ОАО «Информационные спутниковые системы» имени академика М.Ф. Решетнева (г. Железногорск, Красноярский край). Однако общие положения относительно иерархии классов и связей объектов проектирования, описанные в работе, могут быть использованы при настройке и внедрении практически любой СУД в процессы проектирования и производства изделий различных отраслей промышленности.

Литература

1. Боргест Н.М. Онтология проектирования: теоретические основы. Понятия и принципы: учеб. пособие. Самара: Изд-во СГАУ, 2010. Ч. 1. 88 с.
2. Дейт К.Дж. Введение в системы баз данных = Introduction to Database Systems М.: Вильямс, 2006. 8-е изд. 1328 с.
3. Кузнецов С.Д. Основы баз данных. М.: ИНТУИТ; БИНОМ. Лаборатория знаний, 2007. 2-е изд. 484 с.
4. Liskov B., Program development in Java: Abstraction, specification and object-oriented design, 2001.
5. Фаулер М., Скотт К. UML. Основы; [пер. с англ.]. СПб: Символ-Плюс, 2002. 192 с.

References

1. Borgest N., *Ontologiya proektirovaniya: teoreticheskie osnovy. Ponyatiya i printsipy: ucheb. posobie* [Design ontology: theoretical foundations. Concepts and Principles: study guide], SSAU Publ., 2010.
2. Date C.J., *Introduction to Database Systems*, 8th ed., Addison-Wesley, 2006.
3. Kuznetsov S., *Osnovy baz dannykh* [Foundations of databases], 2nd ed., Moscow, INTUIT, BINOM, Laboratoriya Znaniy, 2007.
4. Liskov B., *Program development in Java: Abstraction, specification and object-oriented design*, Addison-Wesley Professional, 1st ed., 2001.
5. Fowler M., Scott K., *UML Distilled: A Brief Guide to the Standard Object Modeling Language*, 2nd ed., Addison-Wesley, 2000.

УДК 004.7

КОРПОРАТИВНАЯ МУЛЬТИСЕРВИСНАЯ СЕТЬ БАНКА. ПРИМЕР ПОСТРОЕНИЯ

Ю.М. Лисецкий, к.т.н., генеральный директор (Компания «ЭС ЭНД ТИ УКРАИНА», просп. Академика Палладина, 44а, г. Киев, 03680, Украина, Iurii.Lisetskyi@snt.ua)

Статья посвящена построению мультисервисных сетей, которые сегодня являются основой ИТ-инфраструктуры, практически любой организации корпоративного уровня, имеющей территориально распределенную структуру. Дано определение мультисервисной сети, сформулированы требования к современным корпоративным мультисервисным сетям, соответствующей им инфраструктуре и функциональности систем. Описаны основные компоненты мультисервисной сети и их назначение. Приведена топология ее построения. Рассмотрены принципы, требования и подходы к построению корпоративной мультисервисной сети банковского учреждения и интеграция в нее контакт-центра. Приведена последовательность задач, решаемых в ходе их интеграции. Описан пример построения корпоративной мультисервисной сети для ВТБ Банка в Украине: состояние проблемы, постановка задачи, разработка решения и проектирование, этапы внедрения, опыт реализации проекта и его результаты для банка.

Ключевые слова: *мультисервисная сеть, ИТ-инфраструктура, контакт-центр, надежность, доступность, отказоустойчивость, контроль качества, мониторинг, территориально распределенные организации, гетерогенная структура.*

BANKING INSTITUTION CORPORATE MULTISERVICE NETWORK. CONSTRUCTION EXAMPLE

***Lysetsky Yu.M.**, Ph.D., director general*
(«S&T Ukraine», Akademika Palladina Av., 44a, Kiev, 03680, Ukraine, Iurii.Lisetskyi@snt.ua)

Abstract. The article is concerned with the question of multiservice networks` construction, which are now the basic of the IT-infrastructure of almost every corporate tier organisation with geographically dispersed structure. The article defines the term “multiservice network”, represents a set of requirements to modern corporate multiservice networks, to corresponding infrastructure and to systems` functionality. Basic components of the multiservice network, their functions and its construction topology are described. The principles, requirements and approaches to corporate multiservice network construction of banking institution and the way of integration of call centre to it are considered in the article. It also presents the task sequence solved during the process of their integration. The example of corporate multiservice network construction for VTB Bank in Ukraine is described, and namely: the problem state, task setting, solution and project development, implementation phases, project realisation experience and its results for the bank.

Keywords: multiservice network, call center, safety, availability, fail-safety, quality control, monitoring, geographically dispersed organizations, heterogeneous structure.

В условиях жесткой конкуренции в банковской сфере для достижения успеха банку уже недостаточно просто предоставлять клиенту набор стандартных услуг. Для обеспечения стабильного роста бизнеса на первое место выходит уровень качества обслуживания, которое напрямую зависит от оперативности и эффективности работы обслуживающего персонала.

Сегодня существует ряд услуг и сервисов, призванных повысить удобство клиента при работе с банком. Эффективность и доступность операторов центра обработки вызовов, надежность банковских сервисов, скорость обработки запросов и оперативность взаимодействия филиалов банка между собой – факторы, имеющие большое значение для клиентов. Следовательно, банку, беспокоящемуся о комфорте работы и лояльности своих клиентов, стоит уделить данному вопросу особое внимание. А это невозможно без развитых информационных технологий, которые должны обеспечивать устойчивое развитие бизнеса и решать задачу надежного функционирования всех банковских сервисов, необходимых для ведения операционной деятельности.

С этой целью создается ИТ-инфраструктура, основа которой – корпоративная мультисервисная сеть (единая сеть, способная передавать голос, видеоизображения и данные). Основным стимулом появления и развития мультисервисных сетей является стремление уменьшить стоимость владения, поддержать сложные, насыщенные мультимедиа прикладные программы и расширить функциональные возможности сетевого оборудования. Мультисервисные сети позволяют также расширить свои сетевые магистрали, предоставляя новые сервисы и дополнительные услуги широкому кругу корпоративных клиентов [1, 2].

Принимая решение о построении корпоративной мультисервисной среды с последующей интеграцией в нее технологий IP-телефонии и центра обработки вызовов, банки прогнозируют значительный рост региональных филиалов и ставят следующие задачи:

– обеспечить прозрачную интеграцию технологий IP-телефонии, полностью сохранив функциональность действующих решений банка в области традиционной телефонии (УАТС);

– создать защищенные каналы передачи данных и предотвратить возможность несанкционированного доступа в сеть;

– создать условия для дальнейшего развития сети (расширение географии филиалов, интеграция новых сервисов и приложений) без существенных инвестиций.

Преимуществами корпоративной мультисервисной среды являются простота подключения новых филиалов и отделений банка, рациональное использование полосы пропускания наземных каналов связи, сокращение расходов на междугородную и международную связь, невысокие требования к квалификации технического персонала.

Это достигается использованием при разработке продуктов Cisco Systems в рамках архитектуры AVVID (Architecture for Voice, Video and Integrated Data), особенность которой – ее распределенная природа (рис. 1). Такое решение создает интеллектуальную сетевую инфраструктуру и обеспечивает поддержку основных сервисов корпоративной сети: передача данных и голоса, безопасность, сетевое управление и механизмы гарантирования качества сервиса (QoS). Коммуникационными каналами могут быть традиционные наземные линии связи ТфОП и цифровые каналы Frame Relay, арендуемые у оператора связи.

Основные компоненты мультисервисной корпоративной сети:

– IP-телефоны Cisco, подключенные в локальную сеть каждого офиса и обеспечивающие как традиционную функциональность телефонов, так и ряд новых функций;

– сервер Cisco CallManager, позволяющий управлять телефонными соединениями и предоставлять дополнительные сервисы IP-телефонии;

– голосовые шлюзы, предназначенные для подключения к ТфОП и стыковки с существующими УАТС;

– коммутаторы, необходимые для подключения активных сетевых устройств: рабочих станций, IP-телефонов и серверов.

Часто филиалы банка развиваются поэтапно: сначала открывается небольшой офис, который по мере развития бизнеса укрупняется. С развитием филиала банку необходимо иметь ресурс для постепенного наращивания количества телефонов и увеличения пропускной способности сети передачи данных. В таких условиях традиционное телефонное решение обходится значительно дороже, чем телефония на базе IP, даже при условии аренды каналов. IP-телефония, в свою очередь, позволяет легко наращивать количество абонентов и реализовывать прозрачную интеграцию с уже существующими традиционными решениями, полностью сохранив их функциональность.

Основу такой интеллектуальной сетевой инфраструктуры для функционирования IP-телефонии составляют коммутаторы, маршрутизаторы, голосовые шлюзы и другое оборудование. IP-инфраструктура поддерживает основные сервисы

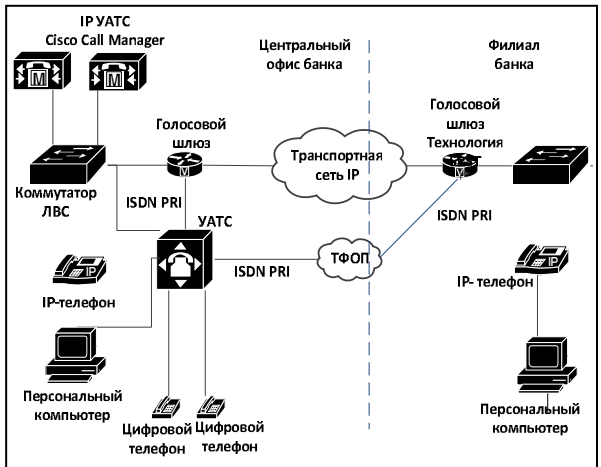

Рис. 1. Мультисервисная сеть банка

корпоративной сети: обеспечение качества сервиса (QoS), безопасности и сетевого управления. Кластер серверов Cisco Call Manager в центральном офисе устанавливает телефонные соединения и управляет IP-телефонами, расположенными в удаленных филиалах банка в пределах корпоративной мультисервисной сети. Если связь между головным офисом и регионами нарушена, региональные филиалы имеют возможность обрабатывать вызовы локально за счет использования средства отказоустойчивой телефонии для удаленных офисов (Survivable Remote Side Telephony).

Центр универсальной обработки вызовов обслуживает все офисы банка с сохранением единого корпоративного стандарта качества, а корпоративная мультисервисная сеть, объединяющая центральный офис банка с региональными филиалами, обеспечивает передачу данных и голоса, безопасность, сетевое управление и механизмы гарантирования качества сервиса.

Решение для построения контакт-центра банка базируется на IPCC (Internet Protocol Contact Center) компании Cisco Systems и интегрируется в мультисервисную сеть (рис. 2). ПО IPCC является одним из структурных компонентов для построения интеллектуальных центров обработки конвергированных вызовов (данные, голос, видео) архитектуры Cisco AVVID.

Контакт-центр позволяет принимать и обрабатывать поток входящих обращений, поступающих как по традиционным телефонным сетям (голос, факс), так и через каналы Интернет (e-mail, web-обращения), используя функцию web-collaboration.

Управление работой контакт-центра осуществляется в режиме реального времени, что позволяет оперативно реагировать на изменения потоков вызовов и обслуживать их оптимальным количеством ресурсов.

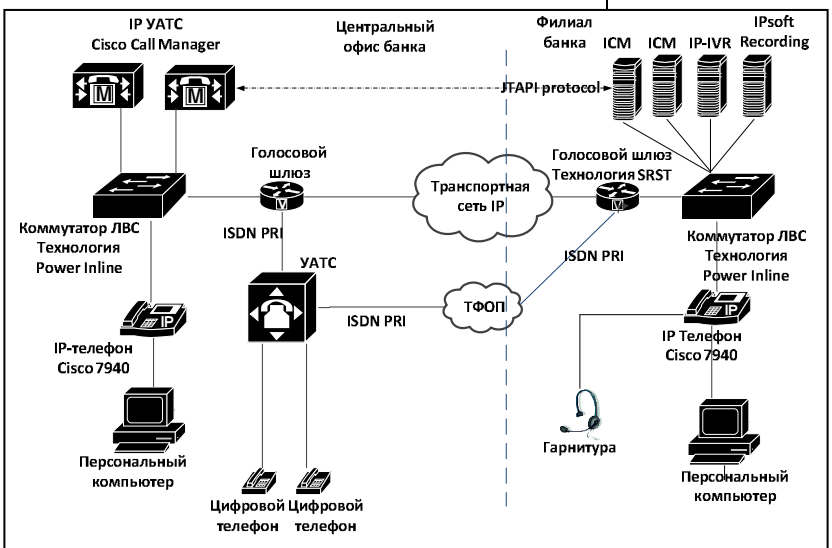

Рис. 2. Схема интеграции контакт-центра в мультисервисную сеть банка

Пример реализации

ОАО ВТБ Банк в Украине – стабильно развивающийся универсальный банк, входящий в группу крупнейших по классификации Национального банка Украины.

По мере развития в банке активно строится ИТ-инфраструктура.

Первостепенной задачей, стоящей перед любой ИТ-инфраструктурой, является обеспечение ее соответствия и соответствия информационных систем предприятия требованиям бизнеса.

Именно поэтому в ВТБ Банке для надежного функционирования всех банковских сервисов, востребованных при ведении операционной деятельности, было принято решение о создании мультисервисной корпоративной сети банка.

Интегратором проекта выступила компания «ЭС ЭНД ТИ УКРАИНА».

В результате реализации проекта была построена корпоративная мультисервисная сеть ВТБ Банка, которая стала фундаментом для внедрения бизнес-приложений, обеспечивающих эффективное взаимодействие с клиентами и дающих возможность расширять спектр предоставляемых банком продуктов и услуг. Построение корпоративной сети сделало возможным внедрение технологических информационных систем, которые позволяют эффективно организовать работу сотрудников банка.

Корпоративная сеть передачи данных ВТБ – это интегрированная среда, позволяющая использовать все многообразие телекоммуникационных услуг (традиционную передачу данных, IP-телефонию, видеоконференц-связь) и предполагающая интеграцию со средствами контроля доступа, охраны и видеонаблюдения.

Посредством построения ВТБ Банком корпоративной сети решена задача доступности для всех сотрудников банка и актуальности информации, обеспечивающей технологические и бизнес-процессы. Построение корпоративной сети позволило начать комплексную централизацию информационных систем, что повысило их управляемость и эффективность использования. Прежде всего централизация бизнес-приложений во много раз повышает скорость распространения новых продуктов и услуг по всей сети банка, предоставляет клиентам равные возможности в пределах всей Украины.

За счет использования защищенных каналов передачи данных значительно повыси-

лась степень информационной безопасности на уровне обмена сотрудниками банка информацией в электронном виде, доступа сотрудников к информационным системам и базам данных, а также на уровне защиты от внешних информационных угроз.

При построении корпоративной сети был сделан акцент на создание отказоустойчивой транспортной сети передачи данных для обеспечения работы филиалов и отделений банка, а также на обеспечение планового открытия новых отделений. Стандарт типового узла сети предполагает наличие основного и резервного каналов связи от разных провайдеров.

В банке развернута система мониторинга корпоративной сети, которая позволяет в режиме реального времени между узлами (отделение–филиал–головной офис) не только осуществлять анализ трафика с точки зрения загрузки канала передачи данных, но и вести статистику по типу трафика (например, АБС, электронная почта, документооборот, Интернет и т.д.). Внедрение такой системы мониторинга также позволяет упростить задачу оптимизации затрат на аренду каналов связи и планирования мероприятий по модернизации транспортной сети передачи данных.

В процессе реализации проекта были успешно решены следующие задачи:

– все головные офисы объединены в единую структуру резервируемыми каналами связи;

– в головном офисе развернута система мониторинга и управления сетевыми устройствами;

– развернута система мониторинга сетевой безопасности;

– развернута IP-телефония с общим количеством абонентов свыше 3 000;

– для обслуживания клиентов развернут центр обработки вызовов на 40 операторов;

– заменено каналообразующее оборудование в 25 областных центрах, а также модернизированы их локальные сети;

– заменено оборудование в существующих отделениях и построены новые, суммарной численностью свыше 180;

– построены защищенные каналы связи как на уровне головной офис–филиал, так и на уровне филиал–отделение;

– построена сеть ATM, каналообразующее оборудование сети подключено к головному офису с использованием технологии DMVPN;

– к сети подключено более 200 банкоматов;

– работоспособность сети подтверждена во время эксплуатации и дополнительного тестирования.

Таким образом, корпоративная мультисервисная сеть ВТБ Банка стала современной сетью, построенной с использованием всех технологических возможностей, которые может предоставить такой производитель телекоммуникационного оборудования, как Cisco. Данная корпоративная сеть – это не только надежные каналы передачи данных: она широко использует такие технологии, как передача средствами корпоративной сети голоса и видео, это и IP-телефония, и видеоконференц-связь, и ряд решений по ИТ-безопасности, а также контакт-центр.

Функционально и надежно построенная корпоративная сеть спроектирована на пятилетнюю перспективу. Корпоративная сеть ВТБ Банка – комплексная система, являющаяся платформой для развития прежде всего бизнес-приложений, обеспечивающих организацию работы с клиентами и повышение уровня предоставляемых сервисов. В то же время отказоустойчивая мультисервисная корпоративная сеть позволяет решать множество других задач.

Построение корпоративной сети для ВТБ Банка – масштабный проект не только для организации банковской сферы, но и для всех территориально распределенных компаний Украины. Уникальность проекта заключается в его масштабности, в специфике дизайна и особенностях архитектуры сети, в широкой функциональности использованного телекоммуникационного оборудования и ПО. В этом состоит несомненное преимущество сети ВТБ Банка и именно поэтому на форуме Cisco Expo она признана лучшей корпоративной сетью года.

В ходе реализации проекта построения корпоративной мультисервисной сети использован и дополнен накопленный опыт по формированию и обоснованию набора требований и соответствующей им функциональной структуры систем, последовательности задач, решаемых в ходе их интеграции, практического применения разработанного математического аппарата, при выборе компонент систем из представленного на рынке набора промышленных программных и аппаратных средств [3–5].

Технологии и подходы к решению задач, примененные в этом проекте, в значительной мере универсализированы, что позволяет применять их при построении подобных корпоративных мультисервисных сетей, имеющих гетерогенную структуру, не только в банковской сфере.

Литература

1. Гриценко В.И., Урсатьев А.А. Распределенные информационные системы. Состояние. Проблемы развития // УСиМ. 2003. № 4. С. 11–21.

2. Лисецкий Ю.М. Опыт построения корпоративной интегрированной информационной системы // Программные продукты и системы. 2007. № 2. С. 26–29.

3. Лисецкий Ю.М. Методы и алгоритмы комплексной количественной оценки качества систем. М.: ЦВСИТ ИМВС РАН, 2002. 20 с.

4. Лисецкий Ю.М. Реализация методики комплексной количественной оценки качества сложных систем в программном комплексе «Вердикт». М.: ЦВСИТ ИМВС РАН, 2005. 26 с.

5. Лисецкий Ю.М. Выбор сложных систем по критерию минимума среднего риска // УСиМ. 2007. № 3. С. 22–26.

References

1. Gritsenko V.I., Ursatyev A.A., *Upravlyayushchie sistemy i mashiny* [Journal of Control Systems and Machines], 2003, no. 4, pp. 11–21.

2. Lisetsky Yu.M., *Programmnye producty i sistemy* [Software & Systems], 2007, no. 2, pp. 26–29.

3. Lisetsky Yu.M., *Metody i algoritmy kompleksnoy kolichestvennoy otsenki kachestva system* [Methods and algorithms of systems complex qualitative assessment], Moscow, TSVSIT IMVS RAS, 2002.

4. Lisetsky Yu.M., *Realizatsiya metodiki kompleksnoy kolichestvennoy otsenki kachestva* [Complex quantitative assessment methods realization in software set], Moscow, TSVSIT IMVS RAS, 2005.

5. Lisetsky Yu.M., *Upravlyayushchie sistemy i mashiny* [Journal of Control Systems and Machines], 2007, no. 3, pp. 22–26.

УДК 004.056

СПОСОБ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ОТ ИССЛЕДОВАНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Работа поддержана грантом Президента Российской Федерации № МК-1039.2013.9)

М.А. Стюгин, к.т.н., старший преподаватель
(Сибирский федеральный университет, просп. Свободный, 79, г. Красноярск, 660041, Россия, styugin@rambler.ru)

В статье обозначена проблема исследования в конфликтных системах. Рассмотрены методы противодействия процессу исследования контрагента, а также противодействия противодействию процесса исследования. Определена модель исследователя в конфликте, включающая информационные ограничения при попытке исследовать объект конфликта. Представлены четыре класса, в которых может находиться исследователь с учетом его информационных ограничений. Приведен алгоритм проектирования защищенных от исследования информационных систем. Проблема исследования контрагента в конфликтной системе заключается в возможности использовать этот процесс с целью дезинформации. Это можно сделать, если знать принципы интерпретации исследователем получаемой информации и получить таким образом возможность рефлексивно управлять противником. Аналогично можно получить схему рефлексивного управления процессом рефлексивного управления. Реально управляющий в данный момент субъект находится в состоянии информационного превосходства. Для достижения состояния информационного превосходства субъект должен получить контроль над объектом конфликта, достаточный для корректировки классов модели исследователя контрагента. Корректируя классы модели исследователя, можно добиться состояния, когда для контрагента станет невозможным сформулировать задачу исследования. Если субъект может получить такой контроль, то, используя алгоритм, предложенный в статье, он достигнет состояния информационного превосходства. Предполагается, что наиболее эффективно данный алгоритм можно применить на стадии разработки программных продуктов в области информационной безопасности. С использованием предложенных алгоритмов уже были разработаны системы анализа несанкционированных действий пользователей на интернет-ресурсах и в локальной сети предприятия (программы ReflexionWeb и ExLook).

Ключевые слова: *защита от исследования, модель конфликта, информационная безопасность, методы проектирования защищенных систем.*

INFORMATION SECURITY SYSTEMS TECHNIQUE SECURED FROM RESEARCHING

***Styugin M.A.**, Ph.D., senior lecturer*
(Siberian Federal University, Svobodny Av., 79, Krasnoyarsk, 660041, Russia, styugin@rambler.ru)

Abstract. Conflict systems form the research area of our study describing the methods of protecting counterparty against research, as well as the methods of counteracting the protection against research. The study determines the researcher model in conflict. This model imposes information restrictions when trying to research the object of the conflict. The study describes four classes of the researcher depending on his information restrictions. The algorithm for designing systems protected against research is also described. The counterparty research problem in a conflict system is that there is an opportunity of using this process to disinform. This is possible, if you know researcher's principles of interpretative work on information received, what gives you the possibility to reflexively control the opponent. Similarly, you can get the scheme to reflexively control the reflexive control process. At the moment the subject that really controls the process has information supremacy. To obtain this information supremacy, the subject has to get conflict's object under control that is sufficient to correct counterparty researcher model classes. By correcting classes of the researcher model, you can achieve the point when it becomes impossible for the counterparty to define the research objective. If the subject can get the process under control of this kind, than using the described algorithm it obtains information supremacy. We assume this algorithm can be effectively applied to information security software development. Using the considered algorithm, the analysis system of unauthorized user activity on enterprise websites and enterprise networks (ReflexionWeb and ExLook software) have already been developed.

Keywords: protection against research, conflict model, information security, methods of designing protected systems.

В системах безопасности существенную роль играет возможность потенциального злоумышленника построить объективный образ атакуемой системы, а противоположной стороне конфликта,