Такое описание осуществляется на стадии «Рабочая документация» в модуле «Физическое проектирование».

Переход к последующим видам описаний в приведенных выше (выражения (1) – (6)) последовательности корректировки и уточнения прототипа проекта и компонентов разрабатываемой ИС требует разработки комплекса имитационных моделей, обеспечивающих получение требуемых параметров по каждому виду описаний.

4. Выводы

Рассмотренный подход эволюционного прототипирования разработки структуры проекта и ИС дает возможность Разработчику и Заказчику на всех стадиях проектирования, начиная с формирования общих параметров проекта, иметь его целостное представление с последующим уточнением составляющих параметров. Модели описания такого проекта фактически являются спиральными моделями, дающими возможность описывать, уточнять, корректировать параметры проекта и разрабатываемой ИС на каждой стадии разработки до получения применяемого результата. Такая технология позволяет:

- иметь эволюционное представление проекта на всех стадиях;
- изменять параметры проекта в динамике проектирования по стадиям;
- находить рациональные решения по параметрам системы на макро- и микроуровнях;
- обеспечивать эффективное взаимодействие Разработчика и Заказчика в процессе проектирования ИС.

В качестве дальнейшего развития предложенного подхода можно выделить разработку комплекса имитационных моделей, регулярных схем алгоритмов, обеспечивающих реализацию процедур переходов от начального описания проекта к физическому.

Список литературы: 1. *Петров Э.Г., Чайников С.И., Овезгельдыев А.О.* Методология структурного системного анализа и проектирования крупномасштабных ИУС. Концепции и методы. Харьков: Рубикон, 1997. 140 с. 2. *Alan M.D.* Operation prototyping new development approach. Software, September, 1992. P. 71-73. 3. *Левыкин В.М.* Концепция создания распределенных информационных управляющих систем // АСУ и приборы автоматики. 1998. Вып.108. С.32-41.

Поступила в редколлегию 21.06.2008

Левыкин Виктор Макарович, д-р. техн.наук, профессор, зав. кафедрой ИУС ХНУРЭ. Научные интересы: разработка корпоративных ИС, синтез сложных ИС. Увлечения: автотуризм, видеофильмы. Адрес: Украина,61022,Харьков, ул. Чичибабина, д.2,кв.83, тел. 705-40-91.

Левыкин Игорь Викторович, канд.техн.наук, доцент кафедры ИКГ ХНУРЭ. Научные интересы: разработка автоматизированных систем управления полиграфическим предприятием. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-18-91.

УДК 681.326

В.М.ЛЕВЫКИН, Т.В.ГАВРИШ

РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рассматривается задача обеспечения безопасности корпоративных информационных систем. Показывается, что совмещение во времени процессов проектирования КИС и разработки политики её информационной безопасности позволяет формализовать построение моделей безопасности на основе традиционного и ролевого подходов, а также обеспечить интеграцию средств безопасности с элементами КИС.

1. Введение

К числу наиболее перспективных направлений применения информационных технологий следует отнести управление бизнес-процессами. Конкурентоспособность бизнеса в значительной степени определяется его гибкостью, открытостью и адекватной реакцией на все изменения внешней среды, что напрямую зависит от качества и оперативности управления бизнес-процессами. Применение информационных систем (ИС) как одного из основных инструментов управления бизнесом, а также возможность доступа к ресурсам киберпространства, обусловленная интеграцией локальных и корпоративных сетей в глобальную сеть, привели к трансформации традиционных форм бизнеса в электронные.

Отличительной чертой электронного бизнеса является применение принципиально новых способов взаимодействия деловых партнёров, сотрудников и клиентов на основе использования современных IT- технологий и Internet.В результате этого достигается снижение расходов на организацию и поддержание инфраструктуры предприятия , совершенствование системы документооборота, повышение оперативности контактов с сотрудниками и деловыми партнёрами, расширение рынков сбыта товаров и услуг, появление новых возможностей для маркетинга.

Однако наряду с неоспоримыми преимуществами появление электронного бизнеса актуализировало задачу обеспечения информационной безопасности корпоративных информационных систем (КИС). Последнее объясняется тем, что несмотря на интенсивное развитие компьютерных средств и IT-технологий, уязвимость КИС и компьютерных систем заметно не снижается и это ставит под сомнение безопасность среды для проведения бизнес-операции в режиме online [1]. Поэтому задача обеспечения информационной безопасности (ИБ) привлекает внимание как специалистов в области компьютерных систем и сетей , так и многочисленных пользователей, заинтересованных в надёжной и качественной защите информационных ресурсов, а также средств осуществления электронных сетевых транзакций.

2. Анализ временного согласования процессов разработки КИС и создания политики её безопасности

Изложенное выше определяет приоритетность задачи обеспечения защиты информационных ресурсов при разработке и использовании КИС и компьютерных сетей.

Указанная задача традиционно решается путём разработки системы информационной безопасности (СИБ), которая должна функционировать абсолютно прозрачно для приложений КИС и быть полностью совместимой с используемыми в КИС техническими средствами и IT- технологиями [2].Одним из факторов, определяющих степень выполнения указанных требований и эффективность функционирования СИБ в целом , является интеграция разработки системы безопасности в процесс проектирования КИС. Данное условие относится, в первую очередь, к созданию политики безопасности предприятия, представляющей собой совокупность документированных управленческих решений, направленных на защиту информации и ассоциируемых с ней ресурсов.

Построение системы ИБ может быть проведено как для функционирующей , так и для разрабатываемой КИС. В первом случае построение (модификация) СИБ осуществляется после аудита безопасности КИС, оценки рисков нарушения ИБ и является по существу выработкой контрмер по снижению рисков до допустимого уровня. При этом аудит может быть как плановым, так и специальным обследованием, представляющим собой анализ причин компьютерных инцидентов. Однако независимо от того, создается или модифицируется СИБ, речь идет о встраивании средств защиты информации в уже существующую КИС. А это в условиях гетерогенной среды обуславливает необходимость согласования взаимодействия продуктов разных производителей.

При создании системы информационной безопасности большинство разработчиков (например [2-4]) исходит из того, что проект КИС априорно известен, т.е. спроектированная КИС дополняется средствами защиты информации. Следует отметить, что некоторые авторы [5] соглашаются, что проектирование КИС изначально в защищенном исполнении позволит учесть требования безопасности непосредственно в процессе её создания и в результате повысит структурированность, однородность и управляемость системы. Однако более обстоятельные рекомендации по технологии разработки системы ИБ в контексте этапов жизненного цикла КИС отсутствуют.

По мнению авторов данной публикации это связано с тем, что в настоящее время вопросами обеспечения ИБ занимаются специалисты подразделений защиты информации, не являющиеся профессионалами в области проектирования информационных систем. В то же время согласование проектных решений на всех этапах разработки и эксплуатации КИС с требованиями информационной безопасности позволит существенно повысить уровень защищённости информационных ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести ущерб владельцам и/или пользователям информации.

Следует отметить, что только совмещение во времени процедур разработки и интеграции функциональных моделей и моделей данных, являющихся обязательными при проектировании КИС , с формированием модели управления безопасностью позволит согласовать ограничения на

безопасность, выдвинутые заказчиком, со спецификой предметной области (условия ведения бизнеса, характеристика внешней бизнес-среды и пр.). Последнее относится к интеграции средств безопасности с остальными элементами КИС и сети, а также к интеграции различных технологий безопасности в целях комплексной защиты информационных ресурсов предприятия.

Отметим также, что в современных публикациях, помимо отсутствия технологии параллельного проектирования КИС и систем ИБ, мало уделено внимания вопросу защиты коммерческой тайны (конфиденциальной информации) с помощью криптографических методов. Последнее связано с неэффективностью законодательной базы, регламентирующей охрану интеллектуальной собственности в Internet .Реализации элементов этой очень важной проблемы и посвящена данная статья.

3. Моделирование процессов управления безопасностью на этапе установления и спецификации требований

Известно [6], что проектирование КИС осуществляется в соответствии с определенной последовательностью этапов. С точки зрения интеграции действий по проектированию КИС и обеспечению ее информационной безопасности наиболее существенными являются этапы анализа (установление и спецификации требований заказчика), проектирования (моделирование системной архитектуры и ее внутренних механизмов) и реализации. Рассмотрим процессы проектирования системы ИБ и, в первую очередь, разработку политики информационной безопасности на этих этапах.

Цель этапа установления требований состоит в получении от заказчика развёрнутого определения функциональных и нефункциональных требований к проектируемой ИС. Функциональные требования формулируют перечень функций, ожидаемых от системы по отношению к отдельным пользователям или их группам, и направлены на определение бизнес-процессов, которые должны быть реализованы в КИС.

Нефункциональные требования определяют структуру обеспечивающего комплекса и ограничения на его функционирование. Примерами ограничений могут быть пожелание заказчика о предпочтительности применения программных и технических средств определенных производителей, а также требование по обеспечению ИБ.

На этапе установления требований может идти речь только о базовом уровне системы ИБ, который включает минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, несанкционированный доступ (НСД) к ресурсам КИС, сбои оборудования. Для устранения этих угроз должны быть приняты контрмеры вне зависимости от вероятности их реализации и степени уязвимости ресурсов ИС, что означает необязательность анализа характеристик угроз. На практике требования к безопасности могут быть изменены в сторону ужесточения после этапа их спецификации.

Однако для уточнения требований заказчика относительно защиты от НСД даже на базовом уровне безопасности необходимо выявить и проанализировать некоторые дополнительные сведения относительно предметной области. Прежде всего, это касается определённого вида информационных ресурсов, для которых следует предусмотреть статус конфиденциальных. Решение данного вопроса имеет следующие аспекты.

Прежде всего, уровень конфиденциальности информационных ресурсов используется для моделирования процедур управления безопасностью. Кроме того, наличие конфиденциальных данных требует на последующих этапах создания СИБ учитывать величину репутационных рисков. Эти риски могут значительно превышать финансовые потери (стоимость повреждённых или разрушенных технических и программных средств), а также возможные неприятности со стороны официальных структур. Следует также отметить, что размещение в базе данных КИС сведений, представляющих собой коммерческую тайну или являющихся объектами интеллектуальной собственности, означает необходимость тщательной проработки таких функций СИБ как криптографическое закрытие хранимой и передаваемой информации, а также управление доступом к ней авторизованных пользователей.

Согласно [7], объектом защиты является не только информация, размещенная в КИС, но и права на эту информацию как на интеллектуальную собственность её владельца (или уполномоченной им особы). Необходимость защиты может устанавливаться как действующим законодательством, так и непосредственно владельцем информации, причём защита конфиденциальной информации регулируется законом о коммерческой тайне, а права её

владельца – нормами авторского права. Однако действенных механизмов защиты информации, особенно при её распространении в киберпространстве, в настоящее время не существует [8].В связи с этим можно считать, что единственным эффективным способом защиты информационных ресурсов являются криптографические методы.

Помимо идентификации информационных ресурсов, существенных с точки зрения обеспечения безопасности КИС, необходимо установить её периметр. Это позволит обосновать разработку процедур сетевого и Web-доступов. Для решения данной задачи следует выяснить:

- необходимость связи головного офиса предприятия с удаленными филиалами и подразделениями;
- необходимость коммуникации предприятия с партнёрами по бизнесу, клиентами и поставщиками через Internet;
- наличие удаленных и/или мобильных сотрудников;
- наличие Web-сайта предприятия;
- необходимость доступа сотрудников предприятия к Internet-сервисам в рамках выполнения служебных обязанностей;
- отношение предприятия к интеграции внутрених бизнес-процессов в Web;
- оценку числа потенциальных пользователей, нуждающихся в доступе к Web-ресурсам предприятия;
- степень доверия к штатным сотрудникам.

Полученные сведения позволят определить ”точки соприкосновения” внешней открытой и защищаемой корпоративной сетей, наметить число межсетевых, персональных (для индивидуальных пользователей) и распределённых (для корпоративных пользователей) экранов, рекомендовать размещение Web-серверов и организацию управления коммуникациями с бизнес-партнерами и заказчиками, а также предварительно выбрать подходящие технологии и средства авторизации.

Все указанные сведения могут быть получены в процессе консультаций с экспертами предметной области и заказчиком. Полученные статистические данные должны быть тщательно проанализированы для выявления неточностей и противоречий и согласованы в окончательном варианте с заказчиком.

Таким образом, на этапе установления требований к проектируемой КИС в контексте ограничений на ее безопасность уточняются цели, задачи и общая стратегия базового уровня ИБ, а также идентифицируются критичные информационные ресурсы предприятия. Дальнейшие действия по разработке системы ИБ направлены на создание непосредственно политики информационной безопасности. Для этого необходима бизнес-модель предприятия , а также описание полномочий всех должностных лиц и пользователей КИС. Эти сведения могут быть получены на этапе спецификации требований.

В качестве входной информации этапа спецификации выступают неформальные требования заказчика, установленные на предыдущем этапе, а его результатом являются модели спецификации проектных решений. Эти модели дают более формальное определение различных сторон функционирования КИС.

Обычно внимание разработчиков КИС акцентируется на моделировании функциональных требований и требований к данным. Результат моделирования зависит от используемого подхода. В случае структурного подхода к процессу моделирования формируется иерархия DFD- и ERD- диаграмм, которые отображают все бизнес-функции и данные системы независимо от программной и аппаратной платформ, на которых должна разворачиваться КИС [9].Последнее не всегда выполнимо, поскольку некоторые формулировки ограничений и/или требований заказчика относительно применения определенных технологий могут фактически навязывать разработчикам КИС необходимость учета особенностей программного и технического обеспечения.

По мнению авторов, совокупность сформированных функциональных моделей и моделей данных, необходимых для разработки проектных решений на последующих этапах создания КИС (описание системы в терминах составляющих ее модулей и внутренних механизмов каждого из них), следует также использовать для моделирования процедур управления безопасностью.

Данное положение базируется на двух обстоятельствах. Во-первых, этапы проектирования архитектуры и детализированного проектирования КИС выполняются в терминах программных и аппаратных платформ, на которых предстоит реализовать систему. А это означает, что уже на этих этапах проектирования КИС необходимо ориентироваться на ее интеграцию с конкретными

продуктами безопасности. Последнее может быть выполнено только при наличии политики информационной безопасности хотя бы базового уровня. Во-вторых, из анализа функциональных моделей в виде иерархии DFD- диаграмм можно извлечь сведения, необходимые для разработки моделей управления безопасностью и на их основе далее предложить специализированные политики безопасности[2]. Остановимся более подробно на данном вопросе.

Одна из основных задач системы ИБ состоит в контроле и управлении порядком доступа к ресурсам КИС соответствующих категорий пользователей. При этом выполняются следующие функции:

- аутентификация или проверка подлинности пользователя;

-управление, позволяющее получать доступ к защищаемым ресурсам только авторизованным пользователям.

Решение данной задачи требует тонкого баланса между получением доступа к критичным ресурсам только авторизованным пользователям и обеспечением необходимой безопасности этих ресурсов, известных и другим сотрудникам предприятия. Следует иметь в виду, что политика доступа определяется не только уровнем конфиденциальности ресурса, но и служебными обязанностями других сотрудников, имеющих прямое или косвенное отношение к этим ресурсам в процессе своей работы.

Модель управления доступом к данным может быть реализована как традиционным способом, так и с помощью подхода, основанного на ролях. В первом случае используются списки управления доступом ACL,хранящиеся в операционной системе или на Web-сервере. В этих списках права доступа к защищаемым ресурсам по каждой из бизнес-функций связываются с идентификаторами ID всех категорий пользователя.

Основанием для формирования списков управления доступом являются сведения по идентификации информационных ресурсов согласно уровню их конфиденциальности, а также иерархия DFD- диаграмм, в которых определено участие пользователей в каждом из бизнес-процессов с указанием используемой информации и характера выполняемых действий.

На предприятиях (организациях) с большим и постоянно изменяющимся числом пользователей подход, персонализирующий права доступа, становится громоздким и плохо реализуемым. Это объясняется трудностями поддержки в корректном состоянии базы данных с учетными записями всех пользователей. В подобных ситуациях целесообразен переход к ролевой модели доступа. Роль описывает, какие действия может выполнять каждый пользователь и с какими ресурсами. Отличие модели состоит в назначении прав доступа пользователя в зависимости от его должностных обязанностей. Таким образом, роли выступают идентификаторами групп пользователей со сходными служебными полномочиями и задают набор действий, выполняемых этими группами с определенными ресурсами. Например, можно установить роли для сотрудников отдела маркетинга, административного аппарата, бухгалтерии и пр. Если роли связать с поддерживающим их списком контроля доступа login ACL, то получаем модель управления безопасностью, определяющую конкретные разрешения и условия для доступа к ресурсам КИС.

Ролевая модель представляет собой граф, структура которого зависит от однотипности служебных полномочий различных категорий персонала и характера конкретных действий по отношению к конфиденциальным ресурсам КИС. При этом следует иметь в виду, что пользователи могут принадлежать не к одной, а к нескольким группам, а каждая группа может включать несколько ролей.

Для разработки ролевой модели управления правами доступа необходимо выполнить следующие действия:

- сформировать роли доступа пользователей к ресурсам;
- сформировать группы пользователей со сходными обязанностями и распределить их по ролям;
- назначить права доступа отдельным ролям.

Источником сведений для создания ролевой модели доступа является каталог пользователей с указанием выполняемых ими работ и действий, который составляется на этапе установления требований и уточняется в процессе определения бизнес-функций по DFD-диаграммам нижнего уровня. Естественно это касается вопросов доступа пользователей к конфиденциальной информации различных уровней.

Ролевые модели широко используются в управлении доступом по схеме однократного входа с авторизацией (SSO). Это позволяет пользователям корпоративных Web-сайтов после

прохождения одной аутентификации получить доступ ко всем авторизованным ресурсам системы согласно установленным ролям. Ролевая модель управления доступом также поддерживается цифровыми сертификатами, в которых вводится дополнительное поле, указывающее роль их владельца. В этом случае исчезает необходимость хранить на серверах КИС списки всех пользователей, их пароли и права доступа. Выбор и разработка ролевой или традиционной моделей доступа определяется сведениями, полученными на этапе установления требований к КИС (например, наличие удаленных сотрудников, использование Web-служб, объем и динамика контингента пользователей, обеспечение подотчетности и пр.).

Из изложенного следует, что использование результатов моделирования функций (этап спецификации требований) позволит на формальном уровне определить порядок доступа субъектов КИС и представить его в виде множества разрешенных отношений доступа: <ресурс, пользователь, тип доступа >,<ресурс, роль пользователя, тип доступа>.

4. Рекомендации по архитектуре безопасности

По результатам проведенного анализа предметной области и ограничений на безопасность следует обосновать и согласовать с заказчиком выбор подхода к проектированию системы ИБ. Последнее необходимо при разработке архитектуры системы информационной безопасности. В случае использования прикладного подхода механизмы безопасности привязаны к конкретному приложению или Internet-сервису (например, бухгалтерия, кадры, электронная почта), в то время как объектный подход ориентирован на структуру предприятия. Примером объектного подхода может быть построение защищенной инфраструктуры внешних информационных обменов, локальной сети и пр. Смешанный подход предполагает комбинирование объектного и прикладного подходов.

В политике безопасности указываются контрмеры против угроз базового уровня ИБ для рассматриваемой предметной области. В частности, описываются компоненты архитектуры безопасности с рекомендациями по их развертыванию и управлению, а также рассматривается возможность реализации механизмов безопасности в компонентах архитектуры КИС. Примерами могут быть рекомендации следующего содержания:

- как организовать управление Web- и сетевым доступом авторизованным пользователям;
-какую выбрать схему подключения межсетевых экранов и целесообразно ли использование персональных экранов;
- где разместить Web-серверы и как управлять коммуникациями с бизнес-партнерами;
- какие методы шифрования и аутентификации следует использовать для обеспечения надежного хранения информации на файловом уровне;
- целесообразно ли совмещение функции маршрутизации и VPN;
- какие использовать средства антивирусной защиты.

Разработка рекомендаций по архитектуре безопасности должна осуществляться параллельно с этапом проектирования системной архитектуры КИС. Данный этап выполняется в терминах программной и аппаратной платформ, на которых предстоит реализовать КИС. Следует отметить, что многие средства безопасности представляют собой программные или программно-аппаратные комплексы, установленные на защищаемом сервере или ПК. Поэтому проведение архитектурного и детализированного проектирования КИС с учетом компонентов архитектурной безопасности можно считать реализацией интегрированных решений, предъявляемых в настоящее время к любым элементам КИС с учетом ее гетерогенности.

Не исключено, что в процессе проектирования защищенного варианта КИС возникнут повышенные требования к режиму безопасности и базовый уровень ИБ окажется недостаточным.

В этом случае следует идентифицировать потенциальные угрозы и уязвимости, делающие возможной их реализацию. Затем необходимо вычислить риски, связанные с осуществлением этих угроз, и предложить контрмеры, обеспечивающие приемлемый уровень информационной безопасности при минимальных затратах. Технология управления рисками согласно NIST 800-30 достаточно хорошо отработана и описана в [2-4].

5. Выводы

Совмещение во времени процессов проектирования КИС и разработки политики ее информационной безопасности позволило формализовать следующие процедуры:

- создание каталога пользователей с указанием их ролей в выполнении соответствующих бизнес-функций;

- разработку моделей управления безопасностью на основе использования как традиционного подхода, персонализирующего права доступа, так и с помощью ролевого подхода.

Кроме того, предложенные изменения в технологии проектирования КИС с учетом требований по обеспечению ИБ обусловили возможность следующих интегрированных решений в части выбора программно-технических средств:

- интеграция средств защиты с элементами КИС – маршрутизаторами, службами каталогов, операционными системами, серверами и пр.;
- интеграция различных технологий безопасности между собой для обеспечения комплексной защиты ИС, например интеграция межсетевого экрана с VPN-шлюзом.

Реализация указанных решений позволяет повысить уровень информационной безопасности, что весьма существенно в условиях сложной гетерогенной структуры современных КИС.

Список литературы: 1.*Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2002. 546 с. 2.*Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. 616 с. 3.*Петренко С.А., Симонов С.В.* Новые инициативы российских компаний в области защиты информации // Конфидент.2003.№1. С.34 -39. 4.*Симонов С.В.* Анализ рисков в информационных системах. Практические аспекты // Конфидент.2001. №2. С.12-18 .5.*Бабков И.Н., Лавров С.А.* Рекомендации по созданию корпоративной системы информационной безопасности//Атомная стратегия.2004.№12. С.17-21.6.*Мацяшек Л.* Анализ требований к проектированию систем. Разработка ИС с использованием UML.М.: Издательский дом «Вильямс», 2002. 432 с.7.Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»// Відомості Верховної Ради. 2005. №26. С.347.8.*Левыкин В.М., Гавриш Т.В.* Информационная безопасность как фактор защиты интеллектуальной собственности в киберпрстранстве//Новые технологии.2007.Вып.1-2 (15-16).С.95-100. 9.*Петров Э.Г., Чайников С.И., Овезгельдиев А.О.* Методология структурного системного анализа в проектировании крупномасштабных ИУС. Харьков: Рубикон, 1997. 140 с.

Поступила в редколлегию 06.03.2008

Левыкин Виктор Макарович, д-р.техн.наук, профессор, зав. кафедрой ИУС ХНУРЭ. Научные интересы: разработка корпоративных ИС, синтез сложных ИС. Увлечения: автотуризм, видеофильмы. Адрес: Украина,61022,Харьков, ул. Чичибабина, д.2,кв.83, тел. 705-40-91.

Гавриш Татьяна Валентиновна, канд.техн.наук, доцент кафедры ИУС ХНУРЭ. Научные интересы: телекоммуникационные технологии, информационная безопасность КИС. Увлечения: литература, плавание. Адрес: Украина, 61166, Харьков, ул. Мироносицкая, д.99, кв.30, тел. 70-21-451.

УДК 004.78

В.И. САЕНКО

ВИЗУАЛЬНЫЙ КОНТРОЛЬ ФУНКЦИОНАЛЬНОСТИ ИНФРАСТРУКТУРЫ КОМПЬЮТЕРНОЙ СЕТИ

Описывается метод визуального контроля состояния компьютерной сети с учетом ее функциональности. Функциональность понимается в смысле обеспечения сервисных услуг в компьютерной сети. На основании оценок качества и их тренда предлагается формировать пространство состояния, в котором и определяется текущее состояние сети. Правильность полученного решения подтверждается на примере.

1. Качество функционирования компьютерной сети и понятие инфраструктуры

Современные компьютерные сети, особенно корпоративные, предполагают наличие постоянного устойчивого доступа к информационным ресурсам. Доступ осуществляется либо в рамках корпоративной сети, либо в рамках Интернет. Основное назначение сети – обеспечение условий нормальной работы информационных систем. При этом информационные системы предоставляют возможность пользователям одновременной работы с одной и той же информацией, размещенной на одних и тех же аппаратных системах. В этом смысле правомерно говорить о ресурсах и сервисах. Сервисы являются абстрактными