ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТЬЮ ВУЗА

В.С. Замятин

В статье уточняются задачи систем управления компьютерными сетями ВУЗов, формулируются подходы к их решению, а также принципы построения комплексной системы управления информационно-вычислительными сетями в рамках рассматриваемой предметной деятельности. При этом особое внимание уделяется проблемам управления безопасностью и производительностью, как наиболее важным для обеспечения надежного функционирования компьютерных сетей и сетевых информационных систем.

В настоящий момент трудно найти организацию, в которой отсутствовала бы компьютерная сеть, обладающая внутренними информационными и вычислительными ресурсами и имеющая выход в глобальные сети. Что касается высших учебных заведений, то работы по созданию и обеспечению функционирования информационно-вычислительных сетей (ИВС) ведутся уже более десяти лет [1, 2] При этом, поскольку в настоящий момент ИВС ВУЗов уже построены и функционируют, на первый план выходит решение задач их гармоничного развития и эффективного использования сетевых ресурсов.

Решаются эти задачи с помощью средств сетевого управления, на основе использования системного подхода, предполагающего построение целостной системы управления, решающей все значимые задачи по управлению сетью и не содержащей слабых мест на стыках отдельных ее компонентов.

Рассмотрим основные особенности ИВС ВУЗов, влияющие на построение комплексной системы сетевого управления:

− ИВС ВУЗа представляет собой корпоративную сеть, объединяющую сотни рабочих станций пользователей, десятки серверов. Как правило, такая сеть территориально распределена и объединяет несколько зданий внутри города или даже несколько филиалов, расположенных в разных городах. Как следствие, ИВС ВУЗа имеет сложную топологию, в ней используются каналы передачи данных различной емкости;

− ИВС ВУЗа имеет выход в глобальные сети - как образовательные, так и коммерческие, с использованием нескольких производительных каналов. При этом практически всегда стоит проблема нехватки внешних канальных емкостей;

− накоплен большой объем разнородных информационных ресурсов, предназначенных как для внутренних, так и для внешних пользователей;

− ИВС ВУЗа обеспечивает решение большого числа задач с использованием различных сетевых приложений и сервисов;

− остро стоят вопросы администрирования различных категорий пользователей (управляющий персонал, преподаватели, студенты, сотрудники), обеспечения соответствующих механизмов разграничения доступа к ресурсам;

− ограничены возможности контроля за деятельностью пользователей, а также использования полностью централизованных механизмов сетевого управления;

− имеет место недостаток финансовых ресурсов, что обусловливает необходимость наиболее эффективного использования существующих аппаратных и программных средств за счет применения средств моделирования и оптимизации. Необходим взвешенный подход к модернизации ИВС, основанный на обеспечении принципа экономической целесообразности. Данный подход становится все более актуальным, поскольку в настоящий момент сложилась ситуация, в которой конечной целью фирм - производителей оборудования и программного обеспечения (ПО) является не выпуск качественного продукта, а максимизация прибыли, при этом маркетинговые решения зачастую становятся приоритетнее инженерно-технических. В результате мероприятия, направленные на оптимизацию функционирования работы существующей ИВС, могут оказаться эффективнее, чем приобретение нового оборудования.

Перечислим основные задачи сетевого управления:

− управление безопасностью;
− управление производительностью;
− учет использования ресурсов;
− управление сбоями;

− мониторинг текущего состояния ИВС, поддержка принятия решений по модернизации и управление модернизацией;

− моделирование работы существующих сетей, включая анализ нагрузки на отдельные их участки;

− управление конфигурацией.

Ключевым и первоочередным является решение первых трех задач: управление безопасностью, производительностью и учет использования ресурсов. Остальные задачи можно в принципе рассматривать как составные части вышеперечисленных. Например, система управления сбоями может рассматриваться как подсистема системы управления безопасностью, моделирование – как подсистема управления производительностью, а мониторинг необходим как для решения задач обеспечения производительности, так и безопасности.

Управление безопасностью

Прежде всего, определим наиболее актуальные *угрозы*, которые имеют место при функционировании ИВС:

1. Спам. Данная угроза становится все более актуальной, поскольку объем нежелательной корреспонденции постоянно увеличивается. Доля спама в общем объеме почтовых отправлений в настоящее время уже значительно превышает долю полезной корреспонденции. При этом не существует эффективных методов борьбы со спамом, позволяющих обеспечить полную защиту пользовательских почтовых ящиков, поскольку в рассылке спама чаще всего принимают участие пользовательские компьютеры, зараженные вредоносными программами. Кроме использования вредоносного ПО стали появляться экономические механизмы, позволяющие эффективно распространять спам – финансовые пирамиды, вовлекающие в процесс распространения спама все большее число пользователей, желающих заработать. Зачастую подобные пользователи даже не предполагают о характере совершаемых ими действий, поскольку механизмы почтовой рассылки спрятаны внутри распространяемого ПО. Принимаемые в некоторых странах законы, призванные бороться со спамом, практически не влияют на его распространение. При этом следует отметить два аспекта данной угрозы: возможна потеря полезной корреспонденции, как в почтовых ящиках пользователей, так и на серверах, вследствие ложных срабатываний антиспамерских фильтров; большой объем паразитного трафика, забивающего каналы связи и излишне нагружающего почтовые серверы.

2. Вредоносное программное обеспечение. Сюда следует отнести компьютерные вирусы и троянские программы. Следует отметить, что характер вредоносного ПО в последнее время претерпел значительные изменения. Изменились механизмы его распространения. В основном вредоносный код попадает на компьютер через различные уязвимые места в системах сетевой защиты, зачастую без участия пользователя (сетевые и почтовые черви). Значительно снизилась в последнее время доля вредоносного ПО, распространяющегося методами социальной инженерии. Изменились цели и мотивы создателей вредоносного ПО. Если раньше целями при создании вирусов в большей части являлись самоутверждение, забава и т.п., то в настоящий момент появилась экономическая составляющая. Множество зараженных компьютеров, доступ к которым можно получить удаленно, можно выгодно «продать» тем же распространителям спама. Еще одной из целей распространения вредоносного ПО является фишинг – воровство номеров кредитных карт, паролей, конфиденциальной информации и пр. Следует отметить, что в Бийском технологическом институте уже зафиксированы факты утечки паролей для доступа к ресурсам за счет использования вредоносного ПО. Кроме вышеперечисленных действий, вредоносное ПО может осуществлять и другие угрозы: уничтожать и модифицировать информацию, блокировать информацию и информационные ресурсы (ограничивать доступность, например, генерируя большой объем паразитного трафика, выводить из строя компоненты ИВС).

3. Несанкционированный доступ к конфиденциальной информации, незаконное тиражирование информационных ресурсов. В ИВС ВУЗа существует большой объем разнородной информации, включая персональные данные преподавателей, сотрудников, студентов, различного рода интеллектуальная информация. Соответственно, существует угроза разглашения конфиденциальных данных. В связи с возрастающей конкуренцией на рынке образовательных услуг появилась проблема разграничения доступа к информационно-образовательным ресурсам. Наиболее ценные ресурсы, обеспечивающие доход ВУЗа и конкурентные преимущества, необходимо относить к информации с ограниченным доступом.

4. Несанкционированная модификация

информационных ресурсов. Данная классическая угроза может проявляться, например, в попытках внести изменения в систему бухгалтерского учета или просто в виде попыток изменить информацию на Web-сервере ради забавы.

5. Несанкционированная модификация компонентов сети, незаконное подключение новых технических средств. Целью осуществления данной угрозы выступает осуществление несанкционированного доступа к информации, а также неавторизованный доступ к внешним ресурсам. Классическим примером данного действия является подмена IP- и MAC-адресов рабочих станций. Более опасным является изменение конфигураций серверов, коммутаторов и маршрутизаторов.

6. Блокирование доступа пользователей к информационным ресурсам. Данная угроза выражается в невозможности получения пользователем необходимой информации, невозможности обслуживания запросов пользователей за приемлемое время, и проявляется как следствие атак на отказ в обслуживании (DoS-атак), а также в результате сбоев и отказов.

В качестве *источников угроз* безопасности могут выступать как субъекты (личности), так и объективные проявления. Причем источники угроз, которые могут находиться как внутри организации, так и вне ее, можно разделить на три основные группы:

− обусловленные действиями субъекта (антропогенные источники угроз);

− обусловленные техническими средствами (техногенные источники угроз);

− стихийные источники угроз.

Антропогенными источниками угроз выступают субъекты, действия которых могут привести к нарушению безопасности информации, и, как следствие, к причинению ущерба. К внешним антропогенным источниками угроз могут относиться, например, потенциальные преступники и хакеры, криминальные структуры, технический персонал поставщиков телематических служб, представители надзорных организаций, силовых структур и пр. К внутренним можно отнести основной, вспомогательный и технический персонал организации, представителей службы защиты информации. Следует отметить, что данная группа источников наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Необходимо серьезно изучать статистику нарушений, вызывающие их причины, личности нарушителей, суть применяемых нарушителями приемов и средств, используемые при этом недостатки приемов и средств защиты, обстоятельства, при которых было выявлено нарушение, и другие вопросы, которые могут быть использованы при построении неформальной модели потенциальных нарушителей.

Вторая группа содержит источники угроз, определяемые технократической деятельностью, последствия которой вышли из под контроля человека и существуют сами по себе. Данные источники менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. В качестве внешних техногенных источников угроз можно привести, например, средства связи, сети инженерных коммуникаций, внутренних – некачественные технические и программные средства обработки информации.

Третья группа источников угроз объединяет обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех, и под которыми понимаются, прежде всего, природные катаклизмы. Данные источники угроз не поддаются прогнозированию, либо их невозможно предотвратить, поэтому меры защиты от них должны применяться всегда.

Угрозы, как возможные опасности совершения какого-либо действия, направленные против объекта защиты, проявляются не сами по себе, а через *уязвимости*. Для удобства анализа уязвимости принято разделять на классы: объективные; субъективные; случайные.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно- техническими методами защиты.

Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами. К ним относятся ошибки и нарушения.

К случайным уязвимостям относят сбои и отказы, а также различные повреждения. Эти факторы, как правило, мало предсказуемы, и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий.

При построении системы обеспечения информационной и сетевой безопасности необходимо решить комплекс организацион-

ных вопросов: от создания службы информационной безопасности, разработки необходимых нормативных документов, регламентов и правил, до проведения необходимого обучения и инструктажа пользователей. Следует отметить, что без поддержки организационных мер техническими защитными механизмами, невозможно обеспечить эффективную защиту сетевых и информационных ресурсов.

Остановим внимание на основных задачах и принципах построения технических защитных механизмов, применяемых в ИВС ВУЗа.

1. В первую очередь необходимо создать и обеспечить поддержание в актуальном состоянии базы данных, содержащей все аппаратные компоненты ИВС и их конфигурации. Это ключевой компонент системы сетевого управления, без реализации которого невозможно решить задачи управления безопасностью, производительностью и учета.

2. Необходимо создать и поддерживать в актуальном состоянии базу данных, содержащую информационные ресурсы, включая классификацию информационных ресурсов по категориям доступа. Сюда же следует отнести создание резервных и эталонных копий наиболее ценных и критичных ресурсов.

3. Предоставление прав доступа пользователей к ресурсам необходимо осуществлять персонифицированно (по пользователям, а не по компьютерам), ни в коем случае не следует создавать групповые учетные записи. В необходимых случаях необходимо обеспечить многоступенчатую систему аутентификации и авторизации. Для разграничения доступа пользователей к Web-ресурсам наиболее перспективно является использование портальных технологий.

4. Построение системы защиты ИВС необходимо осуществлять эшелонированно, разделяя следующие компоненты:

− защита периметра сети. Решение данной задачи обеспечивается использованием межсетевых экранов, включающих следующие основные механизмы: трансляция адресов для сокрытия структуры и адресации внутренней сети, фильтрация проходящего трафика, управление списками доступа на маршрутизаторах, ревизия содержимого пакетов, противодействие атакам на внутренние ресурсы и т.д.;

− защита серверов (внутренних и внешних). При защите почтовых серверов обязательным требованием является применение специальных антиспамовых фильтров, основанных на использовании «цветных» списков, а также лексических, репутационных и сигнатурных анализаторов. Одним из самых распространенных в мире коммерческих серверных спам-фильтров является Symantec Brightmail Anti-Spam. Существуют и другие коммерческие фильтры (зарубежные – SpySweeper Enerprise, Cloudmark Immunity, NetIQ MailMarshal, MessageLabs Anti-Spam и другие; отечественные разработки – Yandex «Спамооборона», Kaspersky Anti-Spam и др.). Уровень фильтрации спама для этих продуктов колеблется в пределах от 90% до 98%, при уровне ложных срабатываний менее 1%. Самым популярным на протяжении нескольких лет из некоммерческих продуктов остается один из старейших спам-фильтров – SpamAssassin. Наличие многочисленных конфигураций SpamAssassin приводит к широкому разбросу оценок эффективности – от 70 % до 98 %. Эффективность работы этого фильтра напрямую зависит особенностей почтового потока и конкретных настроек, то есть от мастерства администратора почтового сервера. Здесь, в отличие от коммерческих продуктов, автоматически приемлемый результат не гарантируется и требуется нетривиальная доводка продукта на месте. При защите файловых серверов необходимо уделять внимание не только вопросам разграничения доступа пользователей, но и антивирусным программным средствам, проверяющих информацию «на лету» при всех обращениях пользователей к файлам;

− защита рабочих станций конечных пользователей. Очень часто, при достаточном уделении внимания задачам защиты периметра сети и серверов, обеспечение защиты конечных рабочих станций осуществляется слабо. Как следствие, большая часть атак осуществляется именно с компьютеров пользователей. Данную проблему помогает решить использование персональных брэндмауэров и антивирусного ПО. В нашей стране лидирующие позиции в этом секторе занимают Symantec Norton Internet Security, продукты «Лаборатории Касперского» и Dr. Web. Следует заметить, что в Бийском технологическом институте была выявлена следующая проблема при использовании средств защиты рабочих станций: пользователи часто (особенно в компьютерных классах) просто отключают подобные средства защиты, ссылаясь на снижение производительности системы при их использовании. Без соответствующей организационной поддержки данную проблему решить невозмож-

но.

5. Одной из интересных и важных задач обеспечения сетевой и информационной безопасности является осуществление контроля целостности компонентов сети и выявление несанкционированных подключений.

Возможны несколько подходов к решению задачи защиты от подмены IP- и MAC-адресов, несанкционированному перемещению рабочих станций и несанкционированному подключению к сети различных устройств. Один из них основан на жестком, централизованном управлении конфигурацией сети. В рамках этого подхода можно обеспечить, например, привязку каждой рабочей станции к конкретному порту сетевого коммутатора, то есть ведение статических таблиц коммутации. Этот подход имеет ряд недостатков, связанных с большим объемом рутинной работы и недостаточной гибкостью.

Второй подход основан на создании и автоматизированном ведении централизованной базы данных сетевых компонентов в сочетании с постоянным мониторингом сети. В этом случае при любом изменении конфигурации сети, данный факт фиксируется в системном журнале, и администратор принимает решение либо о внесении соответствующих изменений в базе данных (то есть «легализации» изменений конфигурации сети), либо производит блокирование объекта сети. Естественно, доступ к критичным внутренним, а также к внешним информационным ресурсам осуществляется только в соответствии с данными о конфигурации сети, отраженными в базе данных. В Бийском технологическом институте решение данной задачи предполагается с использованием именно этого подхода.

6. Для эффективного функционирования защитных механизмов необходимо решить задачу их гибкого управления. Для поддержания и упрощения действий по настройке средств защиты в системе необходимо предусмотреть следующие возможности:

− выборочное подключение защитных механизмов, что обеспечивает возможность реализации режима постепенного поэтапного усиления степени защищенности;

− наличие так называемого «мягкого» режима функционирования средств защиты, при котором несанкционированные действия пользователей фиксируются в системном журнале, но не пресекаются (этот режим позволяет выявлять некорректности настроек средств защиты без нарушения работоспособности системы);

− наличие возможности по автоматизированному изменению полномочий пользователей с учетом информации, накопленных в системных журналах;

− должны поддерживаться возможности управления механизмами защиты как централизованно (с рабочего места администратора безопасности сети), так и децентрализованно (непосредственно с конкретной рабочей станции). Изменения настроек защитных механизмов, произведенные централизованно, должны автоматически распространяться на все объекты, которых они касаются независимо от их состояния (активны или отключены в данный момент). Аналогично, часть изменений, произведенных децентрализованно, должна быть автоматически отражена в центральной базе данных защиты.

Управление производительностью

Задачи управления производительностью можно разделить на три класса: управление производительностью внешних каналов, внутренних или локальных каналов, а также сетевых сервисов.

При этом особое внимание необходимо уделить механизмам, направленным на совершенствование методов управления трафиком. Трафик (объем загрузки) каждого канала связи телекоммуникационной сети является важным фактическим показателем ее работы. Анализ трафика позволяет оценивать фактическую загрузку сети и необходимую емкость ее каналов, выяснять устойчивость работы сети и оперативность реакции на различные нештатные ситуации, судить о динамике развития сети и планировать сроки ее модернизации.

К базовым параметрам функционирования каналов передачи данных относятся следующие показатели, рассматриваемые как в целом, так и в разрезе по основным информационным сервисам: общее число соединений в течение заданного небольшого интервала времени, общий объем переданной информации, общее число переданных пакетов, а также общее время соединений в этом временном интервале. Из имеющихся базовых показателей легко строятся производные показатели, такие как скорость передачи данных, величина загрузки канала и др.

Одним из важнейших показателей функционирования компьютерных сетей является скорость передачи данных конечным пользователям. Под этой величиной понимается отношение количества переданной информации (в байтах) к суммарному времени пере-

дачи информации по всем соединениям за фиксированный промежуток времени. Таким образом, речь идет об усредненной скорости передачи данных конечным пользователям за выбранный промежуток времени. Причем усреднение ведется не только за промежуток времени, но и по всем пользователям, использовавшим сеть в этот промежуток времени. Учет характеристик данной кривой дает сетевому администратору и конечным пользователям возможность корректировать сетевую активность с учетом текущего состояния сети. Определение усредненной скорости передачи данных приобретает особую значимость, когда необходимо оценить эффективность применяемых к сети методов оптимизации трафика.

При управлении производительностью внешних и магистральных каналов связи более предпочтительным является использование *статистического подхода* к анализу загрузки телекоммуникационных каналов. Он основан на значительно меньшей информации, чем требует теория массового обслуживания, поскольку в качестве объекта исследования берется только величина загрузки самого канала, которая фиксируется через определенные равные интервалы времени.

Для решения этих задач разработана статистическая модель внутрисуточных колебаний скорости передачи данных [3]. Суть модели заключается в том, что данные о скорости передачи, для которой наблюдаются значительные колебания в соседние промежутки времени, усредняется по определенному алгоритму. Полученная в результате усреднения функция более информативна при исследовании результатов воздействия на сеть. Учитывая, что скорость передачи данных зависит от активности пользователей, она является нестационарным временным рядом, имеющим различные характеристики в зависимости от времени суток, дня недели, месяца. В нашем случае не имеет значения динамика ряда, существенными являются такие характеристики как поведение процесса в течение суток и временной тренд.

Как показывает анализ временного ряда скорости передачи данных, данный ряд имеет периодичность, и сходные особенности ряда повторяются каждые 24 часа. Вычисление сезонной компоненты можно производить по однофакторной статистической модели процесса, описывающего почасовое изменение скорости передачи данных в течение суток. В качестве 24 уровней фактора в этой модели необходимо рассматривать различные часы суток. В качестве оценки сезонной компоненты в каждый момент времени в аддитивной модели временного ряда можно рассматривать среднее арифметическое разности между среднечасовым значением скорости передачи данных и соответствующим значением ряда скользящих средних.

Поскольку при управлении производительностью внешних каналов администратор сети, как правило, имеет доступ к каналообразующему оборудованию только на одной стороне канала, то управление может осуществляться только путем регулирования потока информационных запросов от пользователей к внешним сетевым сервисам.

При управлении производительностью локальных каналов возможно также использование статистического подхода к анализу, который с одной стороны может являться источником получения исходных данных для имитационного моделирования, с другой стороны – для оптимизации управления.

Особо следует отметить возможность использования имитационного моделирования, с целью определения наиболее эффективных управляющих воздействий [4].

Учет использования ресурсов

Проблема учета использования ресурсов Интернет и контроля за работой пользователей в сети стоит перед каждой организацией. Её решение зависит от типа организации, масштаба локальной сети и количества пользователей Интернет.

Небольшие организации с несколькими десятками пользователей используют для учета, в большинстве случаев, свободно распространяемое программное обеспечение, реже – собственные разработки. Задача системы построения учета использования ресурсов сводится в основном к обеспечению взаиморасчетов с внешними Интернет-провайдерами и к обеспечению контроля за работой сотрудников организации в Сети.

Наиболее часто применяемым решением для крупных организаций и Интернет-провайдеров является использование коммерческих программных продуктов, имеющих соответствующие сертификаты. Данные системы обладают хорошей масштабируемостью и гибкостью, что позволяет настроить их под нужды организации. Функциональность подобных систем расширена за счет развитых подсистем администрирования пользователей, подсистем финансового учета и прочих.

Однако использование подобных систем

в некоторых организациях затруднено из-за их высокой стоимости, а также некоторых ограничений, обусловленных строго определенной моделью учета (например, отсутствие иерархии групп пользователей). В этом случае приходится либо подстраиваться под соответствующие ограничения, либо заниматься доработкой подобных систем. Многие организации выбирают путь создания собственных систем учета, полностью отвечающих предъявленным к ним требованиям.

Рассмотрим вопросы создания системы учета использования ресурсов для сетей ВУЗов на примере Бийского технологического института (БТИ).

Отметим некоторые особенности БТИ:

1. Институт является крупным корпоративным Интернет-клиентом. Одновременно институт является поставщиком Интернет услуг для образовательных учреждений. Следовательно, необходимо обеспечить решение задач не только по учету и контролю за использованием ресурсов преподавателями, сотрудниками и студентами, но и обеспечить ведение взаиморасчетов с организациями-клиентами.

2. Имеется в наличии сложная иерархия пользователей и групп пользователей (отделы, службы, факультеты, кафедры, группы студентов, аспиранты и пр.). Необходимо предусмотреть возможность индивидуального подхода для каждого пользователя и группы (различные лимиты, тарифы и пр.).

Кроме общепринятых требований системности, комплексности и обеспечения безопасности в процессе проектирования системы учета использования ресурсов и управления доступом пользователей Интернет можно сформулировать следующие функциональные требования:

- система должна обеспечивать возможность управления доступом пользователей к ресурсам Интернет, возможность администрирования учетных записей пользователей (регистрация/удаление пользователей, групп пользователей, изменение лицевых счетов), предоставлять статистическую информацию пользователям;

− необходимо вести учет по пользователям, а не по компьютерам, работающим в сети;

− необходимо учитывать в комплексе несколько сервисов, предоставляемых пользователю;

− сервисы могут быть распределены по нескольким серверам (например, несколько прокси-серверов);

− администрирование необходимо проводить централизованно с использованием единой базы данных для всех пользователей и сервисов.

Можно выделить три категории пользователей, на которые ориентирована работа системы:

1. Пользователи Интернет, с соответствующими функциями системы: идентификация, аутентификация и авторизация; получение подробной статистики за любой период, не превышающий одни сутки; возможность получения истории лицевого счета; возможность изменения пароля; предоставление текущей статистики пользователю, а также руководителю группы о работе всей группы.

2. Операторы системы, с функциями: регистрация новых пользователей, удаление существующих, включая группы; перевод пользователя из одной группы в другую; изменение лицевого счета; предоставление статистики о работе всех пользователей.

3. Администратор системы, с функциями: все функции оператора; возможность смены тарифа пользователя, принятого по умолчанию, на индивидуальный; администрирование и аудит операторов.

Особо следует отметить структуру данных в системе учета ресурсов, разрабатываемой в БТИ. Для обеспечения возможности поддержки иерархии групп, таблица с учетными записями пользователей (лицевыми счетами) организована в виде дерева. При этом в этой таблице наблюдается необходимая избыточность данных, обеспечивающая дополнительную гибкость в управлении доступом пользователей к ресурсам Интернет. Однако за счет применения дополнительных средств контроля целостности здесь удается избежать противоречивости данных. Данный подход отличает рассматриваемую систему от аналогичных и обеспечивает максимальную гибкость в использовании. В целом же, структура данных разработана с учетом правил нормализации, обеспечивающих отсутствие противоречивости и избыточности данных.

Система строится с использование трехуровневой архитектуры клиент-сервер: информация хранится в базе данных СУБД Oracle, бизнес-логика реализуется на сервере приложений на основе компонентов Enterprise JAVA Beans. Доступ пользователей и администраторов к системе осуществляется через Web.

Основные интерфейсы управления системой представлены в виде 10 взаимосвя-

занных компонентов. Данная структура оптимизирована с целью минимизации числа интерфейсов. Другими критериями оптимизации являются производительность и удобство работы операторов и администратора. При этом предлагаемая структура обеспечивает необходимую функциональность системы.

Следует отметить, что использование данной системы не ограничено только рамками института. Оригинальные технологические решения, обеспечивающие огромную гибкость и функциональность системы, позволяют использовать ее практически в любой организации. Причем наибольшие преимущества данная система дает, если необходимо обеспечить индивидуальный подход для каждого пользователя или группе пользователей.

Взаимосвязь компонентов системы сетевого управления

Отметим вопросы, касающиеся взаимосвязи компонентов системы сетевого управления, их взаимодействия, а также преимущества, которые дает системный и комплексный подход к ее реализации:

− Во всех подсистемах необходимо использовать единую базу данных компонентов ИВС, информационных ресурсов и пользователей. Это ключевые компоненты, без создания которых невозможно решить вопросы создания системы управления ИВС.

− Получение статистической информации о поведении трафика в системе управления производительностью позволяет выявить аномалии, что может явиться следствием сетевых атак. Следовательно, эффективность системы обеспечения безопасности может значительно возрасти при использовании подобной информации.

− Снижение производительности может быть следствием чрезмерной загрузки каналов передачи данных за счет резкого увеличения объема использования ресурсов. Здесь очевидно взаимодействие системы учета использования ресурсов и системы управления производительностью.

− Снижение производительности может быть следствием сетевых атак. В данном случае просматривается взаимодействие систем обеспечения безопасности и производительности.

− Пользователи, в результате анализа статистики своей работы, могут выявить факты несанкционированного использования своих учетных записей. Это связь систем учета использования ресурсов и безопасности.

В заключение необходимо отметить, что комплексный системный подход к рассматриваемой проблеме в нашем случае полностью оправдал себя, позволив построить в БТИ основные компоненты системы сетевого управления в кратчайшие сроки и с минимальными затратами.

ЛИТЕРАТУРА

1. Попов Ф.А., Титаренко Ю.И. Опыт создания Бийского фрагмента научно - образовательных компьютерных сетей Алтая // Тез. докл. Всероссийской научно - методич. конф. Телематика 96. – С-Петербург: Республиканский научный центр компьютерных телекоммуникационных сетей ВШ, 1996. – С. 46.

2. Попов Ф.А., Титаренко Ю.И. Информационно - вычислительная сеть Бийского технологического института АлтГТУ // Сборник трудов: Новые информационные технологии в университетском образовании: / Новосибирск: НИИ МИОО НГУ,1997. – С.166 -167.

3. Замятин В.С. Использование статистического подхода при решении задач анализа и управления компьютерными сетями // Известия АГУ: №1. - Барнаул: АГУ, 2003. –С. 54-57.

4. Данилюк Ю.С., Попов Ф.А. Система моделирования локальных вычислительных сетей // Изв. АГУ: Спецсборник, 2002. – С. 63-64.