На правах рукописи

Демидов Александр Владимирович

Автоматизация разграничения перекрёстного доступа к информационным ресурсам корпоративных порталов (на примере газотранспортных предприятий)

05.13.06 – Автоматизация и управление технологическими процессами и производствами (промышленность)

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Орёл – 2013

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Государственный университет — учебно-научно-производственный комплекс».

Научный руководитель:	доктор технических наук, профессор Ерёменко Владимир Тарасович
Официальные оппоненты:	Подольский Владимир Ефимович, доктор технических наук, профессор, ФГБОУ ВПО «Тамбовский государственный технический университет», директор ТамбовЦНИТ
	Лебеденко Евгений Викторович, кандидат технических наук, Академии ФСО России, профессор кафедры «Информатика и вычислительная техника»
Ведущая организация:	ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет»

Защита состоится «10» декабря 2013 г. в 09:00 часов на заседании диссертационного совета Д 212.182.01 при ФГБОУ ВПО «Госуниверситет — УНПК» по адресу: 302020, РФ, г. Орёл, Наугорское шоссе, д. 29, аудитория 212.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «Госуниверситет — УНПК».

Автореферат разослан «08» ноября 2013 г.

Учёный секретарь
диссертационного совета,
кандидат технических наук, доцент Волков В. Н.

Общая характеристика работы

Актуальность работы. С точки зрения управления газотранспортное предприятие (ГТП) относится к категории сложных и характеризуется многоуровневой и территориально распределённой структурой, а также тем, что хозяйственная деятельность обусловлена следующими обстоятельствами: усложнением процессов транспортировки газа; потребностью повышения экономической эффективности, а также снижения удельных затрат на добычу и транспортировку газа. Существенное влияние на автоматизацию технологических процессов и производств ГТП оказывают: процессы либерализации газового рынка, повышение требований к защите данных процессов и производств, ужесточение экологического мониторинга.

Современное ГТП использует широкий спектр систем автоматизации деятельности: ERP, SCADA, MES, CRM и т. п. Каждый из этих классов систем предназначен для решения задач в отдельных подразделениях ГТП и может быть представлен различными архитектурными решениями. Интегрированная система управления ГТП строится в виде многоуровневой иерархической структуры, чётко повторяющей административную подчинённость диспетчерских служб и производственных отделов.

В процессе функционирования ГТП создаётся и используется множество информационных ресурсов (ИР) различного уровня конфиденциальности.

С учётом территориально-распределённой структуры типового ГТП, по мнению ведущих специалистов, наиболее эффективным, с точки зрения архитектуры реализации АСУП газотранспортного предприятия является корпоративный портал, который должен представлять собой интегрированное Web-приложение класса B2E, обеспечивающее пользователям единую точку перекрёстного доступа к предназначенным для них распределённым ИР. Под *перекрёстным доступом* понимается взаимное использование ИР различными подразделениями ГТП и их партнёрами, без нарушения их конфиденциальности.

Диссертационное исследование базируется на результатах работ в области: теории распределённой обработки данных (В. Г. Хорошевский, Э. Таненбаум, М. ван Стеет, В. В. Воеводин, Вл. В. Воеводин); теоретических основ построения порталов и информационных ресурсов (А. Д. Иванников, Дж. Терра, К. Гордом, Д. Салливан, Г. Коллинс); теории управления доступом к распределённым информационным ресурсам (Б. Лампсон, М. Абади, П. Н. Девянин); теории алгоритмов и оценки сложности вычислений (Д. Кнут, А. Ахо, Дж. Ульман).

Множественность групп пользователей влечёт за собой *сложность процесса управления перекрёстным доступом к ИР корпоративных порталов*, а также *сложность определения общей политики управления доступом к ИР*.

Кроме того, корпоративные порталы ГТП имеют варьируемую структуру и реализованы на разных аппаратно-программных платформах с помощью разнородных, зачастую несовместимых, технологий.

Это определяет актуальность темы, а также выбор объекта, предмета и цели исследования.

Объектом исследования является процесс организации разграничения перекрёстного доступа к ИР в сети корпоративных порталов ГТП.

В качестве **предмета исследования** рассматриваются модели, методики и алгоритмы подсистемы автоматизации разграничения перекрёстного доступа к ИР в сети корпоративных порталов ГТП.

Целью диссертационной работы является повышение эффективности организации разграничения перекрёстного доступа к ИР корпоративных порталов газотранспортных предприятий, заключающееся в улучшении значений коэффициента доступности и коэффициента конфиденциальности.

Для достижения поставленной цели были сформулированы и решены следующие основные **задачи**:

— анализ и исследование методов организации управления информационными ресурсами в сети корпоративных порталов;

— формализация процесса разграничения перекрёстного доступа к ИР в сети корпоративных порталов;

— разработка способов и приёмов доступа в рамках подсистемы разграничения перекрёстного доступа к ИР в сети корпоративных порталов;

— разработка архитектуры программной реализации подсистемы разграничения перекрёстного доступа в сети корпоративных порталов ГТП и анализ результатов его применения.

Методы исследования. В качестве основных средств теоретических исследований использовались методы системного анализа, математического моделирования, дискретной математики, математической статистики, методы модульного и объектно-ориентированного программирования, методы построения подсистем АСУ, а также методы оценки эффективности алгоритмов.

Достоверность и обоснованность научных положений, результатов, выводов и рекомендаций, приведённых в диссертационной работе, достигается за счёт: корректного применения известного математического аппарата; непротиворечивости и воспроизводимости результатов, полученных теоретическим путём; соответствия результатов теоретических и экспериментальных исследований.

Научная новизна

1. Предложена формализованная модель управления перекрёстного доступом к ИР в сети корпоративных порталов ГТП, базирующаяся на прецедентном подходе к завершённому потоку событий и отличающаяся разработанными правилами предоставления доступа, учитывающими уровень привилегий пользователей и уровень конфиденциальности ресурса.

2. Предложена методика управления перекрёстным доступом к ИР в сети корпоративных порталов базирующаяся на разработанной модели и отличающаяся процедурами: интеграции информационных ресурсов на основе уникального идентификатора, трансляции прав доступа от родительского ресурса.

3. Предложена архитектура программной реализации подсистемы разграничения перекрёстного доступа к ИР в сети корпоративных порталов ГТП, отличающаяся использованием разработанной формализованной модели и методики.

Практическая значимость результатов исследования заключается в том, что разработанные теоретические положения реализованы в виде комплекса алгоритмов и программ (свидетельства о государственной регистрации программ для ЭВМ №2011619386, №2011619387 и №2012616860). Кроме того, разработанные автором положения: использованы в деятельности ООО «НТЦ Космос-Нефть-Газ», а также внедрены в ФГБОУ ВПО «Госуниверситет — УНПК» в рамках дисциплин «Математические основы защиты информации», «Модели безопасности компьютерных систем».

Основные результаты диссертационной работы получены в ходе выполнения работ по ГК №02.740.11.0831 «Исследования в области построения системы управления информационным обменом сети корпоративных порталов». Результаты диссертационной работы были использованы в ходе работ по ГК №16.740.11.0041 «Разработка распределённых автоматически профилируемых средств обработки, архивирования и защиты диагностической информации». Указанные работы выполнены по Федеральной целевой программе «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (Заказчик — Министерство образования и науки РФ).

Апробация работы Основные результаты диссертации докладывались на следующих конференциях:

1. IV Международной научно-технической конференции «Информационные технологии в науке, образовании и производстве (ИТНОП-2010)» (г. Орёл)

2. 2-ая межрегиональная научно-практическая конференция «Информационное развитие России: состояние, тенденции и перспективы (региональный аспект), 22 апреля 2011» (г. Орёл)

3. Международная научно-техническая интернет-конференция «Информационные системы и технологии (ИСиТ-2011)» (г. Орёл)

4. V Международной научно-технической конференции «Информационные технологии в науке, образовании и производстве (ИТНОП-2012)» (г. Орёл)

5. Международная молодёжная конференция «Прикладная математика, управление и информатика» 2012 (г. Белгород)

6. Международная конференция «Intelligent Information Systems (IIS-2013)» (г. Кишинёв)

Положения, выносимые на защиту

— Формализованная модель управления перекрёстным доступом к ИР в сети корпоративных порталов ГТП.

— Методика управления перекрёстным доступом к ИР в сети корпоративных порталов и реализующие её алгоритмы организации управления привилегиями и доменами пользователей системы.

— Архитектура программной реализации подсистемы разграничения перекрёстного доступа к ИР в сети корпоративных порталов ГТП.

Публикации. Материалы диссертации опубликованы в 13 печатных работах, из них 5 статей в рецензируемых журналах входящих в перечень ВАК РФ, 8 статей в сборниках трудов конференций. По результатам исследований получено 3 свидетельства о государственной регистрации программ для ЭВМ.

Структура и объем диссертации. Диссертационная работа изложена на 151 страницах и состоит из введения, четырёх глав, заключения, списка литературы из 135 наименований и 1 приложении; содержит 13 таблиц и 30 рисунков.

Содержание работы

Во введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе проведён анализ методов организации доступа к ИР корпоративных порталов ГТП.

Анализ проектов модернизации объектов газотранспортной системы показал, что в большинстве существующих систем БД технологического оборудования строится на основе реляционных СУБД, и блок транзакционных данных представляет собой нормализованную структуру, исключающую избыточность и обеспечивающую целостность данных на уровне встроенных механизмов СУБД. Однако, одна лишь нормализация структуры не всегда обеспечивает нужный уровень связности данных, так как не всегда с её помощью возможно описать системы со сложной внутренней структурой при обеспечении необходимого уровня согласованности. Вторым существенным недостатком нормализации является сложность внесения корректировок в структуру данных, необходимость которых возникает при изменении модели описания единиц оборудования.

Установлено, что задачи диспетчерского управления ГТП требуют хранения всей ретроспективы данных, вводимых в систему. В сочетании с пожеланием не усложнять ПО избыточно, указанное требование поставило перед разработчиками нетривиальную задачу: помимо хронологии значений технических параметров необходимо было обеспечить работу системы с логической структурой, релевантной на определённый (указанный пользователем) момент времени.

Выявлено, что основная сложность обмена диспетчерско-технологическими сообщениями заключается в том, что физически вычислительные сети автоматизированных систем управления технологическими процессами и вычислительные сети автоматизированных систем управления производственно-хозяйственной деятельностью, в которых функционирует диспетчерский комплекс, разделены и их прямое объединение запрещено нормативными документами.

Определено, что в существующих системах обеспечения защиты данных вынесено управление двумя основными процессами: управление пользовательскими сессиями и контроль доступа к ресурсам. Стандартным способом идентификации пользователя при входе в информационную систему является проверка по условному имени (логину) и паролю. Кроме этого, во время авторизации регистрируется IP-адрес машины, с которой осуществляется доступ, при последующих запросах выполняется его проверка. Предоставляется возможность установить ограничение для пользователя или группы пользователей на конкретный адрес или диапазон адресов.

Выявлено, что не все задачи по автоматизации управления доступом к ИР можно эффективно решить в рамках одной программной среды. При этом рас-

ширение функционала на уровне портала с подключением дополнительных программных модулей абсолютно неприемлемо, т. к. не может быть пропущено через единую подсистему контроля прав доступа к ИР, что представляет собой серьёзную угрозу в системе защиты данных.

Установлено, что подход к решению поставленной задачи должен базироваться не на создании объединённых порталов, зачастую дублирующих информационные массивы предприятий и требующих значительных ресурсов для функционирования и актуализации информации, а на создании сети порталов, интегрирующей распределённые (как территориально, так и административно) ИР ГТП. Это позволяет обеспечить взаимодействие системы управления корпоративного портала с подсистемами управления ГТП (такими как ERP-, CRM-, SCM-системы и др.) через закрытие разделы корпоративных порталов.

Во второй главе рассмотрены особенности процесса разграничения перекрёстного доступа к ИР в сети корпоративных порталов ГТП.

Изложение моделей разграничения доступа в различных источниках, как правило, носит фрагментарный характер. При этом основное внимание уделяется лишь общей формулировке основных определений и результатов моделей либо краткому их перечислению обзорного характера. В работе рассмотрены положения классических моделей разграничения доступа в компьютерных система: дискреционного, мандатного, ролевого. Для осуществления процесса управления доступом (рисунок 1) была разработана и предложена модель управления перекрёстным доступом в сети корпоративных порталов.

Рис. 1. Процесс управления доступом в сети корпоративных порталов

Учитывая вышеописанные особенности была проведена разработка формализованной модели управления перекрёстным доступом к ИР в сети корпоративных порталов ГТП. Формально она определяется следующим образом:

$$M = \langle U, D, P, R, S, Z, W, F \rangle, \tag{1}$$

где

$U = \{u_1, u_2, \ldots, u_{uc}\}$ — множество субъектов доступа (пользователей), при uc — количестве субъектов доступа. Субъекты множества осуществляют информационный обмен в рамках разрешённых протоколов (HTTP/HTTPS). Каждому субъекту соответствует набор уникальных (в рамках пользовательского домена) идентификаторов $I = \{i_1, i_2, \ldots, i_{ic}\}$ — множество идентификаторов, при ic — количестве идентификаторов. Идентификаторы служат для однозначного распознавания субъектов среди всех элементов множества U. С помощью аутентификаторов из множества A возможно подтвердить, что субъект именно тот, за кого себя выдаёт, следовательно $A = \{a_1, a_2, \ldots, a_{ac}\}$ — множество аутентификаторов, при ac — количестве аутентификаторов. Введены следующие функции: $user : I \to U$,

$id : A \to I$. Они включаются в множество базовых функций системы — F, т. е. $\{user, id\} \subset F$.

$D = \{d_1, d_2, \ldots, d_{dc}\}$ — множество пользовательских доменов, при mc — количестве пользовательских доменов. Каждый пользователь u_j включается в пользовательский домен d_i, т. е. $u_j \subset d_i$, для $j \in \{1, \ldots, uc\}$ и $i \in \{1, \ldots, dc\}$. В домен d_i также входит следующее отношение: Введены следующие функции: $dom : Z \to D$, $authorization : w_j \times \{permission(u_k) | u_k \in U\} \times U \to \{ok, access\ denied\}$. Они включаются в множество базовых функций системы — F, т. е. $\{dom, authorization\} \subset F$.

$P = \{p_1, p_2, \ldots, p_{pc}\}$ — множество прав доступа, при pc — количестве прав доступа. Это множество содержит все возможные права доступа к ресурсам Web-порталов. Введены следующие отношения: $UP = U \times P$ — отношение, задающее соответствие между субъектами и правами доступа и $PH \subseteq P \times P$ — отношение частичного порядка (иерархия) на множестве прав доступа, обозначаемое «$\succeq$». Введены следующие функции: $permission : U \to 2^P$ — функция ставящая в соответствие субъекту u_i множество прав доступа $permission(u_i) \subseteq \{p | (\exists p_0 \succeq p) \wedge ((u_i, p_0) \in UP)\}$. Они включаются в множество базовых функций системы — F, т. е. $permission \in F$.

$R = \{r_1, r_2, r_3, r_4, r_5\}$ — множество ролей в рамках системы: r_1 — «неавторизованный пользователь», r_2 — «авторизованный пользователь», r_3 — «администратор портала», r_4 — «администратор пользовательского домена» и r_5 — «администратор сети». Введены следующие отношения: $UR = U \times R$ — отношение, задающее соответствие между субъектами и ролями, $RP = R \times P$ — отношение, задающее соответствие между ролями и правами доступа, $RH \subseteq R \times R$ — отношение частичного порядка (иерархия) на множестве ролей, обозначаемое «$\succeq$». Введена функция: $role : S \to R$ — функция ставящая в соответствие сиссии s_i, одну из ролей допустимых в R.

$S = \{s_1, s_2, \ldots, s_{sc}\}$ — идентификатор сеанса, при sc — количестве таких идентификаторов сеанса. Элемент данного множества создаётся при первом обращении субъекта к объекту, когда субъект проходит идентификацию и аутентификацию. Идентификатор и аутентификатор сохраняются в сеансе и не требуют повторного ввода при обращении к ресурсам. Введены следующие функции: $sid : S \to I$, $suser : S \to U$, $sauth : S \to A$. Они включаются в множество базовых функций системы — F, т. е. $\{suser, sid\} \subset F$.

$W = \{w_1, w_2, \ldots, w_{wc}\}$ — множество Web-порталов, при wc — количестве Web-порталов. Каждый элемент данного множества есть карта Web-портала (site map), представленная в виде дерева, т. е. $w_j = (V_j, E_j)$, где V_j — адреса ресурсов Web-портала определённые как максимальный префикс с отсечённой частью указывающей на протокол URI (например — *portal.dom/chapter1/section/page.html*), а E_j — представляет собой множество рёбер задающих смежность ресурсов. Смежность ресурсов определяется следующим образом: $(u, v) \in E_j$, если полный адрес ресурса v является префиксом ресурса u или наоборот.

$Z = \{z_1, z_2, \ldots, z_{zc}\}$ — множество серверов доступа, при zc — количестве серверов доступа включённых в сеть. Одним сервером доступа могут обслуживаться

несколько Web-порталов, т. е. $z_j = \langle addresses_j, portals_j, d_i \in D \rangle$, где $addresses_j$ — множество адресов сервера доступа, необходимых для целей администрирования, $portals_j$ — взаимно-однозначное соответствие между порталами обслуживающимися на данном сервере доступа и адресами интерфейсов к которым они подключены: $portals_j = \{(w_i, int_k) | (i \leq wc) \wedge (int_k \in InterfacesSet)\}$

$F = \{user, id, permission, suser, sid, sauth, dom, authorization, role\}$ — множество базовых функций системы.

Сформулированы правила перекрёстного доступа к ИР, находящимся под управлением системы. Каждому ИР ставится в соответствие множество пар вида, $\langle domain, privacy \rangle$. В этом случае пользователь имеет доступ к ресурсу только в том случае, если ресурс принадлежит домену пользователя, и уровень его привилегий доступа больше или равен уровню привилегий ресурса. Более формально, пользователь u имеет доступ к ресурсу res, если:

$$\exists \langle domain, privacy \rangle \in D_r(res) : domain \in D_p(u) \& privacy \geq access(u), \quad (2)$$

где D_r — оператор получения множества пар, характеризующих ресурс (характеристического множества);

D_p — оператор получения множество доменов (иерархии доменов), в которых состоит пользователь;

$access$ — функция уровня допуска пользователя.

Сформулировано следующие правила: правило взаимодействия пользователей и ресурсов различных доменов; правило назначения уровней доступа к доменам высшего уровня; правила разграничения доступа для администраторов различных уровней (корпоративных порталов, серверов доступа, сети корпоративных порталов).

Выявлено, что в целях гибкого управления модель допускает внесение дополнительных ограничений на комбинации компонентов, например: время жизни сеанса пользователя, типа соединения между компонентами и т. п.

В третьей главе на основании анализа модели предложенной, во второй главе работы предлагается методика управления перекрёстным доступом к ИР в сети корпоративных порталов ГТП (рисунок 2).

При исследовании модели, описанной во второй главе работы, и предложенной методики определены следующие практические ограничения:

— корпоративный портал включаемый в сеть уже имеет систему управления содержимым (content managemetn system), таким образом, необходимо учесть возможности используемой системы;

— учитывается физическое подключение сервера обслуживающего Web-портал и наличие возможности подключения сервера доступа (особенности связанные с DMZ, NAT, требованиями провайдеров услуг и/или организации дата-центров);

— возможность временного отказа в обслуживании на уровне провайдера услуг.

Для каждого из этапов реализующих методику разработаны алгоритмы.

Определены ключевые участники процесса построения сети корпоративных порталов и их основные задачи (*Этап 1*):

1. Владельцы порталов сети. К их задачам относятся: формирование структуры портала данного узла сети (сервера доступа), управление учётными записями данной доменной группы пользователей, осуществление контроля за функционированием узла системы доступа и обращениями к связанным порталам, управление доступом к ресурсам портала.

2. Центр управления сетью (ЦУС) корпоративных порталов ГТП. К его основным задачам относятся: управление доменными группами, делегирование полномочий администратора домена, управление доступом между доменными группами, контроль за функционированием сети в целом и репликацией данных.

3. Пользователи сети. Они решают задачи получения доступа к открытым разделам порталов и авторизованного доступа к закрытым разделам.

На *Этапе 2* сформулированы основные функциональные задачи администраторов системы:

1. Управление сетью порталов осуществляется посредством создания доменных групп пользователей, установление разрешения доступа между доменными группами и формирование уровня привилегий доступа.

2. Управление перекрёстным доступом к разделам портала различными пользователями осуществляется на основе назначения ресурсов открытыми или закрытыми, и определения привилегий доступа к закрытым ресурсам.

3. Управление учётными записями пользователей.

4. Контроль за функционированием сети и информационным обменом между серверами доступа.

На *Этапе 3* методики осуществляется организация информационного взаимодействия в сети корпоративных порталов и интеграция в сеть ИР участников (владельцев порталов). Специфика построения сети порталов подразумевает создание на серверах доступа базы данных ресурсов в виде дерева портала (карты сайта). Одному пользовательскому домену может быть сопоставлено несколько интернет доменов порталов, а в рамках одного интернет портала множество ресурсов. Поскольку обращение к ресурсам происходит по уникальному идентификатору URI, где ключевой частью является доменное имя портала в виде URL, то первоначально администратору портала (домена) необходимо интегрировать в сеть порталов доменное имя портала, ассоциировав его с определённым пользовательским доменом участником и, соответственно правилами перекрёстного доступа. Для соответствующего портала создаётся необходимое описание и информационный дайджест в портале центра управления сетью.

На *Этапе 4* осуществляется добавление ИР определённых корпоративных порталов ГТП, для которых устанавливаются разрешения в соответствии с группами привилегий доступа. При этом привилегии могут наследоваться от родительского ресурса или же данные ресурсы могут получать новый, но более строгий уровень контроля доступа. Помимо этого, системой предусмотрена инверсия прав доступа с разрешительных на запретительные, которые имеют более высокий приоритет.

В четвёртой главе проводится практическое обоснование модели и методики предложенных в предыдущих главах.

Рис. 2. Методика управления перекрёстным доступом к ИР в сети корпоративных порталов

Предложена архитектура программной реализации подсистемы разграничения перекрёстного доступа к ИР в сети корпоративных порталов ГТП (рисунок 3).

Для решения задачи перераспределения HTTP-трафика между ресурсами порталов, контролируемыми одним сервером доступа предложено техническое решение по применению фронтального Web-сервера в качестве обратного прокси-сервера (reverse proxy-server). Предложены архитектурные конструкции — шаблоны проектирования (design pattern), описывающие необходимую функциональность фронтального Web-сервер. Для организации взаимодействия компонентов подсистемы разграничения перекрёстного доступа проведён анализ: информационных потоков межу компонентами; типа и характера информационного взаимодействия с целью определения применимости различных протоколов. Сформулированы требования к каналам взаимодействия компонентов.

Получена оценка временных и трудовых показателей разработки подсистемы управления перекрёстным доступом к ИР для сети корпоративных порталов и объединённого портала с помощью алгоритмической модели оценки стоимости разработки программного обеспечения The Constructive Cost Model 2 (COCOMO 2).

Эффективность разграничения доступа в исследовании определяется способностью системы обеспечить различные уровни доступа к объектам, для множества групп пользователей, при сохранении возможности выполнять свои функциональные и должностные обязанности. Определены исходные данные для оценки качества управления перекрёстным доступом к ИР корпоративного портала ГТП. При категоризации ИР сети корпоративного портала были выделены их категории и

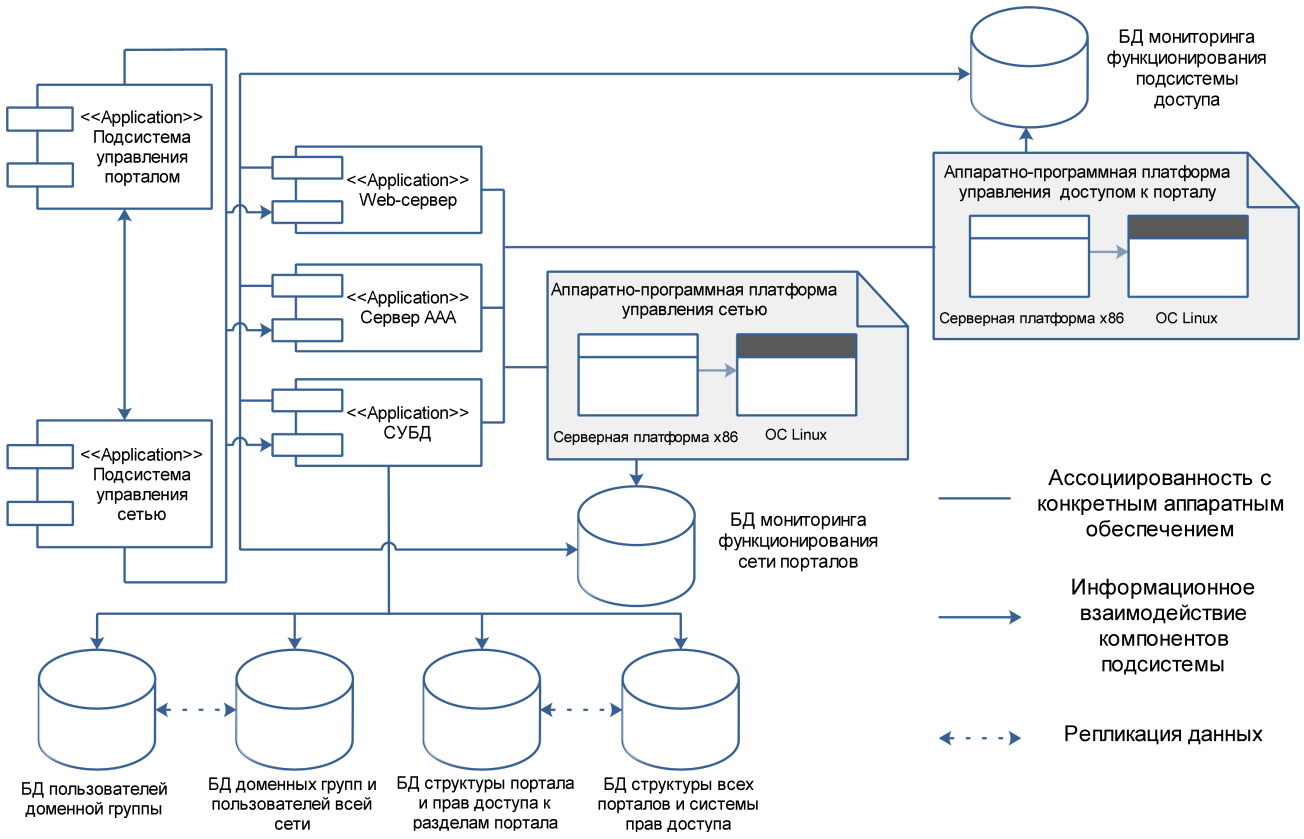

Рис. 3. Архитектура программной реализации подсистемы разграничения перекрёстного доступа к ИР

произведена их классификация по: конфиденциальности, целостности, доступности.

Представлены результаты имитационного моделирования подсистемы разграничения доступа в сети корпоративных порталов ГТП.

Целью моделирования являлось определение эффективности разграничения доступа, при использовании предложенной подсистемы (выражающееся в сокращении ошибок первого и второго рода). Рассматриваемые процессы идентификации, аутентификации и авторизации субъектов представлены в виде системы массового обслуживания. В качестве эндогенных (зависимых) переменных рассматривалось количество получателей запроса на доступ. С учётом этого, а так же характера поступления заявок и распределения запросов от субъектов по сети корпоративных порталов в качестве критерия оценки эффективности функционирования рассматриваемой системы была выбрана пара распределений случайных величин — средние значения количества ошибок первого и второго рода.

При этом, за единицу модельного времени была выбрана величина, позволяющая передавать данные запросов субъектов по каналу за единицу модельного времени. В ходе выполнения программы моделировалось 1 млн. единиц модельного времени. За это время генерировались запросы со случайной принадлежностью к порталу, которая распределена равновероятно. Допустимую вероятность возникновения сбоя в процессе доступа принималась равной 0,01.

В заключении сформулированы основные результаты работы.

В приложениях экранные формы панели администрирования подсистемы разграничения доступа.

Основные выводы и результаты работы:

1. Поставлена и решена новая научная задача разработки способов и приёмов управления перекрёстным доступом в организационно-технологических распределённых комплексов ГТП, функциональных задач и объектов управления и их алгоритмизации.

2. Разработана формализованная модель управления перекрёстным доступом в сети корпоративных порталов ГТП определяющая в качестве основных правил: принадлежность ресурса домену пользователей; уровень его полномочий в виде целочисленного индикатора (доступность операций: поиск, публикация, модификация и т. п.); уровень конфиденциальности ресурса. В целях гибкого разграничения доступа разработанная модель предусматривает учёт дополнительных ограничений на такие комбинации компонентов, как: время жизни сеанса пользователя, типа соединения между компонентами и т. п.

3. Кроме того, правила правила разграничения доступа позволяют выполнять «горизонтальное» объединение пользователей по уровню в иерархии без учёта подразделений, за которыми они закреплены. Это особенно важно для реализации стереотипного назначения прав доступа, поскольку позволяет определить качественные категории пользователей, основываясь на занимаемой должности без учёта распределения по подразделениям организации.

4. Для управления доступом используется формальная модель назначения прав, определяются процедуры объединения пользователей в группы в соответствии с организационной иерархией газотранспортного предприятия — по отделам, филиалам, службам и т. д. Это даёт возможность прозрачного наложения «групповых» ограничений доступа к информации.

5. Разработана методика управления перекрёстным доступом к ИР в сети корпоративных порталов ГТП включающая алгоритмы реализующие: объединение корпоративных порталов в сеть, предоставляющие администратору сети политику разграничения доступа, формализующие правила разграничения доступа в соответствующих настройках сервера доступа и интегрирующие ИР корпоративных порталов.

6. Определено, что в методике управления перекрёстным доступом субъекты доступа представляют роли, которые могут исполнять пользователи системы, а сами прецеденты — те действия, которые они могли бы производить над ИР корпоративных порталов. Каждый прецедент является завершённым потоком событий в подсистеме разграничения доступа к ИР в сети корпоративных порталов ГТП, рассматриваемый с точки зрения пользователя. Выявленные прецеденты в подсистеме разграничения перекрёстного доступа в сети корпоративных порталов ГТП, определяют два важных результата: прецеденты естественным образом описывают функциональные требования к системе, где окружение этой системы определяется описанием различных субъектов, которые используют эту систему так, как это описано в прецедентах; прецеденты структурируют каждую объектную модель. Чтобы справляться со сложностью системы в целом, были структурированы

её объектные модели (классы) таким образом, чтобы каждая из них представляла некоторый отдельный аспект её использования. В используемом подходе каждый аспект соответствует одному прецеденту общей системы, и его описание включает только те объекты, которые участвуют в этом прецеденте. Однако, один объект может использоваться разными прецедентами.

7. Осуществлено проектирование архитектуры программной реализации подсистемы разграничения перекрёстного доступа к ИР в сети корпоративных порталов ГТП путём: рассмотрения особенностей функционирования сети корпоративных порталов и схемы размещения оборудования; распределения программных компонентов и служб между устройствами.

8. Проведённый анализ эффективности использования сети корпоративных порталов, выявил, что использование подсистемы разграничения перекрёстного доступа позволяет с меньшими трудозатратами, в сравнении с построением объединённого портала, интегрировать ИР и управлять доступом к ним.

9. Контроль доступа к ИР осуществляется через настройку доступа к конкретному приложению. Это позволяет для разных уровней доступа иметь разную структуру шаблонов и управляющих элементов. Более тонкие ограничения формируются на основе анализа входного запроса и при наличии в нём переменных, описанных в таблицах «тонкой настройки» прав доступа. Это позволяет выполнять корректировку уровня доступа для конкретной группы пользователей (или пользователя).

10. Произведена оценка разработанной подсистемы разграничения перекрёстного доступа для сети корпоративных порталов ГТП на основе коэффициента эффективности (комбинация конфиденциальности и доступности) и его значение составляет 0,78, которое свидетельствует об эффективности реализованных технических решений по сумме показателей.

Список работ, опубликованных по теме диссертации в изданиях, рекомендованных ВАК при Минобрнауки России

1. Демидов, А. В. Управление информационными потоками на основе резервирования ресурсов в сетях передачи данных предприятий [Текст] / А. И. Офицеров, В. Т. Еременко, А. В. Демидов // Известия ОрелГТУ. Серия «Информационные системы и технологии». — 2007. — №4-2/268 (535). — С. 167–172. (личное участие 30%).

2. Демидов, А. В. Моделирование процессов информационного обмена с приоритетами в сетях передачи данных промышленных предприятий [Текст] / А. И. Офицеров, С. И. Афонин, А. В. Демидов // Информационные системы и технологии. — 2010. — №3(59). — С. 126–133. (личное участие 30%).

3. Демидов, А. В. Концепция построения системы управления информационным обменом сети корпоративных порталов [Текст] / С. А. Лазарев, А. В. Демидов // Информационные системы и технологии. — 2010. — №4(60). — С. 123–129. (личное участие 50%).

4. Демидов, А. В. Применение технологии обратного проксирования в рамках системы управления информационным обменом сети корпоративных порта-

лов [Текст] / С. А. Лазарев, А. В. Демидов // Информационные системы и технологии. — 2012. — №6(68). — С. 131–136. (личное участие 50%).

5. Демидов, А. В. Особенности построения подсистемы управления доступом системы управления информационным обменом сети корпоративных порталов [Текст] / С. А. Лазарев, А. В. Демидов // Информационные системы и технологии. — 2012. — №4(72). — С. 103–110. (личное участие 50%).

Список работ, опубликованных по теме диссертации в материалах конференций

6. Демидов, А. В. Моделирование процессов информационного обмена в сетях передачи данных промышленных предприятий [Текст] / А. И. Офицеров, С. И. Афонин, А. В. Демидов // «Информационные технологиии в науке, образовании и производстве» (ИТНОП). Материалы IV Международной научно-технической конференции. — 2010. — Орёл: ОрёлГТУ. — Т. 5. С. 94–101. (личное участие 30%).

7. Демидов, А. В. Концепция построения системы управления информационным обменом сети образовательных порталов [Текст] / С. А. Лазарев, А. В. Демидов // «Информационные технологиии в науке, образовании и производстве» (ИТНОП). Материалы IV Международной научно-технической конференции. — 2010. — Орёл: ОрёлГТУ. — Т. 5. С. 80–86. (личное участие 50%).

8. Демидов, А. В. Анализ и выбор протоколов взаимодействия распределенных компонентов системы управления информационным обменом сети корпоративных порталов [Текст] / С. А. Лазарев, А. В. Демидов // «Информационные системы и технологиии (ИСиТ-2011)». — 2011. — Орёл: Госуниверситет — УНПК. — Т. 1. С. 180–185. (личное участие 50%).

9. Демидов, А. В. Обратный прокси-сервер в рамках системы управления информационным обменом сети web-порталов [Текст] / В. Т. Еременко, С. А. Лазарев, А. В. Демидов // «Информационные системы и технологиии (ИСиТ-2011)». — 2011. — Орёл: Госуниверситет — УНПК. — Т. 1. С. 170–174. (личное участие 30%).

10. Демидов, А. В. Проектирование подсистемы разграничения доступа к порталам органов государственной власти [Текст] / В. Т. Еременко, А. В. Демидов, Д. В. Агарков // «Информационное развитие России состояние, тендаенции и перспективы (региональный аспект)». Сборник научных статей 2-й межрегиональной научно-практической конференции. — 2011. — Орел: ОРАГС С. 5–11. (личное участие 40%).

11. Демидов, А. В. Управление доступом к ресурсам сети корпоративных порталов [Электронный ресурс] / С. А. Лазарев, А. В. Демидов // «Информационные технологиии в науке, образовании и производстве» (ИТНОП). Материалы V Международной научно-технической конференции. — 2012. — Режим доступа: http://irsit.ru/files/article/125.pdf. (личное участие 50%).

12. Демидов, А. В. Модель подсистемы разграничения доступа системы управления информационным обменом сети корпоративных порталов [Электронный ресурс] / А. В. Демидов // «Прикладная математика, управление и информатика». Сборник трудов Международной молодежной конференции. —

2012. — Режим доступа: http://meta-analysis.bsu.edu.ru/file.php/1/conferences/8/Sbornik_trudov_PMUI-2012_T_2.pdf. (личное участие 100%).

13. Demidov, A. V. Modeling of Access Control System of Gas Transportation Enterprise Portals [Электронный ресурс] / А. В. Демидов // Proceedings of International Conference on Intelligent Information Systems. — 2013. — Режим доступа: http://www.math.md/iis2013/IIS2013_Proceedings.pdf (личное участие 100%).

Свидетельства о регистрации программ для ЭВМ

14. Демидов, А. В. Подсистема аутентификации и авторизации системы управления информационным обменом сети корпоративных корпоративных порталов // И. С. Константинов, С. А. Лазарев, А. В. Демидов и др. — Свидетельство о государственной регистрации программы для ЭВМ №2011619386, зарегистрированно в реестре программ для ЭВМ 8 декабря 2011 г. (личное участие 20%).

15. Демидов, А. В. Подсистема проксирования HTTP-трафика системы управления информационным обменом сети корпоративных корпоративных порталов // И. С. Константинов, С. А. Лазарев, А. В. Демидов и др. — Свидетельство о государственной регистрации программы для ЭВМ №2011619387, зарегистрированно в реестре программ для ЭВМ 8 декабря 2011 г. (личное участие 20%).

16. Демидов, А. В. Клиентская подсистема аутентификации пользователей в сети корпоративных порталов с применением портативного цифрового устройства доступа // И. С. Константинов, С. А. Лазарев, П. П. Силаев, А. В. Демидов — Свидетельство о государственной регистрации программы для ЭВМ №2012616860, зарегистрированно в реестре программ для ЭВМ 1 августа 2012 г. (личное участие 20%).

ЛР ИД №00670 от 05.01.2000 г.
Подписано к печати 01.11.2013 г.
Усл. печ. л.1,00 Тираж 100 экз.
Заказ №168

Полиграфический отдел ФГБОУ ВПО «Госуниверситет — УНПК»
302030, г. Орёл, ул. Московская, 65