДК 004.056.52
Соколова С. П., Горковенко Е. В. **Обеспечение прав доступа к системам с мандатной политикой информационной безопасности.** // Труды СПИИРАН. Вып. 7, т. 2. — СПб.: Наука, 2008.
Аннотация. *Представлены механизмы защиты информации от несанкционированного доступа путем ограничения доступа к распределенным информационным ресурсам с учетом мандатной политики информационной безопасности. Формализованы процессы контроля и анализа свойств матрицы прав доступа с учетом иерархии субъектов и объектов защиты. Рассмотрены условия и процедуры заполнения и формирования этой матрицы при выполнении основных правил разграничения доступа.* — **Библ. 11 назв.**
UDC 004.056.52
Sokolova S. P.,Gorkovenko E. V. **Protection of access rights to the systems with mandate politics of information security.** // SPIIRAS Proceedings. Issue 7, vol. 2. — SPb.: Nauka, 2008.
Abstract. *The machinery of information protections from unauthorized access by access limitation of the corporative information recourses according to the mandate politics of information security have considered. The processes of control and properties analysis of law access matrix according to objects and subjects protection hierarchy have presented. The conditions and procedures of filling and forming of this matrix with execution of basic demarcation access rules have considered.* — **Bibl. 11 items.**

1. Введение

Основой для организации процесса защиты информации является политика безопасности информационно-вычислительной системы (ИВС). Эта политика формируется с целью определения потенциальных угроз и выбора механизмов защиты от них. В системах, основанных на политиках безопасности, актуальной задачей является обнаружение и разрешение противоречий в реализованных политиках, их верификация [1, 2].

При выборе механизмов защиты информации основное внимание уделяется организации эффективного и безопасного доступа к информационным ресурсам с учетом полномочий пользователей и условиями обработки и хранения данных. В информационных системах, в которых хранится и обрабатывается критичная информация, политика безопасности основывается на многоуровневой политике безопасности, базирующейся на проверке полномочий и проверке подлинности и принятой всеми развитыми государствами мира. Нормативная политика безопасности основана на степени доверия пользователя и классификации данных по степени секретности и применяется ко всем пользователям системы. В соответствии с [3] мандатное управление доступа, реализующее полномочную (нормативную) политику безопасности, заключается в разграничении прав доступа субъектов к объектам на основе официального разрешения (допуска) субъектов обращаться к информации такого уровня конфиденциальности. Мандатный контроль доступа включает в себя механизмы разграничения доступа к информации, которые делятся на процедуры, реализующие правила

доступа к информации (чтение, запись, дополнение и т.д.), и на процедуры управления правами (владение, создание, удаление и т.д.).

В статье представлена структура и математическое обеспечение системы с мандатной политикой информационной безопасности, которая имеет модульную структуру и включает следующие подсистемы:

- мандатного разграничения доступа к информации для систем управления с древовидной структурой субъектов и объектов защиты информации различной степени конфиденциальности;
- мониторинга информационной безопасности.

Эта система построена таким образом, чтобы в течение всего времени ее функционирования ни один пользователь не получил возможности обращаться к информации, первоначально принадлежащей владельцу с более высокой категорией допуска и имеющей несравнимый уровень секретности по отношению к уровню допуска пользователя. При попытке различных типов несанкционированного доступа к информационным ресурсам система реагирует на неавторизованных пользователей, на нарушения основных правил доступа и условий контроля доступа.

Рассмотрим функциональное назначение вышеперечисленных подсистем.

2. Подсистема мандатного разграничения доступа

Рассматриваемая подсистема обеспечивает многоуровневую защиту от несанкционированного доступа с выполнением следующего основного правила доступа:

- не позволяющего субъекту получить или записать информацию от субъекта или объекта с более высоким уровнем защиты;
- не позволяющего субъекту получить информацию от объекта при отсутствии права допуска на реализации текущего запроса.

Как известно, к настоящему времени разработано значительное количество моделей обеспечения секретности информационных ресурсов за счет управления контролем доступа через реализацию избирательной или полномочной политик безопасности. Наиболее распространенными являются модели:

- дискреционного управления доступом, реализующего избирательную политику, в рамках которой осуществляется разграничение доступа между поименованными субъектами и поименованными объектами в соответствии с правами доступа субъектов к объектам на основании правил, определенных конкретной дискреционной моделью [3]. При этом для формирования матрицы доступа могут быть использованы механизмы модели Харрисона, Руззо и Ульмана или модели Take Grant;
- мандатного управления доступом, реализующего полномочную политику безопасности через разграничение доступа субъектов к объектам на основе метки конфиденциальности информации, содержащейся в объектах, и официального разрешения (допуска) субъектов обращаться к информации такого уровня конфиденциальности [3]. Классическая модель мандатного управления доступом Белла—Лападула формально записана в терминах теории отношений и при управлении доступом учитывает упорядоченность субъектов и объектов в соответствии с их уровнем безопасности. Состояние системы изменяется согласно правилам трансформации состояний.

Однако, несмотря на все достоинства модели Белла—Лападула, при ее использовании возникает ряд технических трудностей, таких как определение статуса удаленного чтения; определение прав доступа доверенного объекта типа «администратор»; несанкционированная «деклассификация» объекта за-

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

щиты с понижением степени секретности информации. Распространенные интерпретации классической трактовки этой модели страдают по крайней мере двумя существенными недостатками: они не адекватны принятым в стране процедурам обработки секретной информации и не заботятся о достоверности и защите ядра системы - матрицы разграничения доступа.

В представленной ниже модели мандатного разграничения доступа учтены эти недостатки [4, 5].

Основными элементами математической модели $EG = \{S, O, L, A, M, B, R\}$ являются: множество субъектов S; множество объектов O; множество уровней защиты L; множество видов доступа и управления ими A; матрица прав доступа M; список текущего доступа B; список запросов R.

Множество $S = \{s_j, j = 1,\ldots,m\}$ — конечное, упорядоченное множество субъектов защиты, наделенное структурой дерева. Каждому субъекту s_j соответствует список субъектов, непосредственно следующих за ним, т.е. $\forall s_j, \exists H(s_j) = \{s_{ji}, i = 1,\ldots,e\}$ — множество «сыновей» субъекта. Если субъект $s_j \in S$ отличен от корня дерева s_k, ему соответствует единственный субъект $F(s_j)$, непосредственно предшествующий этому субъекту s_j: $\forall s_j, j \neq k, \exists s_k = F(s_j)$ — «отец» субъекта s_j. Каждому субъекту s_j приписывается определенный уровень защиты $J(s_j), j \in J$, остающийся неизменным во время функционирования системы и сохранения статуса субъекта, где $J = \{j_l, l = 1,\ldots,L\}$ — множество уровней защиты. Каждый элемент множества $s_j \in S$ представляется парой $\{\lambda_j, \mu_j\}$, где $\{\lambda_j\}$ — конечное множество классификаций статуса субъектов, $\{\mu_j\}$ — конечное множество категорий допуска. Будем рассматривать множество S как объединение двух подмножеств $S^{(1)}$, $S^{(2)}$: $S = S^{(1)} \cup S^{(2)}$, где $S^{(1)}$ — подмножество субъектов (владельцы объектов), имеющих право подписи документов, право переписки, право на разрешение доступа к объектам и право ликвидации доступа; $S^{(2)}$ — подмножество субъектов, не имеющих вышеперечисленных прав, но имеющих право редактирования и чтения документов.

Владелец объекта — это субъект, который его создал, и он, естественно, может передавать другим субъектам права на доступ к этому объекту. При использовании концепции владельца каждый объект ассоциируется с владельцем (единственным пользователем), имеющим полномочия *контроля доступа* к объекту. Владелец полностью контролирует созданный им объект и не может передавать *полномочия контроля* другому субъекту, но может изменить права доступа с целью разрешения или запрета доступа к контролируемому объекту другим субъектам. Данная политика управления доступом отвечает требованиям многоуровневого контроля доступа и проводится в жизнь администратором безопасности системы.

Множество $O = \{o_j, j = 1,\ldots,n\}$ — конечное множество объектов защиты, также наделенное структурой дерева и сгруппированное по типам $C(o_j) = \{c_q, q = 1,\ldots,Q\}$, где Q — количество типов объектов защиты. Каждому объекту $o_j \in O$ присваивается уровень защиты объекта $J(o_j)$, который соответ-

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ствует уровню секретности информации $l_n \in L$, хранящейся в объекте o_j (файл) или к которой обращается объект o_n (программа). Под уровнем секретности понимается иерархический атрибут в соответствии с градациями: «особой важности», «совершенно секретно», «секретно», «ДСП», «конфиденциально», «персональные данные», «для общего пользования» и т.д. Этот атрибут ассоциирован с сущностью компьютерной системы для обозначения степени ее критичности: $\{l_\omega, \omega = 1,\ldots,\Omega : l_1 > l_2 > \ldots > l_\Omega\}$. Множество L изоморфно множеству категорий допуска, т.е. $\{l_i\} \to \{\mu_j\}$. Каждый объект $o_l \in O$ определяется парой $\{s_j^*, l_i^*\}$, где $\{s_j^*\}$ — множество субъектов-владельцев объектов o_l; $\{l_i^*\}$ — множество степеней секретности.

Множество видов доступа субъектов к объектам защиты и управления правами доступа $A = \{a_k, k = 1,\ldots,K\}$ представлено в виде: $A = A^{(1)} \cup A^{(2)}$.

Подмножество $A^{(1)} = \{RD, G, D, W, E, OT\}$ включает следующие элементы: RD — чтение; G — перезапись информации из объекта в объект; D — добавление информации в объект, без предварительного чтения; W — запись после предварительного чтения; E — исполнение команды; OT — отказ в выполнении запроса.

Подмножество $A^{(2)} = \{CR, U, LU, P, PV, I, PR, CP, KL, Y\}$ состоит из элементов: CR — создание объекта, U — уничтожение объекта, LU — лишения прав на доступ, P — право передачи прав между субъектами, PV — наделение правом владения объектом, I — изменение уровня защиты, PR — право порождения объекта, CP — копирование, KL — право классификации объектов, Y — разрешение на реализацию запроса.

Матрица прав доступа $M = \{m_{ij}, i = 1,\ldots,n^*, j = 1,\ldots,m^*\}$ содержит список видов доступа субъекта $s_i \in S$ к объекту $o_j \in O$, на которые он может претендовать и которые ему в данный момент разрешены. Каждый элемент m_{ij} матрицы прав доступа M представляет особый кортеж $(s_\nu, a_1, a_2, \ldots, a_n)$, где $s_\nu \in S^{(1)}$ — шифр субъекта, разрешившего субъекту s_ν доступы $a_1, a_2, \ldots, a_n$ к объекту o_j.

Список текущего доступа $B = \{b_t, t = 1,\ldots,T\}$ описывает разрешенный в данный момент доступ субъектов к объектам $b_t = (s_j, o_j, a_k)$, $a_k \in A, t = 1,\ldots,T$, и это разрешение к настоящему моменту не отменено, т.е. разрешено право «реализация запроса»; T — количество разрешенных доступов к информационным ресурсам ИВС в текущий момент времени. Разрешение действует до тех пор, пока субъект не обратится с запросом об отказе доступа.

Список запросов $R = \{r_n, n = 1,\ldots,N\}, R \subseteq A,$ содержит запросы всех видов доступа в множестве видов доступа: виды доступа субъектов к объектам, создания и уничтожения объектов, передачи и лишения прав доступа, а также отказ от доступа. Разрешение запроса вызывает изменение состояния вычислительной системы только в том случае, если при обращении к объекту o_j с уровнем защиты $J(o_j)$ субъект o_j не только имеет классификацию не ниже, чем объект защиты $J(s_j) \geq J(o_j)$, и соответствующую категорию допуска μ_j, но имеет право на реализации своего запроса.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Чтобы администратор безопасности смог задать права доступа субъектов к объектам защиты, зафиксировав их в матрице прав доступа, необходимо заполнить формы спецификаций на основе результатов предварительного обследования предметной области пользователей и требований безопасности, зафиксированных в политике безопасности предприятия. Выделенные объекты и субъекты защиты определяются параметрами, характеризующими выбранную систему разграничения доступа. В спецификацию субъекта защиты входят параметры, идентифицирующие субъект и определяющие его категорию допуска, классификацию статуса субъектов (куратор, руководитель, исполнитель, гость и пр.), право владения объектами защиты, право порождения субъектов и объектов («отец», «сын»), правила выбора и защиты идентификатора субъекта. В спецификацию объекта защиты входят параметры, идентифицирующие объект и определяющие его тип группы (файлы, директории, процедуры); степень секретности информации; идентификатор субъекта-владельца; место и способы хранения информации; статус объекта (первичный, вторичный, порожденный).

Процесс обращения к матрице прав доступа как ядру многоуровневой системы защиты с мандатным контролем доступа связан с выполнением таких процедур, как

- задание условий и видов доступа к данным различной степени секретности;
- задание правил управления правами доступа;
- анализ заполнения матрицы доступа с учетом выполнения основного правила доступа;
- реализация права владения и права порождения с учетом иерархии субъектов и объектов защиты;
- контроль выполнения текущего запроса с учетом выполнения основного правила доступа;
- защита матрицы доступа от попыток несанкционированной модификации.

Утвержденные спецификации на обработку данных пользователями в соответствии с их функциональными обязанностями формируются на этапе определения требований защиты к ИВС. Затем проверяется полнота описания характеристик выделенных объектов и субъектов защиты. Если спецификации на пару «субъект — объект» неполные, заполнение матрицы прекращается до полного описания характеристик пары. При задании полного списка разрешенных запросов к паре «субъект — объект» обязательно указывается право реализации по каждому запросу (разрешено, не разрешено).

Первоначальное заполнение матрицы прав доступа начинается с тех субъектов, чья классификация имеет наибольший статус, например «руководитель проекта». Затем вносятся требования субъектов, чей статус ниже, например «ответственный исполнитель». Если имела место последовательность передачи прав доступа: $\lambda_v > \lambda_{j1} > \lambda_{j2} > .. > \lambda_{jk}$, то первой компонентой кортежа будет шифр первого субъекта последовательности, а именно субъекта $s_v \in S^{(1)}$, разрешившего субъекту s_j доступы $(a_1, a_2, \ldots, a_n)$ к объекту o_j.

На основании утвержденных списков запросов-действий над данными субъекта защиты, администратор безопасности вносит заявленные виды доступа с использованием классификаторов, в которых представлены типовые группы и статус информации, виды степеней секретности и т.д. При этом проверяется условие, не позволяющее субъекту запрашивать любые виды доступа к субъекту или объекту с более высоким уровнем защиты. Если субъект защиты является «владельцем» объекта защиты, то ему разрешены запросы по моди-

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

фикации содержимого объекта. Если условия не выполняются, то заявленный вид доступа не записывается в матрицу, пока не будут изменены характеристики пары «субъект — объект»: понизить степень секретности объекта или повысить категорию допуска субъекта.

Если характеристики пары «субъект — объект» не согласованы, то выполнение спорной операции обработки данных исключается из обязанностей субъекта. При первоначальном внесении списков запросов-действий заявленные виды доступа считаются безусловно разрешенными к реализации. В дальнейшем некоторые из разрешенных видов доступа пары «субъект — объект» могут быть временно приостановлены или запрещены к реализации. Матрица считается незаполненной, если поле «право реализации» пусто.

Рассмотрим механизмы *анализа* заполнения матрицы прав доступа с учетом выполнения основного правила разграничения доступа для двух видов доступа: «читать (R)» и «писать (W)». Задание полного списка условий доступа к данным различной степени секретности и правила управления правами доступа подробно рассмотрены в [4].

Добавление субъекта возможно при полном описании классификаторов и спецификаций s_j и o_j. Для нового s_j выводится список объектов, помечаются необходимые объекты защиты, выбираются из классификатора виды доступа и проверяется основное правило. Если $J(s_j) \geq J(o_j)$ и субъект s_j является владельцем o_j, то $a_k = W$, иначе $a_k = R$. Для каждого разрешенного вида доступа пары «субъект — объект» определяется «право реализации»: «разрешено» или «запрещено».

Удаление субъекта s_j влечет за собой удаление из матрицы доступа строки, принадлежавшей этому субъекту. Так как матрица прав доступа не должна содержать пустых столбцов, из нее удаляются объекты, к которым не имеет доступа ни один субъект системы.

Добавление новых связей в матрице доступа происходит за счет увеличения связей s_j с другими новыми объектами o_j^*. Выводится список объектов, помечаются необходимые объекты защиты, выбираются из классификатора виды доступа и проверяется основное правило защиты. В поле «право реализации» вносится «разрешено».

Удаление связей в матрице доступа влечет за собой удаление строки пары «субъект — объект».

Редактирование связей в матрице прав доступа может происходить в двух случаях. Это изменения по праву реализации, когда разрешенный ранее вид доступа запрещается (временно приостанавливается), и наоборот. Изменения по виду доступа могут произойти, если повышается статус субъекта защиты или понижается степень секретности объекта из-за старения информации, тогда невыполняемая ранее проверка $J(s_j) \geq J(o_j)$ будет удовлетворять основному правилу разграничения доступа.

Рассмотрим механизмы *контроля* обращения к матрице прав доступа с учетом заданной иерархии субъектов и объектов защиты. Наделение субъектов и объектов защиты структурой дерева дает оптимальную картину управления доступом и обеспечивает реализацию корректного управления такими правами доступа, как «право порождения новых объектов», «лишение права доступа», «передача прав доступа субъектом s_j субъекту $s_v, v \neq j$», «право создания или

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

уничтожения субъектом s_j объекта o_j ». Указанная модель, реализованная на древовидной структуре субъектов и объектов защиты, предназначена для обеспечения режима секретности, действующего в Республике Казахстан [5]. В перспективе планируется рассмотрение данной постановки задачи на сетевой структуре (графовая модель).

Реализация права владения с учетом иерархии субъектов и объектов защиты связана с созданием (уничтожением) субъектом s_j объекта o_j или выполнением запросов s_j по модификации содержимого o_j.

Реализация права порождения с учетом иерархии субъектов и объектов защиты связана с созданием (порождением) субъектом-владельцем s_j из объекта o_j нового объекта o_j^*, при этом $J(o_j) \geq J(o_j^*)$.

Реализация права передачи прав доступа субъектом s_j субъекту $s_\nu, \nu \neq j$ заключается в том, что субъект-владелец s_j может передать часть своих прав по доступу к объекту o_j другому субъекту s_ν, оставаясь владельцем o_j. Таким правом передачи прав обладают субъекты $s_j \in S^{(1)}$.

3. Подсистема мониторинга безопасности

Проверка подлинности (аутентификация) идентификационных имен различных категорий субъектов защиты осуществляется через функцию подтверждения подлинности на основе пароля. Применение схем криптопреобразований для аутентификации различных групп субъектов защиты ориентировано на удовлетворительные характеристики надежности. Пароль хранится в зашифрованном виде, что существенно снижает риск его раскрытия. При аутентификации введенный пользователем пароль также зашифровывается и сравнивается с хранящимся зашифрованным значением. Файл, хранящий пароли, должен быть сам защищен от попыток несанкционированного доступа, так же как и информация о грифе секретности объектов и уровне допуска субъектов системы. Предусмотрен динамический контроль качества назначаемых паролей и обработка статистических данных (дата и время предыдущего входа и окончания сеанса работы), позволяющих обнаружить факт несанкционированного входа в систему под именем легального пользователя.

Выполнение текущего запроса к информационным ресурсам с учетом основного правила доступа происходит только после успешной аутентификации субъекта. Анализируется поступивший запрос пары «субъект - объект» на запрашиваемый вид доступа. Если уровень допуска субъекта противоречит правилам доступа выбранной модели или субъект не имеет права на реализацию подобного запроса, то субъекту будет отказано в доступе, а в журнале подобный запрос зарегистрируется как попытка несанкционированного доступа, и администратор предпримет действия по блокировке действий злоумышленника.

Защита матрицы прав доступа от попыток несанкционированной модификации осуществляется через блокировку неверных значений и контроль журнала безопасности. Реагирование на попытки несанкционированного доступа неавторизованных пользователей происходит после неверного ввода пароля субъекта защиты, незарегистрированного абонента, неразрешенного вида доступа, противоречивого ввода параметров спецификаций субъектов и объектов защиты.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

В подсистеме мониторинга безопасности для решения отдельных из вышеперечисленных задач реализована интеллектуальная информационная технология — иммунокомпьютинг с возможностями мониторинга для входной информации, представленной либо в виде временных рядов с точечными и интервальными параметрами, либо OLAP-кубов с аналогичными параметрами. Математические модели и вычислительные процедуры иммунокомпьютинга [6 — 9] являются новой вычислительной парадигмой, основанной на формализованных механизмах иммунной системы. Этот подход обладает высокой степенью робастности и распараллеливания вычислительных процессов, эффективность которых была неоднократно продемонстрирована на примере реальных приложений по информационной безопасности [7 — 9]. Разработанные математические модели и вычислительные процедуры предложены для реализации в подсистеме интеллектуального мониторинга для решения следующих задач: идентификация личности по фотоизображению; распознавание рукописного символа; формирование электронной цифровой подписи; идентификация личности по изображению отпечатка пальца; мониторинг динамических процессов.

Рассматриваемая подсистема включает следующие модули: обучение, иммунизация, апоптоз, распознавание, оптимизация коэффициентов и вычисление значений индексов риска, интерпретация полученных результатов. Как было отмечено выше, процессы мониторинга могут представляться математическими моделями с точечными параметрами либо с неопределенными параметрами интервального типа. Функциональное назначение отдельных модулей подсистемы следующее:

- обучение — формирование обучающих матриц, которые могут быть либо плоскими, либо OLAP-кубами, с точечными или интервальными элементами; сингулярное разложение этих матриц; формирование информации об «антителе» и «антигене»;
- распознавание — проецирование исходного образа, сформированного на основании информации об «антителе» и «антигене», в пространство формальной иммунной сети (евклидово или интервальное); вычисление значений энергии связи, обоснование и выбор метрики, формирование классов;
- оптимизация — формирование матрицы индексов [8], которая в зависимости от выбранного варианта аппроксимации может иметь элементы, представленные в ортогональных базисах (Чебышева, Лежандра, Лагерра или Эрмита); сингулярное разложение этой матрицы и решение задачи оптимизации коэффициентов индекса с использованием обобщенного спектрально-аналитического метода [7 — 9].

4. Заключение

Разработанная система с мандатной политикой информационной безопасности имеет следующие преимущества:

- сложившаяся практика работы с документами ограниченного пользования спроецирована на работу с аналогичными электронными документами и всем документооборотом в целом и ориентирована на особенности документооборота, согласно положению (инструкции) 1-го отдела;
- выделенные множества объектов и субъектов защиты характеризуются параметрами, которые позволяют учесть особенности предметной области и адекватно формализовать процесс документооборота;
- множества объектов и субъектов защиты наделены структурами дерева, что позволяет реализовать полную систему многоуровневой защиты и эффективнее выполнять запрос (отказ по запросу) пользователя;

- множество субъектов защиты делится на два подкласса $S = S^{(1)} \cup S^{(2)}$, что позволяет эффективнее контролировать процесс управления правами субъектов защиты;
- существенно расширен список запросов и учтено специфическое «право реализации запроса»;
- эффективно решены отдельные задачи обеспечения информационной безопасности: идентификация и аутентификация личности по фотоизображению и отпечатку пальца; формирование и вычисление индексов риска, мониторинг и исследование динамических процессов.

Эффективность разработанной системы с мандатной политикой информационной безопасности продемонстрирована при построении и эксплуатации корпоративной сети космической инфраструктуры [10,11].

ЛИТЕРАТУРА

1. Тишков А.В., Котенко И.В., Сидельникова Е.В., Черватюк О.В. Обнаружение и разрешение противоречий в политиках безопасности // Проблемы безопасности и противодействия терроризму. Материалы второй междунар. научн. конф. по проблемам безопасности и противодействия терроризму, МГУ им. М.В.Ломоносова. М.: МЦНМО, 2006. С.172 — 185.
2. Степашкин М.В., Котенко И.В., Богданов В.С. Интеллектуальная система анализа защищенности компьютерных сетей // КИИ-2006. X Национальная конференция по искусственному интеллекту с международным участием: Труды конференции. Т. 1. М.: Физматлит, 2006. С.149 — 157.
3. Защита от несанкционированно доступа к информации. Термины и определения: Руководящий документ // Сб. руковод. докум. по защите информации от несанкционированного доступа. М.: Гостехкоммисия России, 1998.
4. *Горковенко Е. В.* Формализованное представление механизмов защиты при мандатном разграничении доступа // Изв. НАН РК. 2006. №3. С.79 — 85.
5. *Горковенко Е. В.* Формирование множеств субъектов и объектов защиты для многоуровневой модели разграничения доступа // Вест. Казах. нац. ун-та им. аль-Фараби. Алматы: КазНУ. 2006. № 3(50). С. 104 — 110.
6. *Tarakanov A. O., Skormin V. A., Sokolova S. P.* Immunocomputing: Principles and Applications., N.Y.: Springer. 2003. 193 p.
7. *Соколова С.П., Соколова Л.А.* Интеллектуальные информационные системы на основе иммунокомпьютинга: Учебное пособие. Алматы: КБТУ, 2005. 168 с.
8. *Sokolova L. A.* Index design by Immunocomputing. Lecture Notes in Computer Science, Vol. 2787. Berlin: Springer. 2003. P. 120 — 127.
9. *Соколова С. П. и др.* Интеллектуальный анализ многомерных данных на основе иммунокомпьютинга. Алматы: ИПИУ МОН РК, 2006. 110 с.
10. *Горковенко Е. В.* Многоуровневый контроль доступа в корпоративной сети космической инфраструктуры // Математ. журн. Алматы: ИПИУ МОН РК, 2007. Т. 7, №3(25). С. 28 — 34.
11. *Горковенко Е. В.* Организация информационной безопасности в корпоративной сети космической инфраструктуры // Вестн. Национальной инженерной академии Республики Казахстан. Алматы, 2007. №1(23). С. 60 — 65.