Широков Александр Николаевич. Обеспечение сетевого взаимодействия и информационной безопасности в системе генерации многоуровневых программных комплексов клиент-серверной архитектуры : Дис. ... канд. техн. наук : 05.13.11 Москва, 2005 156 с. РГБ ОД, 61:05-5/2346

Широков Александр Николаевич

Обеспечение сетевого взаимодействия и информационной безопасности в

системе генерации многоуровневых программных комплексов

клиент-серверной архитектуры

05.13.11 - математическое и программное обеспечение вычислительных машин,

комплексов и компьютерных сетей

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель

кандидат физико-математических наук

Вышинский Леонид Леонидович

СОДЕРЖАНИЕ

Введение 5

1 Инструментальная система "Генератор Проектов" 15

1.1 Проектный подход к разработке информационных систем 15

1.2 Архитектура «клиент-сервер» 17

1.3 Структурная модель проектируемых систем 19

1.4 Язык описания проектов 27

1.5 Состав файлов описания проекта 37

1.6 Генерация и сборка программного комплекса 39

1.7 Преимущества проектного подхода в Генераторе Проектов 40

2 Информационная безопасность 41

2.1 Концепция информационной безопасности 42

2.2 Обеспечение конфиденциальности информации 43

2.2.1 Симметричные алгоритмы 44

2.2.2 Асимметричные алгоритмы 46

2.2.3 Электронная цифровая подпись 47

2.3 Контроль целостности данных 48

2.3.1 Хеширование 48

2.4 Аутентификация информации 49

2.5 Идентификация сторон информационного обмена 50

2.5.1 Протокол трехфазной аутентификации 51

2.6 Цифровые сертификаты 56

2.7 Особенности концепции информационной безопасности 59

2.8 Методы обеспечения информационной безопасности 60

2.8.1 Компоненты модели 60

2.8.2 Структура модели 61

2.9 Программная реализация 67

2.9.1 Программные компоненты подсистемы безопасности 69

з

2.9.2 Структура Базы Ключей Сервера Безопасности 73

2.10 Транспортная модель передачи данных 77

2.10.1 Протокол и пакеты аутентификации 79

2.10.2 Взаимодействие с удаленным Сервером Безопасности 81

2.10.3 Протокол и пакеты контроля канала передачи 83

2.10.4 Протокол и пакеты передачи данных 84

2.11 Первоначальное развертывание системы 87

3 Пример описания проекта информационной системы 89

3.1 Архитектура 89

3.2 Описание проекта 91

3.2.1 Общее описание проекта 92

3.2.2 Описание Баз Данных 95

3.2.3 Описание Серверов 96

3.2.4 Описание пользовательского интерфейса 98

3.3 Логика работы Клиентских Модулей 104

3.3.1 Клиентский Модуль Город 104

3.3.2 Клиентский Модуль Район 105

3.3.3 Модуль Администратора Безопасности 107

3.4 Состав файлов информационной системы 109

3.5 Пользовательский интерфейс 110

4 Практическое применение 114

4.1 Система Банковского Самообслуживания MassPay 115

4.1.1 Архитектура Системы 115

4.1.2 Язык Настройки Сценариев (ЯНС) 119

4.1.3 Реализация проекта 122

4.2 Система Мобильного Банковского Обслуживания MobilPay .... 123

4.2.1 Описание системы мобильного банкинга 124

4.2.2 Задачи мобильной коммерции 126

4.2.3 Информационная безопасность 127

4.2.4 Основные функции СМБ 127

4.2.5 Реализация макета СМБ 128

4.3 Система обслуживания микропроцессорных карт DUPLET 130

4.3.1 Технология расчетов в Системе 131

4.3.2 Архитектура Системы 131

4.3.3 Функции компонент системы DUPLET 134

4.3.3.1 Серверы DUET 134

4.3.3.2 Модуль «Оператор расчетов» 134

4.3.3.3 Модуль «Региональный клиент» (РК) 135

4.3.3.4 Модуль «Персональный клиент» (ПК) 137

4.3.3.5 Интернет-магазин 138

4.3.3.6 Прикладной Сервер 139

4.3.3.7 Сервер терминальных карт (СТК) 139

4.3.3.8 Подсистема безопасности 140

4.3.4 Надежность расчетов 141

4.3.5 Информационная безопасность 143

4.3.5.1 Защита Базы Данных Системы DUPLET 143

4.3.5.2 Защита терминальных карт 144

4.3.5.3 Защита Системы DUET 145

4.3.5.4 Защита информационного обмена между центральным

сервером Системы и Интернет-магазином 145

4.3.5.5 Защита информационного обмена между центральным

сервером Системы и банками — участниками Системы 145

Заключение 146

Литература 149

**Заключение**

В настоящей работе изложена концепция, архитектура и реализация подсистемы информационной безопасности, разработанной в рамках промышленной инструментальной системы Генератор Проектов. Необходимость разработки описанной подсистемы информационной

безопасности вызвана современными требованиями к безопасности

прикладных систем и отсутствием инструментальных систем подобного класса, отвечающих этим требованиям. Генератор Проектов основан на современном проектном подходе к разработке информационных систем, главным преимуществом которого является то, что он не перемешивает две области деятельности - содержательное моделирование прикладных задач и технологические проблемы программирования. Благодаря этому появляется возможность достаточно глубокой формализации на этапе постановки задачи, то есть в процессе проектирования системы. С другой стороны средства проек­тирования, то есть правила описания системы, их форма и содержание, одно­значно соответствуют доступной в данный момент технологии создания про­грамм, которая заложена в Генераторе Проектов и той структурной модели, на которую он опирается. Развитие структурной модели, расширение возможно­стей автоматической генерации программ будут совершенствовать и средства проектирования. В связи с этим представляется, что дальнейшее углубление проектного подхода, разработка более мощных языковых средств описания содержательных объектов, моделей и процедур, может быть даже их специализация и ориентация на конкретные предметные области, являются весьма актуальной задачей для разработчиков прикладных информационных систем.

Автор представляемой диссертации является одним из разработчиков инструментальной системы "Генератор Проектов". Ниже перечислены основные результаты, которые получены лично автором:

* Разработана концепция и архитектура подсистемы информационной безопасности, отвечающая современным требованиям прикладных промышленных систем, обладающая очень высоким уровнем гибкости, функциональности и масштабируемости и при этом позволяющая обес­печить высокую степень защищенности конфиденциальной информации от несанкционированного доступа. Гибкость и функциональность выра­жается в возможности выбора различных схем защиты и контроля ин­формационных потоков и ресурсов. А масштабируемость выражается в том, что подсистема информационной безопасности позволяет обеспе­чить высокую эффективность обработки прикладных задач благодаря возможности грамотного распределения нагрузки по различным компо­нентам проектируемых прикладных систем.
* Разработанная подсистема информационной безопасности реализована и интегрирована в инструментальную систему Генератор Проектов. Пред­ставленная реализация, позволяет разрабатывать прикладные промыш­ленные системы под широкий спектр программно-аппаратных платформ, что, несомненно, расширяет возможности практического применения ин­струментальной системы Генератор Проектов.
* Разработана структурная модель подсистемы безопасности в архитектуре «многоуровневый клиент-сервер». Выделены основные логические ком­поненты системы. Некоторые логические компоненты могут быть выде­лены в разные программные модули, что позволяет территориально рас­пределить компоненты системы. В том числе есть возможность выделить наиболее важные компоненты, такие как Сервер Безопасности, хранящий ключевую информацию пользователей, в отдельные сегменты сети, обес­печив, таким образом, дополнительный уровень безопасности.
* В реализации транспортной модели подсистемы безопасности применен пакетный метод передачи данных, позволяющий обеспечить независимые потоки данных в любых направлениях. Применение этого метода позво­лило в некоторых случаях обеспечить возможность инициации передачи данных от сервера к клиенту.
* Разработаны две схемы трехфазной аутентификации сторон информаци­онного обмена в архитектуре клиент-сервер. Аутентификация с примене­нием симметричных и асимметричных алгоритмов шифрования. Схема на симметричных алгоритмах при достаточно высоком уровне крипто­стойкости позволяет обеспечить быстрое и несложное развертывание прикладной системы. В то время как схема на асимметричных алгорит­мах, более сложная в развертывании и сопровождении, позволяет обеспе­чить очень высокий уровень защищенности и конфиденциальности.
* Применена сетевая база данных для хранения аутентификационной ин­формации, включая криптографические ключи пользователей и списки привилегий на выполнение тех или иных операций.
* Разработаны удобные средства администрирования подсистемы безопас­ности. В том числе реализован Модуль Администратора Безопасности, выполненный в виде графического программного приложения, позво­ляющего интуитивно понятном способом управлять системой.
* В промышленной Системе MassPay автор реализовал подсистему инфор­мационной безопасности, несколько десятков Интерфейсных Клиентских Модулей для связи с различными Биллингами по специфическим прото­колам.
* В пилотной Системе MobilPay автор реализовал подсистему информаци­онной безопасности, взаимодействие с Центром приема коротких сооб­щений (SMS) по протоколу SMPP v3.4 через канал TCP/IP.
* В промышленной Системе Duplet автор разработал транспортную архи­тектуру, реализовал подсистему информационной безопасности, Цен­тральный Сервер Системы, Карточные Модули, Модуль Регионального Клиента.