УДК 004.414.22

Р. В. Бубнов, А. С. Черников

# ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ДЛЯ ПОДДЕРЖКИ УПРАВЛЕНИЯ УНИВЕРСИТЕТОМ

*Рассмотрены особенности интегрированных информационных систем для поддержки управления университетом с точки зрения их информационного наполнения, архитектуры и администрирования. Сформулированы основные принципы обеспечения информационной безопасности применительно к таким системам. Приведены практические рекомендации по формированию и поддержанию режима информационной безопасности для этих систем, предложена методика разграничения прав доступа к базам данных произвольной структуры.*

Проблема создания эффективной интегрированной информационной системы (ИИС) для поддержки управления университетом становится все более актуальной в условиях вхождения России в Болонский процесс и связанного с этим введения единой системы кредитных зачетов, возрастания мобильности студентов, динамики учебных планов, разнообразия и объема предоставляемых образовательных услуг.

Действительно, наряду с общей тенденцией возрастания количества информации появление новых специальностей и специализаций, внедрение бакалавриата и магистратуры, второго образования, платных форм подготовки и переподготовки требует привлечения значительных дополнительных интеллектуальных ресурсов и перехода на новый качественный уровень обработки информации с точки зрения не только ее объема, но и скорости обработки.

Эффективное управление университетом возможно, если информация о деятельности его подразделений собирается, обрабатывается и становится доступной всем участникам процесса в реальном или квазиреальном масштабе времени, что достижимо только при использовании компьютерных сетей.

Поскольку возрастает доля внешней деятельности университета и необходимо наряду с традиционным внутриуниверситетским обменом информацией осуществлять ведение общих баз данных с отечественными и зарубежными партнерами-университетами (например, по со-

вместно обучаемым студентам или совместно выполняемым научным проектам), то создаваемые информационные системы должны быть приспособлены к функционированию в сети Internet.

Использование ИИС позволяет на качественно новом уровне обеспечивать поддержку основных видов деятельности в университете:

— архивной (хранение личных дел сотрудников, студентов, нормативно-правовых документов, отчетов и др.);

— текущей (информационное обеспечение процессов повседневной деятельности университета);

— аналитической (информационное обеспечение процессов оперативного и стратегического планирования различных сторон деятельности университета).

Использование ИИС позволяет обеспечивать эффективную поддержку управления основными направлениями деятельности университета:

— учебным процессом (разработка учебных планов и программ, расчет и распределение нагрузки преподавателей, учет успеваемости и посещаемости студентов, составление расписаний занятий, консультаций, экзаменов и т.д.);

— научной работой (организация и проведение научно-исследовательских и опытно-конструкторских работ, конкурсов грантов, научно-технических конференций и выставок, подготовка публикаций, научно-технических отчетов и т.д.);

— административно-хозяйственной деятельностью (работа с кадрами, ведение документооборота, ремонт и обслуживание зданий, помещений и оборудования, транспортное обслуживание, связь и т.д.);

— международной деятельностью (набор иностранных студентов, подготовка международных договоров и контрактов, сопровождение международных проектов, визовая поддержка и организация визитов и обменов студентами и преподавателями, работа с международными грантами и т.д.);

— финансово-хозяйственной деятельностью (планирование финансовой деятельности, учет движения материальных ценностей и финансовых ресурсов, планирование сметы расходов, расчет различных выплат сотрудникам и студентам университета, выплат по закупкам приборов и оборудования, услугам сторонних организаций и т.д.).

ИИС позволяет обеспечить персонализированный доступ к информации для студентов, аспирантов и сотрудников университета. Всем пользователям может быть предоставлен доступ к двум видам информации:

— к справочной информации общего пользования, такой как норма-

тивные документы, расписания занятий, открытые отчеты, файлы электронной библиотеки и т.п. (эта информация может просматриваться и копироваться, но ее нельзя модифицировать);

— к персональной информации личного и производственного характера, такой как личные данные пользователя, индивидуальный учебный план студента или аспиранта, расписание занятий, индивидуальный план работы преподавателя, зачетная или экзаменационная ведомость и т.п. (эта информация может не только просматриваться и копироваться, но и при определенных условиях модифицироваться).

Таким образом, использование ИИС в университете позволяет создать единую информационную среду, которая обеспечивает простоту и эффективность обмена информацией между любыми взаимодействующими структурами университета, уменьшает объем операций с бумажными документами, поддерживает не только текущую учебную, научную, административную деятельность университета, но и оперативное и стратегическое планирование, ускоряет процессы подготовки, принятия и выполнения управленческих решений.

**Особенности ИИС для поддержки управления университетом.** Фирменные образцы ИИС с момента появления наиболее широко применяются для поддержки управления предприятиями, банками, коммерческими организациями и другими учреждениями. В качестве ядра в этих системах используются такие продукты, как Interbase, R/3, Oracle, MS SQL Server, Sybase и др. ИИС университетского типа появились несколько позже. Первыми версиями таких систем были адаптированные к университетским задачам системы, изначально разработанные для поддержки управления предприятиями (например, R/3, созданная немецкой фирмой SAP). Они были внедрены в университетах Германии, США, Великобритании и других стран наряду с такими системами, как система “QL Students” компании MicroCompass Systems Limited, специально разработанными для университетов.

Вместе с тем, установка любой из перечисленных ИИС в университете требует ее адаптации к местным условиям на стадиях инсталляции и работы с ней, что практически исключает возможность самостоятельного сопровождения и доработки системы университетом в процессе эксплуатации.

Версии ИИС, разработанные для зарубежных университетов, не подходят для российских вузов ввиду множественных различий в законодательной базе, структуре управления университетами, принципах организации учебного процесса, научно-исследовательских работ и др. В настоящее время известна только одна ИИС, разработанная для российских университетов и в той или иной степени поддерживающая

различные виды их деятельности. Это система "Университет" компании REDLAB, созданная на базе платформы SAP R/3 и внедренная на одном из факультетов МГУ им. М.В. Ломоносова. Вместе с тем, она не получила широкого распространения из-за ряда присущих ей недостатков, включая дороговизну.

При проектировании ИИС для поддержки управления университетом следует учитывать особенности информационной структуры, архитектуры и администрирования ИИС. Далее рассмотрим каждую из особенностей более подробно.

*Особенности информационной структуры ИИС*. К ним можно отнести следующие особенности.

1. Большая степень ротации контингента пользователей. В течение года контингент пользователей ИИС университета изменяется на 15–20% только из-за набора и выпуска студентов и аспирантов.

2. Сложная структура контингента пользователей. В университете с развитой инфраструктурой присутствуют самые различные категории пользователей ИИС: студенты, аспиранты, преподаватели, научные сотрудники, инженерно-технические работники, медики, юристы, психологи, экологи и т.д. Уровень компьютерной подготовки пользователей изменяется в широких пределах: от начальной до профессиональной. Некоторые категории пользователей могут изменять свой статус. Например, один и тот же студент в процессе обучения может иметь несколько статусов: "учится", "академический отпуск", "представлен к отчислению", "отчислен" и т.п. У каждого пользователя одновременно может быть не одна, а несколько ролей. Например, преподаватель одновременно может по совместительству быть научным работником, выполнять функции куратора группы, заместителя декана и т.п.

3. Разнообразие видов деятельности. В стенах вуза происходит не только обучение студентов и аспирантов, но и переподготовка специалистов, ведутся научно-исследовательские и опытно-конструкторские работы, международные проекты. Университет может иметь собственные производственные мощности, библиотеки, медицинские учреждения, общежития, спортивно-оздоровительные лагеря и комплексы, школы, детские сады и т.п. ИИС университета должна не только охватывать все аспекты его деятельности, но и обеспечивать максимально близкое к естественному взаимодействие распределенных субъектов в процессе принятия решений, требуемое многообразие вариантов представления однотипной информации, адаптируемость к многообразию запросов пользователей, работающих на одном или на различных иерархических уровнях управления вузом.

4. Большой объем слабо структурированной информации. В университете имеется, как правило, электронная библиотека, подлежащие хранению учебно-методические материалы, приказы, архивные документы подразделений инфраструктуры и т.д.

5. Большой объем структурированной информации. Это информация, используемая для решения задач управления вузом.

6. Разнообразие используемых технических и программных средств. Необходимо учитывать разнообразие как с точки зрения используемых платформ, так и с точки зрения устаревания программных и аппаратных средств, используемых подразделениями университета.

7. Противоречивость требований к защите информации. Эта противоречивость в университетских ИИС обусловлена, с одной стороны, разнообразием видов деятельности и развитой инфраструктурой университета. Например, любой университет стремится сделать максимально доступной информацию о своих направлениях подготовки для абитуриентов, о расписании занятий и наличии литературы в библиотеке для студентов и сотрудников. В то же время, университет может проводить научно-исследовательские и опытно-конструкторские работы, которые по уровню секретности сопоставимы с работами, проводимыми на "закрытых" объектах. С другой стороны, один и тот же пользователь университетской ИИС может иметь совершенно различные уровни доступа к разным видам информации; при этом как уровни доступа, так и виды "открываемой" информации могут динамично изменяться. Например, профессор университета имеет полный доступ к информации об успеваемости студентов, может изменять оценки только по читаемому курсу, но не может давать допуск для пересдачи экзамена или зачета, не имеет доступа к личным делам сотрудников факультета. Тот же профессор, но избранный деканом факультета, имеет право подписи допусков для пересдачи экзаменов и зачетов, а также полный доступ к личным делам сотрудников и студентов возглавляемого факультета.

*Особенности архитектуры ИИС*. Внедрение ИИС или переход на новую ИИС как на предприятиях, так и в университетах является сложным процессом [1, 2]. Однако банки и крупные предприятия имеют некоторые преимущества перед университетами в решении данной проблемы.

Если предприятию необходимо в минимальный срок внедрить систему с функциональностью, максимально покрывающей предметную область, то предприятие исследует существующие системы, выбирает и закупает необходимую готовую систему, выделяет персонал для обслуживания и адаптации системы, средства на ее поддержку и развитие фирмой-поставщиком в рамках продукта и различных его приложений.

При необходимости предприятие может сменить технические средства (персональные компьютеры на рабочих местах операторов, серверы, сетевое оборудование) для улучшения производительности системы или для удовлетворения техническим требованиям данной системы.

В отличие от предприятий и банков, университеты Российской Федерации в большинстве своем вынуждены разрабатывать собственные ИИС для поддержки управления. Процесс разработки и поэтапного наращивания функциональности является длительным, не все принимаемые решения являются оптимальными с точки зрения множества возможных решений. Это обусловлено рядом причин, связанных с исторически сложившимися особенностями структуры, технического оснащения и экономического положения университетов.

Во-первых, бюджетные возможности университетов на приобретение, установку, сопровождение и дальнейшее развитие системы обычно весьма ограничены. Например, минимальный комплекс услуг по инсталляции такими фирмами, как SAP (Германия) или BAAN (США), полнофункциональной ИИС для управления предприятием стоит от миллиона долларов, а ее сопровождение — десятки тысяч долларов в год [3]. Большинство университетов России не в состоянии затрачивать такие средства.

Во-вторых, техническая база большинства университетов очень неоднородна, и ИИС приходится устанавливать на существующие (зачастую устаревшие) системные и программные средства. Это накладывает ограничения не только на выбор архитектуры ИИС, но и на быстродействие и совместимость программных и аппаратных средств.

В-третьих, университет имеет сложную организационную структуру. Если в большинстве организаций иерархия подразделений имеет небольшую вложенность (например, руководство организации — департамент — отдел — сектор) и разветвленность, то в университете в подобной иерархии может быть много уровней вложенности (например, ректорат — научно-учебный комплекс — факультет — курс — поток — группа) и более разветвленная структура.

В-четвертых, архитектура ИИС должна адекватно отражать сложную иерархию реального взаимодействия динамично изменяющихся ролей пользователей в процессе ввода, обработки информации и принятия управленческих решений. Например, оценку может поставить или изменить только преподаватель, решение об отчислении студента может принять ректор (проректор) после прохождения процедуры согласования по цепи: куратор группы — кафедра — заместитель декана — декан факультета. Таким образом, каждый участник процесса принятия

решений по разным видам деятельности университета имеет свои административные полномочия, и технические полномочия ИИС должны им полностью соответствовать. Данное требование касается также ИИС других организаций (банков, заводов и т.д.). Отличительной чертой ИИС университета является намного большее разнообразие статусов, а зачастую — их совмещение, для каждого из пользователей системы. Один человек может выступать в нескольких ролях, и эти роли могут изменяться (раз в полгода, год). Например, преподаватель может быть участником научно-исследовательской работы, деканом факультета и одновременно заведующим кафедрой и куратором студенческой группы. В следующем семестре этот же преподаватель может избавиться от части обязанностей или получить новые. Система должна поддерживать такую динамику изменения статусов сотрудников университета.

В-пятых, архитектура ИИС должна проектироваться с учетом особенностей жизненного цикла системы. Внедрение ИИС предполагает ее дальнейшую эксплуатацию, развитие и модернизацию. Большинство университетов из-за ограниченности финансовых ресурсов не может привлекать извне высококвалифицированных (и дорогостоящих) специалистов для сопровождения, развития и модернизации ИИС, а стремится это делать собственными силами. Следовательно, архитектура ИИС должна позволять эксплуатировать систему, не выходя за пределы возможностей штатного расписания университета по соответствующим категориям сотрудников.

Рассмотрим теперь влияние перечисленных факторов на архитектуру ИИС для поддержки управления университетом.

Разветвленная организационная структура университета подразумевает наличие сетевой обработки информации. Самым распространенным вариантом на данный момент является трехзвенная клиент-серверная архитектура (клиент — сервер приложений — сервер баз данных), которая используется в большинстве подобных ИИС.

Ввиду разнородности существующих в университете аппаратных и программных средств системе необходим “тонкий клиент”. В этом случае на машины пользователей системы ложится минимальная нагрузка при работе с системой, а основная нагрузка приходится на сервер приложений и сервер баз данных. Соответственно, учитывая ограниченные финансовые ресурсы университета, легче купить один мощный сервер баз данных, чем заменить ряд клиентских мест.

В результате, достаточно эффективным вариантом архитектуры системы является вариант, представленный на рис. 1. Подобный вариант

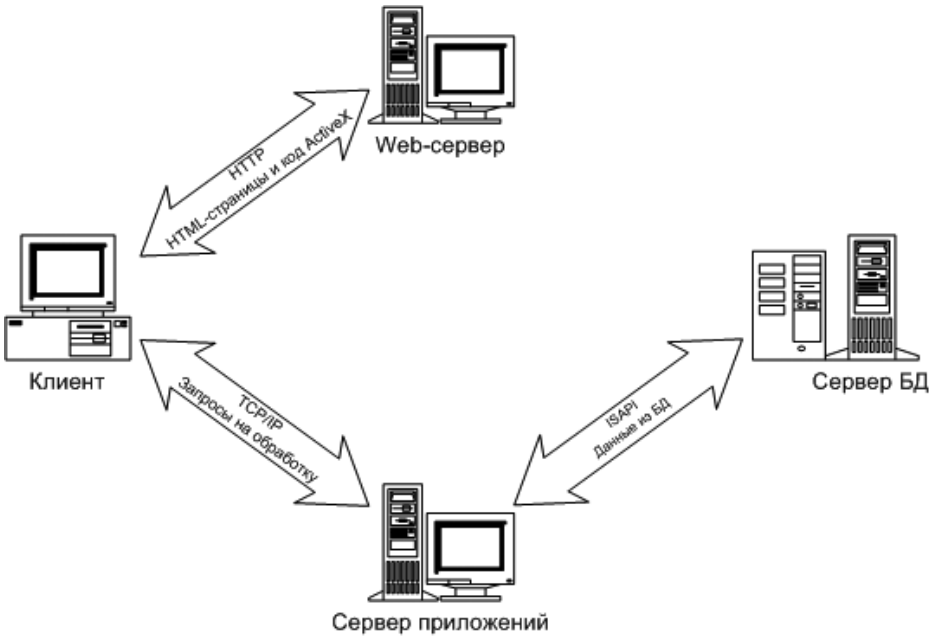


**Рис. 1. Архитектура системы (БД — база данных)**

архитектуры ИИС для поддержки управления вузом разработан и внедрен в МГТУ им. Н.Э. Баумана в рамках научно-учебного комплекса "Информатика и системы управления".

В данном варианте взаимодействие сервера и приложения происходит на основе трехуровневой клиент-серверной архитектуры. В качестве архитектуры промежуточного уровня выбрана технология MIDAS (Multi-tiered Distributed Application Services) компании Inprise. Технология MIDAS позволяет вынести все модули обработки данных на удаленную машину. Взаимодействие с такими удаленными модулями осуществляется через технологию DCOM или непосредственно по протоколу TCP/IP. Клиентское приложение для работы с подсистемой разграничения доступа выполнено в виде ActiveX-компонента. В целом, система функционирует следующим образом.

Клиент использует программу просмотра для доступа к системе. На сервере Web хранятся HTML-страницы и соответствующие ActiveX-компоненты. MIDAS выступает в роли сервера приложений, на нем исполняются удаленные модули доступа к данным.

Рассмотрим подробнее работу системы (рис. 2).

Клиент запрашивает страницу, соответствующую подсистеме разграничения доступа (этап 1). Сервер возвращает страницу (этап 2). Этапы 1 и 2 выполняются каждый раз либо лишь при изменении страницы — в зависимости от настроек клиента и сервера.

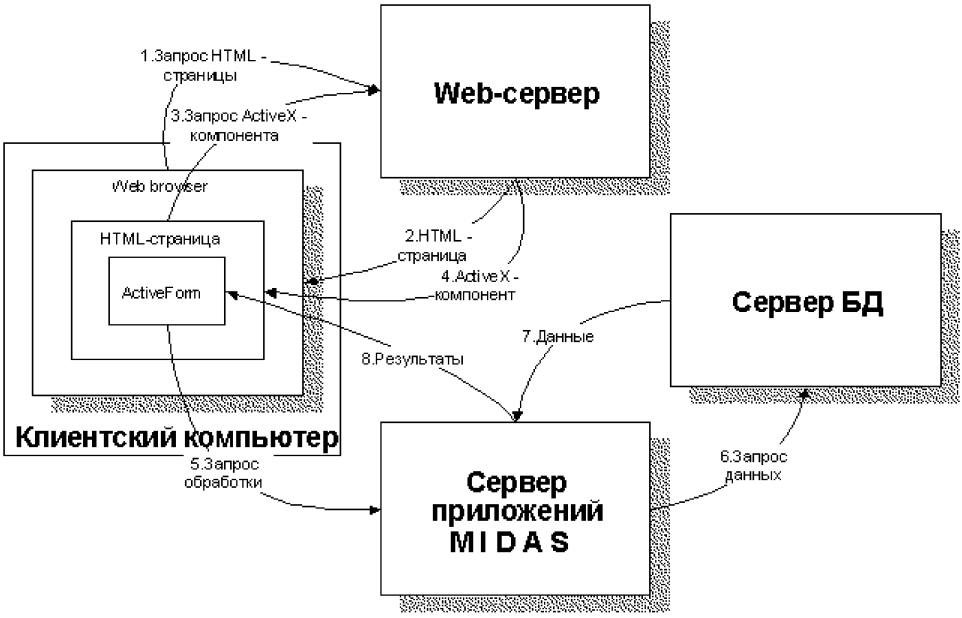


**Рис. 2. Взаимодействие компонентов в системе**

Программа просмотра разбирает страницу и запрашивает необходимые компоненты (этап 3). Сервер возвращает компоненты, и они устанавливаются на машине пользователя (этап 4). Этапы 3 и 4 выполняются только при смене версии компонента и обеспечивают автоматическое распространение и установку новых версий.

Этапы 5–8 могут повторяться произвольное число раз. При этом сервер приложений не обязательно будет просто передавать клиенту данные из баз данных. Он может производить с ними любые необходимые преобразования, а может сам генерировать данные, не обращаясь к базам данных.

Это один из многих вариантов построения системы; подобные системы разрабатываются сейчас многими университетами. Однако повышение степени автоматизации управления ставит университеты в зависимость от уровня безопасности разрабатываемых и используемых ИИС ввиду того, что в подобных системах содержится информация как общедоступная, так и конфиденциальная. Следовательно, доступ к информации должен быть разграничен для различных пользователей системы, а для этого необходим продуманный метод администрирования системы.

*Особенности администрирования ИИС*. Из-за сложной иерархии организационной структуры вуза и ее сильной разветвленности в ИИС для поддержки управления университетом необходимо обеспечить гибкий подход к распределению прав на администрирование системы.

Данное требование фактически состоит из двух.

1. Необходимо децентрализовать администрирование системы. Действительно, централизованное администрирование прав доступа к базе данных информационной системы неэффективно в силу разветвленной иерархической структуры управления в университете. Следовательно, системе необходим метод частичного делегирования прав доступа к базе данных от администраторов более высоких уровней администраторам низких уровней.

2. Необходимо разделять функции администратора системы и администратора базы данных; администратор системы не должен иметь прав доступа к базе данных. Исходя из того, что должностные инструкции университета строго определяют перечень лиц, имеющих право доступа к различного рода информации и ее изменению, системный администратор должен иметь право доступа к информации только на уровне файлов и не иметь доступа непосредственно к данным (например, к отметкам студентов) и, тем более, к их модификации. Доступ непосредственно к данным должен предоставляться администратору базы данных, который может делегировать часть своих полномочий администраторам более низких иерархических уровней. При этом персональные полномочия администраторов баз данных всех уровней должны подтверждаться их персональными должностными инструкциями.

Как правило, администрирование систем неразрывно связано с такими понятиями, как информационная безопасность и политика безопасности [4]. Системы, разработанные университетом самостоятельно, могут эксплуатироваться полномасштабно только при наличии систем защиты информации и хорошо продуманной политики безопасности. Именно последнее условие тормозит процесс внедрения многих информационных систем. Кроме этого, как было указано ранее, круг пользователей данной системы может выходить за рамки университета, т.е. система может использоваться как в сети Intranet, так и в сети Internet, что накладывает на систему безопасности более жесткие требования.

**Требования к обеспечению безопасности в ИИС для поддержки управления университетом**. Политика безопасности сочетает в себе законодательные, организационные и программно-технические меры, направленные на обеспечение информационной безопасности систем. Политика безопасности ИИС университета должна учитывать специфику работы вуза, его сложную разветвленную структуру управления и экономические трудности, характерные для большинства российских университетов.

Как известно, в России законодательной базой для обеспечения информационной безопасности систем является Федеральный закон “Об

информации, информатизации и защите информации" от 20 февраля 1995 г. [5] и Указ Президента Российской Федерации от 3 апреля 1995 г. [6]. Эти основополагающие документы носят в основном запретительный характер и, к сожалению, слабо препятствуют нарушениям, совершаемым в области информационных технологий.

Более эффективным в данном случае является организационный аспект информационной безопасности. Как правило, руководство каждой организации обращает внимание на режим безопасности и выделяет на обеспечение безопасности значительные ресурсы. При этом необходимо выработать политику безопасности, которая задает общее направление работам в данной области [7]. Применительно к университету политика безопасности должна преследовать следующие цели:

— обеспечение уровня безопасности, соответствующего нормативным документам, которыми руководствуется университет в своей деятельности;

— обеспечение безопасности в каждой функциональной области локальной сети университета (на кафедрах, в деканатах, в аудиториях);

— обеспечение подотчетности всех действий пользователей в ИИС;

— предоставление пользователям необходимой и достаточной информации для выполнения их служебных обязанностей;

— разработка планов восстановления системы после аварийных ситуаций с целью обеспечения бесперебойной работы системы;

— следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности).

Это далеко не полный перечень организационных мер, направленных на обеспечение информационной безопасности ИИС университета. Сюда можно включить также физическую защиту серверов базы данных, четкое разделение обязанностей сотрудников, минимизацию привилегий при работе с ИИС (т.е. пользователям выдаются только те права доступа, которые необходимы им для выполнения служебных обязанностей) и т.д.

Напомним, что именно реализация организационного аспекта информационной безопасности является первоочередной задачей и первым шагом на пути к построению системы защиты информации в ИИС университета. Если организационный аспект информационной безопасности не будет реализован в полной мере, то дальнейшее развитие системы безопасности просто бессмысленно.

Для поддержания режима информационной безопасности особенно важны программно-технические меры, поскольку основная угроза компьютерным системам исходит от самих этих систем (сбои оборудо-

вания, ошибки пользователей и администраторов и т.п.). Программно-технические меры образуют последний и самый важный рубеж информационной защиты, который может противостоять некомпетентности и неаккуратности при выполнении служебных обязанностей пользователями системы [4, 7]. В настоящей работе не будем рассматривать технические средства обеспечения информационной безопасности (брандмауэры, защита каналов связи, биопараметрические устройства считывания и т.д.), так как они являются дорогостоящими, а самостоятельная их реализация в рамках университета зачастую нецелесообразна или просто невозможна.

Для ИИС университета наиболее важными представляются следующие сервисы безопасности:

— идентификация и аутентификация;

— протоколирование и аудит;

— управление доступом к информации.

*Идентификация и аутентификация*. Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация — это первая "линия обороны", на которую попадает пользователь системы при попытке входа в ИИС [7].

К сожалению, для ИИС вуза надежная идентификация и аутентификация затруднена по следующим причинам.

1. Чем надежнее средство защиты, тем оно дороже. Особенно дороги средства измерения биометрических характеристик. Естественно, такие средства вуз не может приобрести и внедрить в ИИС.

2. Имеется противоречие между надежностью аутентификации и удобствами пользователя и системного администратора. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (на его место мог сесть другой человек), а это повышает вероятность подглядывания за вводом.

3. Почти все аутентификационные сущности можно узнать, украсть или подделать, что в случае сложной организационной структуры университета и особенностей его контингента представляет большую угрозу безопасности системы.

Таким образом, университетам необходимо найти компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Наиболее распространенным средством аутентификации для ИИС университета являются пароли. Основное достоинство аутентифика-

ции при помощи пароля — это простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемую для университета проверку подлинности пользователя. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Надежность паролей основывается на способности помнить их и хранить в тайне. Чтобы пароль был запоминающимся, его зачастую делают простым (имя знакомого человека, географическое название и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Иногда пароли с самого начала не являются тайной, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена (например, пароли системных пользователей в системе управления базами данных (СУБД) Oracle).

Пароли нередко сообщают коллегам, чтобы те смогли выполнить какие-либо нестандартные действия (например, подменить на некоторое время владельца пароля).

Пароль можно угадать, используя, например, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (алгоритм шифрования предполагается известным). Написать подобную программу сейчас способен почти каждый студент.

Один из существенных недостатков пароля — возможность его перехвата при передаче по сети. Необходимо использовать криптографию для шифрования паролей перед передачей по линиям связи.

Тем не менее, следующие меры позволяют значительно повысить надежность защиты при помощи паролей [7]:

— наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации);

— управление сроком действия паролей, их периодическая смена;

— ограничение числа неудачных попыток входа в систему (это затруднит применение метода грубой силы).

*Протоколирование и аудит*. Реализация протоколирования и аудита преследует следующие цели:

— обнаружение попыток нарушения информационной безопасности;

— обеспечение подотчетности пользователей и администраторов;

— обеспечение возможности восстановления последовательности событий;

— предоставление информации для выявления и анализа проблем.

Одной из особенностей протоколирования и аудита является их зависимость от других средств безопасности [5]. Идентификация и аутентификация являются исходной точкой подотчетности пользователей, логическое управление доступом защищает конфиденциальность и целостность регистрационной информации.

Обеспечение подотчетности пользователей ИИС важно, в первую очередь, как средство сдерживания. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Очевидно, если есть основания подозревать какого-либо пользователя в противоправных действиях, можно регистрировать его действия особенно детально. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и устранения некорректных изменений (если в протоколе присутствуют данные до и после модификации). Тем самым, защищается целостность информации, что очень важно для использования ИИС в университете.

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

*Управление доступом к информации*. Прежде чем перейти к рассмотрению подходов управления доступом к информации, рассмотрим на примере предложенной архитектуры ИИС варианты встраивания системы безопасности, т.е. системы разграничения прав доступа, и поясним, почему все подходы к управлению доступом основаны на сервере баз данных.

Возможны следующие варианты расположения системы разграничения доступа к информации: на уровне сервера приложений и на уровне базы данных.

В первом случае приложение, которое осуществляет политику безопасности, встраивается между базой данных и серверным компонентом (рис. 3), его функционирование заключается в том, что все данные, которые передаются от сервера базы данных клиентам и в обратном направлении, подвергаются модификации. Такое встраивание возможно благодаря отсутствию прямой связи между клиентом и сервером. При таком варианте возможна реализация гибкой системы разграничения прав доступа исходя из того, что в данном случае нет зависимости от средств разграничения доступа на уровне СУБД. Однако данный вариант имеет существенный недостаток: пользователь с помощью клиентского программного обеспечения типа SQLPlus [8] может осуществить непосредственное соединение с сервером базы данных. Это означает,

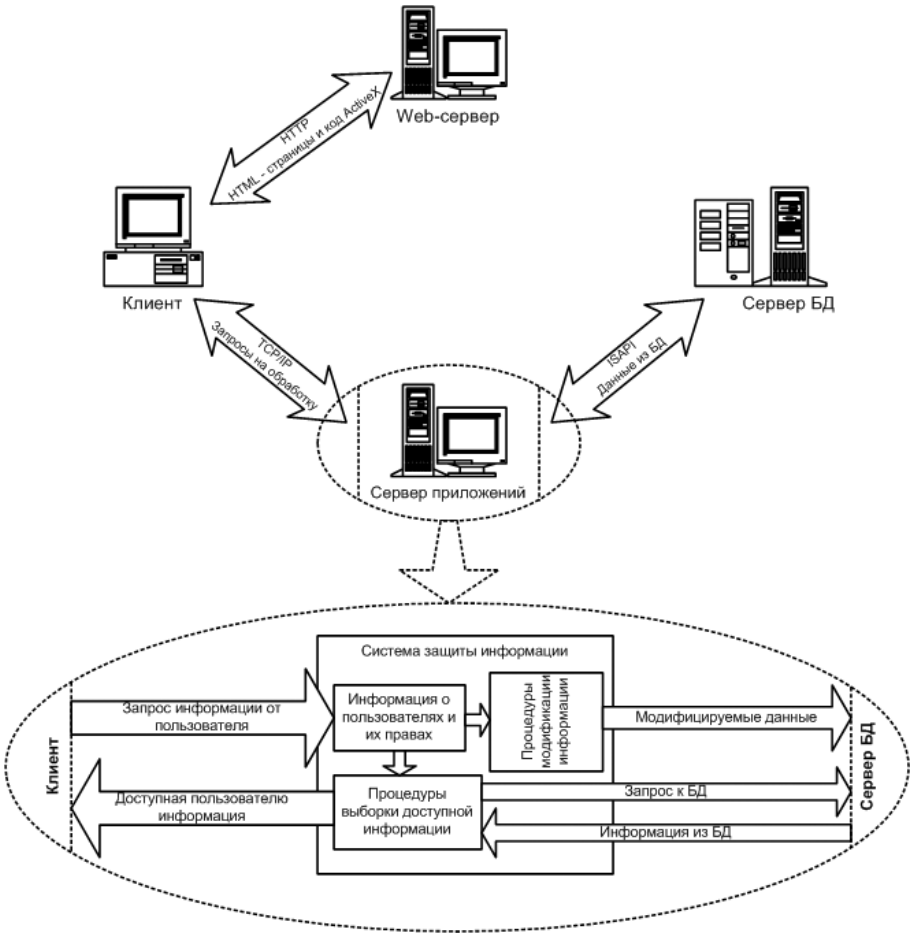


**Рис. 3. Расположение системы разграничения доступа к информации на уровне сервера приложений**

что систему защиты информации можно обойти с помощью штатных программных средств СУБД. Поскольку в СУБД нет стандартизированных средств предотвращения подключения SQL-консолей, с помощью которых пользователь может подсоединиться к системе, то данный подход является неприемлемым с точки зрения надежности.

В случае расположения системы разграничения доступа к информации на уровне базы данных возможно организовать защиту, которая обладает той же степенью надежности, что и базовые механизмы СУБД. К тому же, детальное рассмотрение возможностей различных СУБД показало, что все СУБД (за исключением облегченных вариантов типа MySQL [8]) обладают необходимым набором средств для организации системы защиты требуемого уровня (рис. 4).

Рассмотрим варианты управления доступом к информации. В настоящее время при разработке систем безопасности информационных

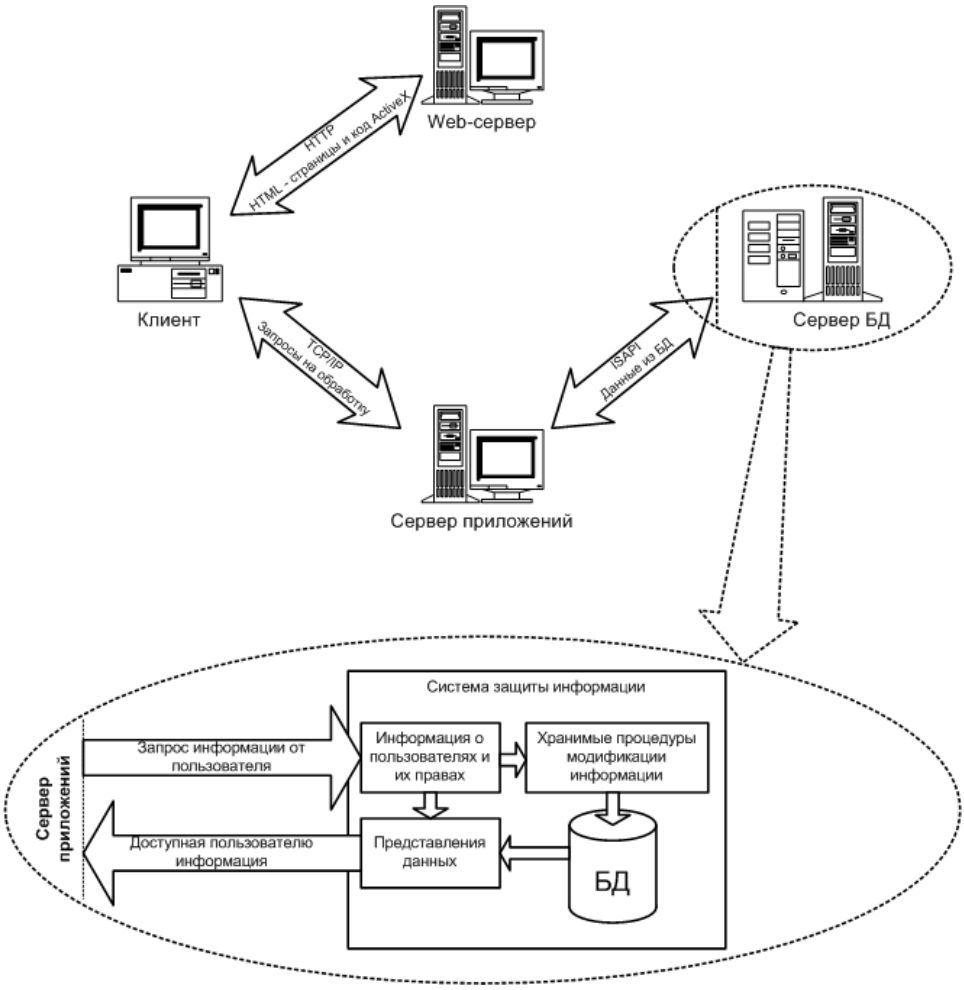


**Рис. 4. Расположение системы разграничения доступа к информации на уровне базы данных**

систем используются два известных подхода к определению полномочий пользователя — произвольное и принудительное управление доступом.

В случае произвольного управления (discretionary access control, DAC) явно указывается возможность доступа субъекта к объекту. Типичный пример DAC — это реализация контроля прав доступа к объектам в систему Windows NT, где всякий объект имеет ассоциированный с ним объект Security Descriptor, который имеет список ACL (Access Control List) из каталога ACE (Access Control Entry) [8]. Данные списки содержат уникальный идентификатор (ID) всех пользователей, которым разрешено определенное действие над объектом. В действующем стандарте языка SQL предусматривается поддержка только произвольного управления доступом. Она основана на двух более или менее

независимых частях языка SQL. Одна из них называется механизмом представлений, который может быть использован для скрытия очень важных данных от несанкционированных пользователей. Другая часть называется подсистемой полномочий и наделяет одних пользователей правом избирательно и динамически задавать различные полномочия другим пользователям, а также отбирать такие полномочия в случае необходимости.

В случае принудительного управления (mandatory access control, MAC) происходит сравнение набора признаков, ассоциированных с субъектом и объектом (отдельные признаки могут являться в общем случае множеством). Методы принудительного управления доступом применяются к базам данных, в которых данные имеют достаточно статичную структуру (например, к большим информационно-справочным системам). При этом в качестве признаков, составляющих метки безопасности, выбираются уровни доступа, предметные области и т.п. [8, 9].

На практике оба эти подхода реализуются в системе совместно, поскольку каждый из них эффективен для решения различных задач [4, 7]. Такой комбинированный тип управления доступом предполагает хранение информации о правах конкретного пользователя на осуществление операций чтения, редактирования, удаления и вставки данных как на уровне таблицы, так и на уровне конкретной строки в таблице. При этом осуществляется привязка меток безопасности к строкам защищаемой базы данных.

На первый взгляд, построение списка ACL для доступа к каждой строке базы данных не представляет проблем. Однако при рассмотрении данной задачи возникает вопрос, какие именно объекты базы данных должен видеть администратор для выполнения задач по разграничению доступа к информации. Для реализации отношений между различными таблицами базы данных СУБД поддерживает значительный объем служебной информации, не информативной для пользователя. Более того, можно утверждать: физическая структура базы данных является абсолютно неприемлемой для администрирования с точки зрения удобства (так как требует детального знания датологической модели базы данных). Поэтому предлагаемая методика разграничения доступа к базе данных произвольной структуры включает три этапа.

1. Отображение физической структуры базы данных в логическую. Данный этап является особенностью предлагаемой методики. На этом этапе происходит интерпретация физической структуры базы данных и определение на ее основе логической структуры (объектов), с которой в дальнейшем предстоит работать администраторам системы. Данный

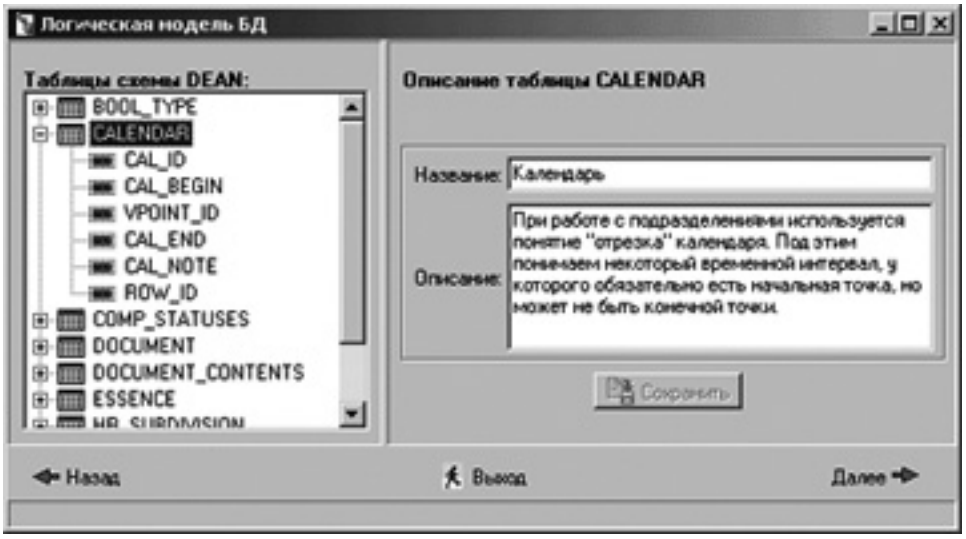


**Рис. 5. Утилита "Логическая модель базы данных"**

этап выполняется проектировщиками или разработчиками информационной системы (так как они в большей мере знают структуру базы данных) с помощью отдельной утилиты, доступ к которой никакому администратору не предоставляется. Администраторы всех уровней работают исключительно с логической моделью базы данных, созданной с помощью данной утилиты. Пример интерфейса данной утилиты приведен на рис. 5.

2. Построение иерархии учетных записей пользователей-администраторов системы. Нельзя утверждать, что администрирование в системе распределенное, если в системе нет отражения организационной структуры предприятия, которая является естественным механизмом группировки пользователей. Учитывая специфику предметной области университета, необходимо обеспечить назначение учетным записям пользователей определенных категорий или ролей. Данные роли определяются должностными обязанностями и инструкциями пользователей — сотрудников и студентов (рис. 6). Для каждой роли объем доступной информации и действия над ней должны быть определены нормативными документами университета. Назначение какой-либо из ролей учетной записи пользователя также должно соответствовать внутриорганизационным правилам, указанным в регламентирующих документах. При этом каждому пользователю может быть назначено несколько ролей, соответствующих его должностным обязанностям в определенный момент времени.

Отличительной чертой данного подхода к построению иерархии учетных записей является то, что когда определяется администратор

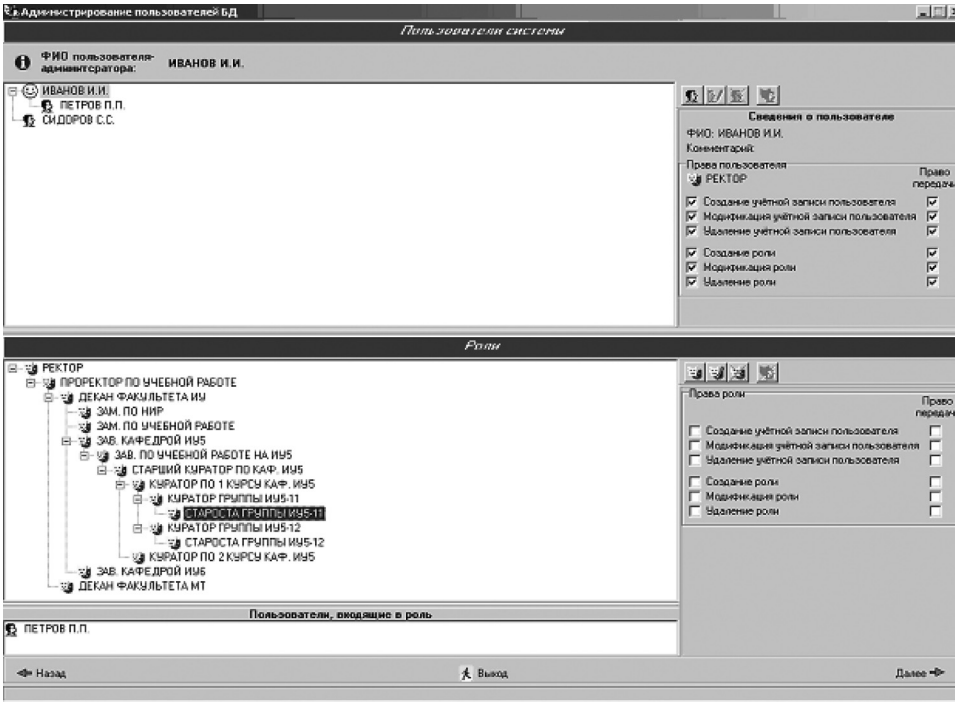


**Рис. 6. Утилита "Администрирование пользователей базы данных" — иерархия ролей пользователей**

более низкого уровня, то ему передается некоторое подмножество из множества объектов, доступных администратору верхнего уровня. Таким образом, реализовав данную концепцию "усечения прав" по уровням иерархии для ролей пользователей в автоматизированной системе разграничения прав доступа, можно воссоздать организационную структуру университета в рамках автоматизированной системы и, тем самым, повысить информационную безопасность системы и максимально приблизить ИИС к предметной области. Последнее очень важно при использовании системы пользователями, которые не знают структуру защищаемой базы данных, но хорошо разбираются в предметной области.

3. Назначение прав доступа к отдельным элементам данных. На данном этапе производится собственно администрирование прав доступа к данным. Для выборки строк, на которые распространяются вновь назначаемые права, используется подход QBE (Query By Example) в простой модификации.

Администратор более высокого уровня может изменить представление об объекте для администратора нижнего уровня как качественно (закрыв некоторые поля объекта), так и количественно, выбрав определенное подмножество строк. Например, администратор уровня фа-

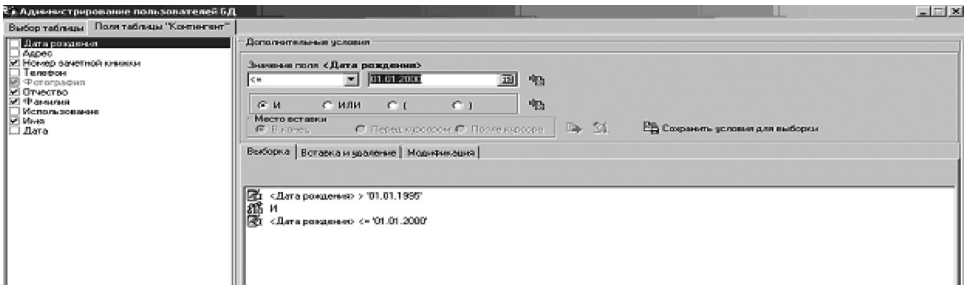


**Рис. 7. Утилита "Администрирование пользователей базы данных" — назначение прав доступа**

культета может делегировать право на администрирование студентов кафедры администратору этой кафедры. При этом может быть указано, что администратор более низкого уровня не может собственно видеть данные, которые он администрирует (рис. 7).

Этот этап является логическим продолжением предыдущего этапа, и для него справедливы все методы и способы реализации, указанные для предыдущего этапа.

**Заключение**. 1. В связи с выявленными особенностями информационной структуры и жизненного цикла ИИС университетского типа при их проектировании должны использоваться специфические критерии оптимизации.

2. Наиболее приемлемой архитектурой ИИС является трехуровневая клиент-серверная архитектура с "тонким клиентом".

3. Из-за сложной иерархии организационной структуры университета и ее сильной разветвленности необходимо использовать децентрализованное администрирование ИИС с разделением функций администратора системы и администратора базы данных.

4. Наиболее важными сервисами безопасности ИИС университета являются идентификация и аутентификация; протоколирование и аудит; управление доступом к информации.

5. Наиболее эффективным для ИИС университета является комбинированный тип управления доступом, сочетающий в себе DAC- и MAC-подходы.

Предложенная методика позволяет обеспечить разграничение прав доступа к базе данных произвольной структуры и разбивается на три основных этапа: отображение физической структуры базы данных в логическую; построение иерархии учетных записей пользователей-администраторов системы; назначение прав доступа к отдельным элементам данных.

Такой подход позволяет администраторам всех уровней работать исключительно с логической моделью базы данных. В тех случаях, когда это не диктуется производственной необходимостью, администра-

тор соответствующего уровня не имеет возможности видеть и изменять данные, которые он администрирует.

ИИС адекватно отражает существующую в университете структуру управления, так как каждому пользователю может быть назначена одна или несколько ролей, соответствующих его должностным обязанностям в данный момент времени.

Описанные принципы и методы внедрены в информационную систему "Контингент", эксплуатирующуюся в научно-учебном комплексе "Информатика и системы управления" МГТУ им. Н.Э. Баумана.

## СПИСОК ЛИТЕРАТУРЫ


1. Ландсберг С. Е., Геллер А. В. Создание автоматизированной системы управления вузом на базе локальной вычислительной сети компьютеров // Тез. докл. Всероссийской научно-методической конф. "Компьютерные технологии в высшем образовании". – СПб., 1994.
2. Автоматизированные системы управления вузом: Сб. науч. трудов. – Новосибирск: М-во высш. и сред. спец. образования РСФСР, 1980. – 152 с.
3. Кулапин Л. Г., Ландсберг С. Е. Эффективность использования телекоммуникаций в вузе в условиях ограниченных ресурсов // Тез. докл. Всероссийской научно-методической конф. "Телематика-95". – СПб., 1995.
4. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
5. Федеральный закон "Об информации, информатизации и защите информации". №24-ФЗ от 20.02.1995.
6. Указ Президента Российской Федерации "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации". №334 от 3.04.1995.
7. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.
8. Урман С. Oracle8. Программирование на языке PL/SQL. – М.: Изд-во "ЛОРИ", 1999.
9. Урман С. Oracle8i. Новые возможности программирования на языке PL/SQL. – М.: Изд-во "ЛОРИ", 2001.


Статья поступила в редакцию 25.12.2003

Роман Викторович Бубнов родился в 1978 г., окончил в 2002 г. МГТУ им. Н.Э. Баумана. Аспирант кафедры "Автоматизированные системы обработки информации и управления" МГТУ им. Н.Э. Баумана. Автор трех научных работ в области безопасности информационных систем.

R.V. Bubnov (b. 1978) graduated from the Bauman Moscow State Technical University in 2002. Post-graduate of "Automated systems of Data Processing and Control" department of the Bauman Moscow State Technical University. Author of 3 publications in the field of security of information systems.

Александр Сергеевич Черников родился в 1951 г., окончил в 1974 г. МВТУ им. Н.Э. Баумана. Канд. техн. наук, доцент кафедры "Компьютерные системы и сети", начальник учебно-научной лаборатории "Компьютерные информационные системы и технологии" МГТУ им. Н.Э. Баумана. Почетный д-р компьютерных наук Де Монтфортского университета (Великобритания). Академик Международной академии информатизации, член-корреспондент Международной академии информационных процессов и технологий. Автор более 70 научных работ в области информационно-управляющих систем.

A.S. Chernikov (b. 1951) graduated from the Bauman Moscow Higher Technical School in 1974. Ph.D. (Eng.), ass. professor of "Computer Systems and Networks" department, head of tutorial and scientific laboratory "Computer Information Systems and Technologies" of the Bauman Moscow State Technical University. Honorable Doctor of Computer Sciences of De Montfort University. Academician of the International Academy of Informatization, corresponding member of Academy of Information Processes and Technologies. Author of over 70 publications in the field of information and control systems.

---