Вестник Московского международного университета

научный электронный журнал

1 / 2018

Обеспечение заданного уровня безопасности при решении функциональных задач электронного документооборота в образовательном процессе высшего образования

КЕЛДЫШ Наталья Всеволодовна

АНОВО «Московский Международный Университет», NKeldish@rambler.ru

Ключевые слова:
электронная образовательная среда, информационная система, система электронного документооборота, защита информации, информационный обмен, типология задач классификации

Аннотация:
в статье рассматривается возможности формирования единого информационного пространства ВУЗа, формулируется оптимизационная задача синтеза структуры подсистемы защищенного обмена информацией, проведен анализ применения известных подходов, определены основные этапы и принципы решения в интересах распределенной ведомственной системы электронного документооборота.

Подписана к печати: 22 октября 2018 года

Введение

В настоящее время информационный обмен является неотъемлемым элементом решения большинства практических задач управления, учета и информационного обеспечения электронной образовательной среды в сфере высшего образования. Организация обмена информацией, осуществляется на основе открытых сетей передачи данных и телефонной сети общего пользования с привлечением провайдеров телекоммуникационных услуг и телекоммуникационного оборудования для построения «собственных» сетей передачи данных. Основным требованием для разработки подсистемы обмена является обеспечение заданных уровней производительности и надежности функционирования.

Объекты и методы исследований

При организации защищенного информационного обмена в число основных требований на разработку входит также обеспечение заданного уровня безопасности передачи информации. При этом каждое из перечисленных условий имеет антагонистический характер, так как улучшение одного показателя приводит к ухудшению остальных. Задача синтеза оптимальной структуры подсистемы защищенного обмена информацией (ПЗОИ), которая может быть формализована в виде оптимизационной задачи на множестве допустимых структур, не имеет общего универсального решения [9]. Частное решение, полученное для конкретных условий применения, имеет индивидуальный характер, что практически исключает возможность его применения при других условиях. Все это обусловлено актуальностью постановки задачи синтеза, которая применительно к обеспечению ведомственного распределенного электронного документооборота может быть формализована в виде задачи поиска подмножества (), доставляющего локальный максимум целевой функции (*T*):

$$\hat{S}_0 = \arg\max_{H_k \subset B} T(S, N_k, M_k, R_k, C_k),$$

где $S = \{s_i\}, i = \overline{1,n}$ – множество типов коммуникаций, программных и технических

средств, а также типов структур подсистемы, допустимое для разработки ПЗОИ;

$N_k = f_1(\hat{S}_k),\ M_k = f_2(\hat{S}_k),\ R_k = f_3(\hat{S}_k),\ C_k = f_4(\hat{S}_k)$ – показатели надежности, производительности, безопасности обмена и стоимости разработки *k*-го варианта ПЗОИ соответственно;

$\hat{S}_k = \{s_j\},\ j = \overline{1, m_k}$ – подмножество коммуникаций, типов средств и структур, используемое для разработки *k*-го варианта ПЗОИ;

$T(S, N_k, M_k, R_k, C_k)$ – целевая функция, характеризующая эффективность обмена информацией в процессе решения функциональных задач ведомственной распределенной системы электронного документооборота;

$H_k = \{N_k, M_k, R_k, C_k\}$ – множество характеристик *k*-го варианта ПЗОИ;

$B = \{N_0, M_0, R_0, C_0\}$ – множество характеристик ПЗОИ, определенное заказчиком ведомственной распределенной системы электронного документооборота.

Рассмотрим возможность применения известных подходов к построению подсистемы защищенного обмена информацией для обеспе-

чения функционирования распределенной системы электронного документооборота ВУЗа.

Исходя из особенностей эффективного информационно-технологического формирования ВУЗа, автоматизированная система электронного документооборота должна обладать следующими особенностями:

ü территориальная распределённость и иерархичность структуры системы;

ü обеспечение многопользовательского режима;

ü возможность одновременной обработки и хранения информации разного уровня конфиденциальности;

ü поэтапное развертывание системы и оснащение объектов информатизации;

ü возможность обработки массивов неформализованных и слабо структурированных данных;

ü функционирование всех объектов информатизации в едином информационном пространстве.

Однако до настоящего времени, как правило, информационные и телекоммуникационные технологии создавались и развивались обособленно, а при разработке распределенных информационных систем синтез информационно-прикладного и телекоммуникационного компонентов проводился автономно. Данная ситуация объясняется в первую очередь существенным превышением скорости передачи данных над скоростью внутрисистемной обработки данных, имевшим место вплоть до недавних пор [2]. Существующие требования, предъявляемые к оперативности передачи и обработки данных, а также различия в методических подходах к синтезу информационной и

телекоммуникационной составляющих объективно не

способствовали переходу к совместной оптимизации при обосновании структуры ПЗОИ.

Возможности локальной оптимизации информационного и телекоммуникационного компонентов значительно ограничены вследствие исчерпания множества возможностей имеющихся резервов и сопоставимости скоростей обработки и передачи данных, достигаемых при использовании современной элементной базы.

Продолжение практики локального обоснования компонентов ПЗОИ в ходе разработки информационной системы электронного документооборота в деятельности вузов, может привести к несбалансированности по параметрам, а, следовательно, и по ресурсам.

В конечном итоге это ведет к обесцениванию всей работы по обоснованию структуры подсистемы защищенного обмена информацией.

Наиболее перспективные подходы для построения защищенного обмена информацией основаны на использовании криптографических методов, протокольно-алгоритмического аппарата защищенных виртуальных сетей (VPN) и конвертации протоколов (мультипротокольные телекоммуникационные взаимодействия) [3].

В существующих телекоммуникационных системах, как правило, задачи обеспечения безопасности информационных и телекоммуникационных систем в интересах отдельных потребителей решались путем создания защищенных специализированных сетей передачи данных, ориентированных на распределенную обработку информации [6]. Характерными чертами этих сетей являются специфическое исполнение комплексов технических средств и в некоторых случаях использование специализированного протокольного базиса, что приводит к высокой стоимости развертывания и эксплуатации. Кроме того, при реализации закрытых телекоммуникационных систем использовался принцип коммутации каналов, позволяющий строить сети, обеспечивающие связь по принципу «точка-точка».

Суть менее затратного подхода заключается в использовании ресурсов существующих сетей общего пользования для передачи информации, содержащих сведения, составляющие конфиденциальную информацию. Наиболее прогрессивным направлением при реализации сетевой технологии является использование коммутации пакетов, что позволяет более рационально организовывать каналы связи «каждый с каждым», обеспечивая централизованную политику безопасности и централизованное управление трафиком.

В целях экономии затрат технические средства ПЗОИ должны обеспечивать надежность функционирования собственных сетей потребителей и безопасную транспортировку информации по незащищенным первичным каналам и уже существующим сетям передачи данных, имеющим различные протокольные стеки [7]. При этом внутренние сети должны быть защищены в первую очередь от «внешних» атак, приводящих к перегрузке средств коммутации, отключению отдельных абонентов и невозможности обмена информацией.

Пользователю должны предоставляться одна-две точки доступа (транспортные точки доступа) для подключения одиночных рабочих станций (ПЭВМ) или локальных вычислительных сетей. При этом ресурсы каналов передачи данных должны использоваться интегрально и обеспечивать обмен файлами, сообщениями, информацией в Web-пространстве, включая на последующих этапах обмен речевой информацией (технология

IP-телефонии) и видео - информацией. В состав технических средств ПЗОИ должны входить устройства коммутации и менеджеры управления для построения собственных сетей потребителя, а также защищенные серверы баз данных, почтовые, Web- и файловые серверы [4].

Для интеграции средств системы и ПЗОИ предлагается ввести промежуточную сущность и через нее осуществить интеграцию.

Таким объектом может выступать, например, глобальная роль пользователя в системе. В ПЗОИ передается запрос, содержащий имя пользователя, а возвращается список глобальных ролей для этого пользователя. В ПЗОИ роль представлена как объект доступа, а пользователь является субъектом доступа. Систему ролей можно сделать достаточно разветвленной и иерархической, что позволит достаточно гибко настраивать доступ в системе.

ПЗОИ будет хранить отображения многие-ко-многим пользователей на роли, а система будет хранить отображения ролей на действия над объектами.

Проблема этого варианта заключается в том, что для работы более или менее сложной системы необходимы как минимум локальные роли, а как максимум динамические. Локальные роли – это роли, зависящие от конкретного объекта в системе, например роль ректора ВУЗа. Динамические – это роли, которые могут зависеть от контекста, времени суток, сеанса и т.п.

Предлагается использовать собственный механизм мандатного распределения доступа в ПЗОИ. Т.е. передается запрос на мандат для пользователя, далее система по мандату определяет права на объекты системы, в там числе и «роли».

Кроме того, в мандате ПЗОИ помимо уровня доступа имеются категории, которые мы используем по прямому назначению, разграничивая доступ к отдельным ресурсам. Например, к документообороту, к частям оргструктуры и т.д.

Это является наиболее хорошим вариантом, т.к. во-первых не заставляем ПЗОИ делать излишнюю работу, а во-вторых разграничиваем доступ на верхнем уровне с помощью мандатов. Для этого необходимо будет разработать соответствие мандатным уровням и категориям на отдельные действия в системе (это задача этапа анализа), а также разработать средства для удобной настройки соответствия мандатов и действий в системе (разрешить карточку – запретить карточку).

Основные моменты:

– роль, ее описание и ввод в систему выступает как объект доступа;

– при создании «роли» осуществляется контроль службой безопасности ее корректности с точки зрения правил разграничения доступа к ресурсам, фиксация роли и учет как нового объекта в системе;

– «роль» это таблица (матрица) доступа к данным (папкам, файлам, записям, полям записи и пр.) с определенными уровнями (чтение, запись и пр.);

– далее через программный интерфейс, проводится контроль доступа пользователя с определенным мандатом к ранее введенной «роли»;

– по результатам проверки соответствия пользователя и роли принимается решение о его доступе к действиям, предписанным по ролевому механизму.

Учет специфики электронного документооборота и изложенных результатов сравнительного анализа вариантов организации информационного обмена обусловливает необходимость реализации следующих принципов построения защищенной подсистемы обмена:

– использование незащищенных первичных каналов для транспортировки информации;

– организация связи по схеме «каждый с каждым»;

– реализация единой политики безопасности в интересах обеспечения безопасности транспортировки информации;

– централизация управления ресурсами ПЗОИ.

Таким образом, основные этапы решения задачи синтеза рациональной структуры подсистемы защищенного обмена информацией в рамках автоматизированной системы электронного документооборота организации могут быть определены в следующем виде:

– определение порядка и критериев выбора программно-технических средств, обеспечивающих выполнение требований по производительности и по безопасности;

– построение модели оценки затрат на создание и функционирование комплекса средств автоматизации подсистемы обмена информацией;

– формирование целевой функции и ограничений для выбора рационального варианта структуры комплекса средств автоматизации подсистемы обмена информацией;

– выбор и обоснование метода решения оптимизационной задачи [5].

Реализация изложенного подхода обеспечивает разработку информационного и телекоммуникационного компонентов подсистемы обмена, сбалансированных по параметрам и ресурсам. В конечном итоге, это ведет к повышению эффективности функционирования распределенной информационной системы документооборота в образовательном процессе ВУЗа.

Литература

1. Баканова Н. Б. Проектирование подсистем сбора и анализ информации для территориально распределенных информационных систем // Научно-техническая ин-формация. Серия 1. Организация и методика информационной работы / Нижегородский госуниверситет. – Нижний - Новгород, 2006.– С. 26-38.

2. Дудин Б. Е., Захарова Э. Г., Сметанин Ю. Г. Информационно-вычислительные технологии в распределенной среде. Обзор // Научно-техническая информация. Серия 2. Информационные процессы и системы / Нижегородский госуниверситет. – Нижний - Новгород, 2008.– С. 16-32.

3. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. – М. : КУДИЦ-ОБРАЗ, 2001. – С. 12-18.

4. Келдыш Н. В. Направления развития и безопасности современных систем ор-ганов управления. // Материалы Научно-практ. конференции / ВА МО. – М., 2007.– С. 15-33

5. Келдыш Н. В. Подсистема автоматизированного документооборота перспек-тивной системы управления кадрового органа. // Научно-метод. сборник № 56 / ВА МО. – М., 2009. –.С. 60-66.

6. Олифер В. Г., Олифер И. А. Компьютерные сети. Принципы, технологии, прото-колы. – СПб.: Питер, 2001.

7. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпора-тивных сетях и системах. – М. : ДМК Пресс, 2002. – С. 16-28.

8. Штрик А. А. Использование информационно-коммуникационных технологий для эконо-мического развития и государственного управления в странах современного мира. // Приложение к журналу «Информационные технологии». – 2009. – № 6. – С. 26 – 38.

9. Шаламов А. С. Создание информационно-телекоммуникационных систем высо-кой доступности на принципах CALS. // Наукоёмкие технологии. – 2006. – № 2. – С. 10-14.

Providing a given level of security when solving the functional problems of electronic document turnover in the educational process of higher

education

KELDISH N

ANOHE "Moscow International University", NKeldish@rambler.ru

Keywords:
electronic educational environment, information system, electronic document management system, information protection, information exchange, typology of classification problems.

Annotation:
the article discusses the possibilities of forming a unified information space of the university, formulates the optimization task of synthesizing the structure of the protected information exchange subsystem, analyzes the application of known approaches, determines the main steps and principles of the solution in the interests of a distributed departmental electronic document management system.

Цитирование: Келдыш Н. В. Обеспечение заданного уровня безопасности при решении функциональных задач электронного документооборота в образовательном процессе высшего образования // Вестник Московского международного университета. 2018.№1 (1), URL: https://vestnik.mi.university/journal/article.php?id=2133.
Cited as: Keldish N. V. “Providing a given level of security when solving the functional problems of electronic document turnover in the educational process of higher education” // Vestnik. №1 (1), (2018):