На правах рукописи

Македонский Сергей Александрович

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В СИСТЕМЕ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ И СОЦИОЛОГИЧЕСКОГО ОПРОСА

05.13.01 "Системный анализ, управление и обработка информации" (промышленность)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Волгоград – 2010

Работа выполнена на кафедре ЭВМ и систем Волгоградского государственного технического университета

Научный руководитель	доктор технических наук, профессор Лукьянов Виктор Сергеевич.
Официальные оппоненты:	доктор технических наук, профессор Фоменков Сергей Алексеевич.
	доктор технических наук, профессор Лобейко Владимир Иванович.
Ведущая организация	Волгоградский государственный университет.

Защита состоится 28 декабря 2010 г. в 13:00 час. на заседании диссертационного совета Д 212.028.04 при Волгоградском государственном техническом университете по адресу: 400131, г. Волгоград, пр. Ленина 28, ауд. 209.

С диссертационной работой можно ознакомиться в библиотеке Волгоградского государственного технического университета.

Автореферат разослан "25" ноября 2010 г.

Ученый секретарь
диссертационного совета _____ Водопьянов В.И.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Повсеместное развитие информационных систем создает условия для разработки и внедрения современных информационных средств, позволяющих автоматизировать, и, тем самым, более эффективно реализовывать процессы управления. В то же время, в связи с возрастающей сложностью информационных систем и используемых в них информационных технологий, возрастает объем предъявляемых к ним требований.

Одним из таких процессов, которые необходимо автоматизировать, является проведение тайного голосования, например, на совете акционеров какой-либо крупной компании, при голосовании в больших компаниях, имеющих распределенную структуру, в любой организации, где периодически проводятся голосования, в том числе в учебных заведениях при проведении текущих выборов профессорско-преподавательского состава. Кроме того, большой интерес представляет собой возможность автоматизировать государственные выборы разных уровней. Именно поэтому большинство разработок на данный момент осуществляется в этом направлении.

Создание системы электронного голосования позволит не только автоматизировать процесс выборов, но и существенно сократить расходы на выборы, повысить скорость и уменьшить вероятность ошибок в подсчете голосов. Подобная система должна отвечать ряду требований, среди которых:

1. Обеспечение тайны (анонимности) волеизъявления участника голосования.
2. Обеспечение одноразового учета голоса участника голосования.
3. Предотвращение возможности дублирования голоса какого-то другого участника выборов.
4. Обеспечение строгой однозначной идентификации участников голосования.
5. Обеспечение достоверности переданных сообщений (например, использование электронно-цифровых подписей).
6. Обеспечение корректности подсчета конечного результата.
7. Обеспечение возможности проверки любым из участников, что результат подсчитан правильно.
8. Обеспечение работоспособности протокола в случае, когда некоторые из его участников нечестны.
9. Обеспечение бесперебойной работы программно-технических средств

Если коротко охарактеризовать эти требования, то можно сказать, что к системам электронного голосования предъявляются требования, выполнение которых должно гарантировать соблюдение тайны волеизъявления участников голосования и достоверность результатов голосования.

Для выполнения этих требований не существует общепринятых алгоритмов. Однако имеется ряд работ в данной области и реализованные и опробованные системы электронного голосования.

В первую очередь в диссертации рассматриваются вопросы проведения электронного голосования в организациях. Системы электронного голосования для организаций на данный момент представлены системами, в которых голос подается с помощью нажатия кнопки на пульте голосования или выбора соответствующего пункта голосования на терминале. Такие системы предназначены для проведения интерактивных опросов и представляют собой лишь средство учета поданных голосов. А в связи с тем, что алгоритмы работы таких систем представляют собой коммерческую тайну и производителями не разглашаются, у пользователей не может быть никаких гарантий в анонимности.

Системы интерактивного опроса могут использоваться для проведения социологических опросов. В связи с этим в диссертации также рассматриваются вопросы проведения анонимных социологических опросов с применением технологий, лежащих в основе систем тайного электронного голосования. Выполнение в используемой для проведения анонимного соцопроса системе перечисленных требований позволит обеспечить высокий уровень доверия к системе и результатам соцопросов со стороны опрашиваемых. Кроме того, выполнение требования строгой однозначной идентификации участников предоставляет возможность проводить соцопросы, ориентированные на определенный круг опрашиваемых.

К разработкам, в которых требование анонимности не просто обязательно, а является основополагающим, относятся системы электронного голосования для государственных выборов. В настоящее время в некоторых странах есть опыт внедрения и использования подобных систем. Например, в Эстонии с осени 2005 года муниципальные выборы проводятся через Интернет, в Казахстане система электронного голосования «Сайлау», закупленная в Белоруссии, впервые испытывалась на 10% избирательных участков на выборах депутатов в 2004-м году и с тех пор активно внедряется по всей республике. Внедряемые в России в рамках проекта «ГАС Выборы» двумерные считыватели заполненных бюллетеней КОИБ автоматизируют лишь процедуру подсчета результатов по участку и имеют высокую стоимость (около 70,0 тыс. руб.). В ряде регионов 12-го октября 2008 года по инициативе Тульской областной избирательной комиссии, поддержанной центральной избирательной комиссией (ЦИК) России, в порядке эксперимента было проведено электронное голосование, для которого использовались возможности сети Интернет. Для того чтобы принять участие в электронном голосовании, избирателю необходимо было получить специальный диск электронного опроса и воспользоваться любым компьютером с выходом в интернет. Этой системой воспользовалось 5,4% от общего количества граждан, принявших участие в выборах. Позже этот эксперимент был повторен 1 марта 2009 года в Вологодской, Волгоградской и Томской областях, а также 11 октября 2009 года в городе Кингисепп Ленинградской области. К возможности проголосовать с использованием диска электронного опроса добавились технологии голосования с использованием мобильного телефона и электронной социальной карты. Однако эти технологии не подходят, например, для выборов все-

российского масштаба, в первую очередь потому, что задачей экспериментов являлось, прежде всего, изучение отношения избирателей к новым формам голосования, и поэтому выполнение перечисленных выше требований было далеко не самым важным. Таким образом, в России нет разработанной и готовой для внедрения системы тайного электронного голосования, позволяющей осуществлять подачу голоса и его подсчет в электронном виде.

Поэтому исследования, направленные на создание системы тайного электронного голосования, являются весьма актуальными.

Целью диссертационной работы является создание системы, позволяющей проводить тайное голосование (анонимный соцопрос) в электронном виде и удовлетворяющей всем предъявляемым к таким системам требованиям. Для достижения указанной цели решаются следующие основные задачи:

1. Проведение системного анализа предметной области (существующих алгоритмов и систем проведения электронных выборов, соцопросов).
2. Разработка необходимого математического аппарата для его реализации в системе тайного электронного голосования (анонимного социологического опроса).
3. Определение требуемых структурных элементов разрабатываемой системы.
4. Реализация системы проведения электронных выборов (анонимных социологических опросов) на основе разработанного для нее математического аппарата и выделенных структурных элементов.
5. Разработка структурной модели системы электронного голосования масштаба нашей страны.

Объектом исследования являются процессы, происходящие в системах и протоколах электронного голосования.

Предметом исследования является соответствие существующих систем проведения электронного голосования предъявляемым к ним требованиям и возможность их реализации и использования в различных условиях.

Методы исследования, использовавшиеся в работе: системный анализ, математическое моделирование, методы формального анализа криптографических протоколов, криптоанализ.

Научная новизна:

1. Предложена новая версия протокола голосования с разделением, которая в отличие от существующей версии протокола, позволяющего производить выбор одного варианта из двух, позволяет проводить тайное голосование произвольной формы – осуществлять выбор одного или нескольких вариантов из многих, а также не превышающих заданное количество.
2. Предложено доказательство выполнения предъявляемых к разработанному протоколу требований, основанное на проведении его формального анализа, результаты которого позволяют утверждать, что протокол обеспечивает тайну волеизъявления и достоверность результатов голосования.
3. Предложена новая структурная модель системы электронного голосования, основанной на разработанном математическом аппарате, которую

можно использовать для проведения электронного голосования в нашей стране.

Практическую значимость работы составляют:

1. Разработанный протокол электронного голосования, который можно использовать для создания программ проведения тайного электронного голосования (анонимного соцопроса).
2. Созданный программный комплекс «Система защищенного электронного голосования», позволяющий проводить тайные электронные голосования и анонимные социологические опросы в локальной вычислительной сети.
3. Использование основных результатов работы в ВолгГТУ, ЗАО «ЭнергоАльянс», ООО «Радеж».

На защиту выносятся следующие результаты исследований:

1. Математическая модель протокола электронного голосования
2. Результаты применения разработанного протокола и программного средства для решения практических задач проведения тайного электронного голосования и анонимного социологического опроса.
3. Модель системы электронного голосования, которую возможно использовать в выборах масштаба нашей страны.

Реализация и внедрение результатов. На созданный программный комплекс «Система защищенного электронного голосования» оформлена и подана заявка № 2010616696 на получение свидетельства о регистрации программы в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам (Роспатенте). Реализованный программный комплекс применяется при проведении голосований на собраниях акционеров в ЗАО «ЭнергоАльянс», а так же при проведении социологических опросов студентов ВолгГТУ, персонала ООО «Радеж».

Достоверность полученных результатов подтверждается теоретическим обоснованием разработанного протокола электронного голосования, а также результатами апробации созданного программного обеспечения.

Апробация работы. Основные положения работы докладывались и обсуждались в ходе научных семинаров кафедры «ЭВМ и систем» ВолгГТУ, а так же на региональных, всероссийских и международных конференциях (III Региональная научно-практическая конференция «Проблемы обеспечения информационной безопасности в регионе» Волгоград, 2010; «Инновационные технологии в управлении, образовании, промышленности «АСТИНТЕХ», Астрахань, 2008, 2009, 2010; «Информационные технологии в науке, образовании, телекоммуникации и бизнесе IT + S&E», Ялта – Гурзуф, 2009, 2010, 2010 осень). По теме диссертации опубликовано 10 печатных работ, в том числе 5 в центральных изданиях.

Структура и содержание диссертационной работы. Диссертационная работа состоит из введения, четырех глав, заключения, а также библиографического списка со 107 наименованиями и приложений. Общий объем работы 134 страницы, в том числе 25 рисунков и 3 таблицы.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы диссертации, сформулированы цели и задачи исследования, научная новизна, методы исследования, практическая значимость работы, излагается краткое содержание глав диссертации.

В **первой главе** дается общая характеристика существующих систем электронного голосования, принципов их функционирования и организации работы с ними. Проводится системный анализ некоторых систем и существующих протоколов проведения электронного голосования на соответствие предъявляемым к ним требованиям с целью выявления имеющихся в этом направлении проблем. Рассматриваются вопросы возможности применения технологий тайного электронного голосования для проведения анонимных социологических опросов.

Системы электронного голосования, применяемые в организациях, в большинстве своем представлены системами интерактивного голосования, в которых голос подается с помощью пультов для голосования или с помощью сенсорного терминала. Алгоритмы работы таких систем представляют собой коммерческую тайну и производителями не разглашаются, поэтому у пользователей нет никаких гарантий в соблюдении тайны их волеизъявления.

Системы проведения социологических опросов представляют собой лишь средства учета подаваемых данных опроса. Создателями таких систем необходимость выполнения требований соблюдения анонимности опрашиваемых и достоверности результатов не учитывается.

Среди известных государственных систем голосования для рассмотрения были отобраны системы, использующиеся в Эстонии, Казахстане и России. В Эстонии и Казахстане системы электронного голосования используются при проведении государственных выборов уже не один год, то есть представляют собой законченный и опробованный продукт, кроме того создатели систем утверждают, что их системы отвечают всем предъявляемым к ним требованиям по соблюдению тайны голосования и достоверности результатов. А анализ систем электронного голосования, внедряемых центральной избирательной комиссией России, дает четкое представление о состоянии работ по внедрению технологий электронного голосования в нашей стране.

Результаты исследований систем и протоколов электронного голосования занесены в табл. 1, где плюс означает выполнение требования, а минус – требование либо не выполняется, либо его выполнение под угрозой.

На основе проведенных исследований делается вывод, что ни одна из реализованных и используемых систем электронного голосования либо не отвечает в полной мере предъявляемым к таким системам требованиям (Эстония, Россия), то есть не способна на должном уровне гарантировать, например, соблюдение тайны голосования, либо не достаточно эффективна, с точки зрения уровня автоматизации (Казахстан). Несмотря на то, что система электронного голосования Казахстана отвечает всем, предъявляемым к ней требованием, она представляет собой лишь средство автоматизации подсчета

голосов. Другими словами, от системы электронного голосования можно получить гораздо больше преимуществ в случае еще большей автоматизации процессов проведения выборов, как например в Эстонии.

Из предложенных на сегодняшний день протоколов проведения тайного голосования самым эффективным признается протокол голосования с разделением, так как он, в отличие от остальных протоколов, способен обеспечить выполнение всех предъявляемых к протоколам голосования требований. Однако его возможности ограничены тем, что он не позволяет проводить голосование с произвольными вариантами выбора.

Таблица 1

Результаты исследований систем и протоколов электронного голосования

	Требования	Система электронного голосования			Протокол электронного голосования		
		Эстонии	Казахстана	России	С перемешиванием	С применением слепой подписи	С разделением
1	обеспечение тайны волеизъявления участника голосования;	–	+	–	+	–	+
2	обеспечение одноразового учета голоса участника голосования;	+	+	+	+	+	+
3	предотвращение возможности дублирования голоса какого-то другого участника выборов;	+	+	+	+	–	+
4	обеспечение строгой однозначной идентификации участников голосования;	+	+	+	+	+	+
5	обеспечение достоверности переданных сообщений;	+	+	+	+	+	+
6	обеспечение корректности подсчета конечного результата;	–	+	–	–	+	+
7	обеспечение возможности проверки любым из участников, что результат подсчитан правильно;	–	+	–	+	+	+
8	обеспечение работоспособности протокола в случае, когда некоторые из его участников нечестны;	+	+	+	–	+	+
9	обеспечение бесперебойной работы программно-технических средств	+	+	+	+	+	+

С учетом отмеченных недостатков приведенных протоколов задачами исследования в диссертации становится поиск решения, в котором будут устранены выявленные в ходе исследований проблемы.

Во **второй главе** описана разработка математической модели протокола электронного голосования, в которой должны быть устранены недостатки свойственные уже существующим протоколам. За основу разрабатываемого протокола взята математическая модель протокола голосования с разделением, так как по результатам проведенных исследований именно он в большей степени отвечает требованиям, предъявляемым к протоколам голосования (см. табл. 1).

В исходном протоколе голосования с разделением каждый участник шифрует все сообщения и подписывает их своей электронно-цифровой под-

писью. Так же в протоколе используются схемы Шамира разделения секрета, обязательства и доказательства с нулевым разглашением.

Все вычисления в алгоритме происходят в мультипликативной группе конечного поля кольца вычетов по модулю Q (Q – 160 битовое простое число).

Для работы схемы обязательств, используемой в протоколе, выбрана пара псевдослучайных чисел B и G. Эти числа сформированы на основе хэш-функции, вычисленной из даты выборов и списка кандидатов. В связи с неразрешимостью задачи дискретного логарифмирования в мультипликативной группе конечного поля, никто (включая счетные комиссии) не знает решения уравнения $B = G^x \pmod{Q}$, что гарантирует невозможность раскрыть из обязательства скрытое в нем значение.

В разрабатываемом протоколе голосования предлагается подачу голоса по каждому кандидату осуществлять отдельно. Таким образом, протокол голосования с разделением в исходном виде в разрабатываемом протоколе выполняется для каждого кандидата, по каждому пункту голосования, отдельно. Каждому кандидату в соответствие ставится число из множества {-1;1}, означающее, был ли осуществлен выбор конкретного кандидата в списке (значение "1") или нет (значение "-1"). В итоге при подаче голоса у избирателя получается список из значений для каждого кандидата из множества {-1;1}.

В связи с новым принципом подачи голосов у избирателя появляется новая возможность для фальсификации результатов. А именно, в таком виде протокол позволяет избирателю проголосовать неопределенным образом, то есть не обеспечивает организаторов выборов уверенностью, что избиратель будет действовать в требуемых рамках. Например, избиратель может вместо требуемого одного кандидата поставить положительный голос, то есть 1, нескольким.

Поэтому для предотвращения фальсификации со стороны избирателя вводится дополнительная процедура проверки счетными комиссиями.

Для этого предлагается воспользоваться тем, что все голоса по кандидатам для любого избирателя в сумме будут давать одно и то же число. Так как можно проголосовать только за наперед заданное количество кандидатов, то в списке голосов будет только это наперед заданное число положительных единиц. Соответственно число отрицательных единиц так же будет фиксировано. Таким образом, и сумма у всех избирателей всех значений из списка голосов будет давать одно и то же число, независимо от того, как они проголосовали.

Для того чтобы воспользоваться этим предлагается использовать предусмотренные в протоколе обязательства избирателя. Для каждого голоса избирателю потребуется передавать свое обязательство. Произведение обязательств $D_{j,k}$ для j-го избирателя по всем k голосам будет давать следующее значение:

$$\prod_k D_{j,k} = \prod_k B^{v_{j,k}} G^{a_{j,k}} \pmod{Q} = B^{\sum_k v_{j,k}} G^{\sum_k a_{j,k}} \pmod{Q} = B^{v} G^{a_j} \pmod{Q} \qquad (1)$$

где k – индекс кандидата в списке, $v_{j,k}$ и $a_{j,k}$ – голос и затемняющее число j-го избирателя по k-му пункту голосования, a_j – сумма затемняющих чисел j-го избирателя, v – сумма голосов по всем пунктам голосования.

Значения B и G известны всем сторонам голосования, как и значение суммы всех голосов v. Составляющие суммы голосов v будут разные, так как избиратели голосуют по-разному. Однако результат будет один и тот же, так как количество кандидатов, за которых можно проголосовать едино для всех.

В этом уравнении есть значение, равное сумме затемняющих чисел. Зная это значение, организаторы выборов смогут проверить, что равенство выполняется. Следовательно, необходимо потребовать от избирателя передавать значение суммы затемняющих чисел a_j. В этом случае, так как все остальные значения известны, чтобы проверить соответствие опубликованных обязательств сумме затемняющих чисел при заданном значении суммы голосов v, а, следовательно, убедиться в корректности количества выбранных кандидатов из списка, необходимо проверить, выполняется ли уравнение (2).

$$\frac{\prod_k D_{j,k}}{B^v} (\mathrm{mod} Q) = \frac{\prod_k B^{v_{j,k}} G^{a_{j,k}}}{B^v} (\mathrm{mod} Q) = \frac{B^{\sum_k v_{j,k}} G^{\sum_k a_{j,k}}}{B^v} (\mathrm{mod} Q) = G^{a_j} (\mathrm{mod} Q) \quad (2)$$

Никто из организаторов не сможет вычислить ни один из затемняющих чисел, входящих в сумму, так как это невозможно. Следовательно, публикация избирателем суммы затемняющих чисел не позволит раскрыть никакое из обязательств и узнать, как проголосовал избиратель по конкретному пункту голосования.

Для мультипликативной группы конечного поля, в которой происходят вычисления, сложность задачи дискретного логарифмирования оценивается как $L_M(1/3,c)$, где c – некоторая константа, зависящая от типа поля. Иначе говоря, в связи с неразрешимостью задачи дискретного логарифмирования для поля, в котором происходят вычисления алгоритма голосования, считается невозможным за приемлемое время подобрать такое значение суммы затемняющих чисел a_j, чтобы избиратель мог, изменить сумму голосов, иначе говоря – подобрать соответствующее a_j, чтобы равенство выполнялось при неправильном v. Следовательно, фальсификация результатов избирателем при использовании суммы затемняющих чисел невозможна.

Предлагаемая в работе новая версия протокола голосования с разделением с учетом предлагаемых нововведений представляет собой нижеследующее.

В стандартной нотации протокол имеет вид:

$$\begin{aligned}
&1.\ M \to N : \{D_{j,k}, (A_1, A_2, C, D_1, D_2, R_1, R_2), a_j, u_{i,j,k}, w_{i,j,k}, D_{i,j,k}, SignM\}_{k_C} \\
&2.\ N \to C : \{D_{j,k}, D_{i,j,k}, U_{i,k}, W_{i,k}, SignN\}_{k_C} \\
&3.\ C \to M : \{D_{j,k}, D_{i,j,k}, U_{i,k}, W_{i,k}, SignC\}_{k_M}
\end{aligned} \quad (3)$$

Где N – счетная комиссия, M – избиратель, C – центр управления выборами, i – идентификатор счетной комиссии N, j – идентификатор избирателя M, k – идентификатор голоса в списке кандидатов, k_N k_M k_C – открытые ключи счетной комиссии, избирателя и центра управления выборами соответствен-

но, $D_{j,k}$ – обязательства по голосам, $(A_1, A_2, C, D_1, D_2 R_1, R_2)$ – аргументы с нулевым разглашением, a_j сумма затемняющих чисел, $u_{i,j,k}$ и $w_{i,j,k}$ – части голосов и затемняющих чисел, $D_{i,j,k}$ – обязательства по частям голосов и затемняющих чисел, $U_{i,j}$ – суммы частей голосов, $W_{i,j}$ – суммы затемняющих чисел, *SignM, SignN, SignC* – подписи избирателя, счетной комиссии и центра управления выборами соответственно.

Предполагается, что в голосовании участвуют m лиц с правом голоса и n счетных комиссий. Использование большого числа счетных комиссий обеспечивает анонимность голосующего и предотвращает возможность фальсификации результатов голосования. Избиратели могут осуществить выбор заданного количества кандидатов из k кандидатов.

В первом сообщении от избирателя счетной комиссии 1. $M \to N : \{D_{j,k}, (A_1, A_2, C, D_1, D_2, R_1, R_2), a_j, u_{i,j,k}, w_{i,j,k}, D_{i,j,k}, SignM\}_{k_N}$ избиратель j отправляет обязательства по голосам $D_{j,k}$, аргументы с нулевым разглашением $(A_1, A_2, C, D_1, D_2, R_1, R_2)$, сумму затемняющих чисел a_j, части голосов и затемняющих чисел $u_{i,j,k}$ и $w_{i,j,k}$, а так же обязательства по частям голосов и затемняющих чисел $D_{i,j,k}$. Сообщение так же содержит подпись избирателя *SignM* и зашифровано открытым ключом счетной комиссии k_N.

Для формирования сообщения:

1. Каждый j-ый избиратель отдельно выбирает голос $\upsilon_{j,k} \in \{-1, 1\}$ по каждому k-му пункту голосования и случайные затемняющие числа $a_{j,k} \in Z/QZ$ (Z/QZ – мультипликативная группа конечного поля кольца вычетов по модулю Q) и вычисляет обязательства по голосам, используя схему обязательств:

$$D_{j,k} = D_{a_{j,k}}(\upsilon_{j,k}) = B^{\upsilon_{j,k}} G^{a_{j,k}} (\mathrm{mod} Q) \qquad (4)$$

2. Вместе с $D_{j,k}$ избиратель вычисляет автономные версии протокола доказательства с нулевым разглашением $(A_1, A_2, C, D_1, D_2, R_1, R_2)$ в подтверждение того, что его голоса действительно выбраны из множества {-1, 1}. Для этого избиратель выбирает d, r, t – случайные числа из Z/QZ и производит следующие вычисления

$$A_1 = \begin{cases} G^t (D_a(x) B)^{-d} (\mathrm{mod} Q), & \text{если } \upsilon_{j,k} = 1 \\ G^t (\mathrm{mod} Q), & \text{если } \upsilon_{j,k} = -1 \end{cases}$$
$$A_2 = \begin{cases} G^t (\mathrm{mod} Q), & \text{если } \upsilon_{j,k} = 1 \\ G^r (D_a(x) B^{-1})^{-d} (\mathrm{mod} Q), & \text{если } \upsilon_{j,k} = -1 \end{cases} \qquad (5)$$

Далее избиратель вычисляет C как значение хэш-функции от (A_1, A_2) и для полученного C вычисляет $d' = C - d (\mathrm{mod} Q)$, $r' = t + ad' (\mathrm{mod} Q)$. Используя полученные значения избиратель вычисляет:

$$(D_1, D_2, R_1, R_2) = \begin{cases} (d, d', r, r'), & \text{если } \upsilon_{j,k} = 1 \\ (d', d, r', r), & \text{если } \upsilon_{j,k} = -1 \end{cases} \qquad (6)$$

3. Согласно нововведениям в протоколе для доказательства того, что голоса сформированы корректно, каждый j-ый избиратель публикует сумму затемняющих чисел $a_j = \sum_k a_{j,k}$.

4. Для передачи голосов $v_{j,k}$ и затемняющих чисел $a_{j,k}$ счетным комиссиям каждый избиратель применяет схему Шамира разделения секрета. С этой целью для каждого k-го голоса он выбирает два случайных многочлена по модулю Q степени $T<n$

$$R_{j,k}(X) = \upsilon_{j,k} + r_{1,j,k}X + \cdots + r_{T,j,k}X^T \,(\mathrm{mod}\, Q)$$
$$S_{j,k}(X) = a_{j,k} + s_{1,j,k}X + \cdots + s_{T,j,k}X^T \,(\mathrm{mod}\, Q) \qquad (7)$$

и вычисляет

$$(u_{i,j,k}, w_{i,j,k}) = (R_{j,k}(i), S_{j,k}(i)) \quad при\, 1 \le i \le n. \qquad (8)$$

Для каждой i-ой счетной комиссии в сообщение вставляет свою пару $(u_{i,j,k}, w_{i,j,k})$ – часть голоса и часть затемняющего числа для i-ой счетной комиссии.

5. Для доказательства принадлежности пары $(u_{i,j,k}, w_{i,j,k})$ конкретному голосу избиратель вычисляет для каждой счетной комиссии обязательства по частям голосов:

$$D_{l,j,k} = D_{s_{l,j,k}}(r_{l,j,k}) = B^{r_{l,j,k}} G^{s_{l,j,k}} \,(\mathrm{mod}\, Q) \quad при\, 1 \le l \le T \qquad (9)$$

Избиратель подписывает полученные значения своей электронно-цифровой подписью *SignM*, шифрует сообщение вместе с подписью открытым ключом k_N соответствующей счетной комиссии, и отправляет сообщение.

6. Каждая счетная комиссия, получив сообщение от избирателя, проверяет согласно схеме аргумента с нулевым разглашением, что значения, скрытые в обязательствах, принадлежат множеству $\{-1;1\}$. Это достигается проверкой выполнения следующих равенств:

$$C = D_1 = D_2,$$
$$G^{R_1} = A_1 (D_a(x) B)^{D_1}, \quad G^{R_2} = A_2 (D_a(x) B^{-1})^{D_2} \qquad (10)$$

Счетная комиссия, убедившись в истинности равенств (10) переходит к проверке, успешное выполнение которой означает, что пара $(u_{i,j,k}, w_{i,j,k})$ согласуется с переданным обязательством, то есть эти значения действительно являются частями голоса. Проверка достигается выполнением следующего равенства:

$$D_{j,k} \prod_{l=1}^{T} D_{l,j,k}^{l'} \,(\mathrm{mod}\, Q) = D_{a_{j,k}}(\upsilon_{j,k}) \prod_{l=1}^{T} D_{s_{l,j,k}}(r_{l,j,k})^{l'} \,(\mathrm{mod}\, Q) =$$
$$= B^{\upsilon_{j,k}} G^{a_{j,k}} \prod_{l=1}^{T} (B^{r_{l,j,k}} G^{s_{l,j,k}})^{l'} \,(\mathrm{mod}\, Q) = \qquad (11)$$
$$= B^{(\upsilon_{j,k} + \sum_{l=1}^{T} r_{l,j,k} l')} G^{(a_{j,k} + \sum_{l=1}^{T} s_{l,j,k} l')} \,(\mathrm{mod}\, Q) = B^{w_{i,j,k}} G^{w_{i,j,k}} \,(\mathrm{mod}\, Q)$$

Так же каждая счетная комиссия согласно нововведениям в протоколе проверяет, что все голоса сформированы корректно, и избиратель правильно подал голоса, проголосовав только за наперед заданное количество кандидатов. Для этого избирательной комиссией вычисляется сумма υ единиц количества кандидатов, за которых можно проголосовать, и отрицательных единиц количества остальных кандидатов и проверяется равенство:

$$\frac{\prod_k D_{j,k}}{B^{v}} (\mathrm{mod} Q) = \frac{\prod_k B^{v_{j,k}} G^{a_{j,k}}}{B^{v}} (\mathrm{mod} Q) = \frac{B^{\sum_k v_{j,k}} G^{\sum_k a_{j,k}}}{B^{v}} (\mathrm{mod} Q) = G^{a_j} (\mathrm{mod} Q) \quad (12)$$

Если избиратель подал голоса корректно, то $\sum_k v_{j,k} = v$, и тогда равенство должно выполняться.

Если все проверки пройдены успешно – полученные от избирателя данные принимаются счетной комиссией и должны быть учтены в итоговом результате.

Во втором сообщении 2. $N \to C : \{D_{j,k}, D_{l,j,k}, U_{i,k}, W_{i,k}, SignN\}_{k_C}$ после окончания приема голосов каждая счетная комиссия передает центру управления выборами все полученные обязательства $D_{j,k}$ по голосам и обязательства $D_{l,j,k}$ по частям голосов и затемняющих чисел, суммы частей голосов $U_{i,j}$ и затемняющих чисел $W_{i,j}$. Сообщение так же содержит подпись счетной комиссии *SignN* и зашифровано открытым ключом центра управления выборами k_C.

Для подготовки сообщения счетная комиссия подсчитывает результаты по каждому k-му кандидату, суммируя все полученные части голосов:

$$U_{i,k} = \sum_{j=1}^{m} u_{i,j,k} (\mathrm{mod} Q) \quad (13)$$

Кроме того, она подготавливает сумму частей затемняющих чисел:

$$W_{i,k} = \sum_{j=1}^{m} w_{i,j,k} (\mathrm{mod} Q) \quad (14)$$

Счетная комиссия подписывает подготовленные для отправки данные своей электронно-цифровой подписью *SignN*. Сообщение шифруется вместе с подписью открытым ключом k_C центра управления выборами, и отправляется.

Центр управления выборами, получая данные от счетной комиссии, осуществляет проверку их корректности, то есть проверяет, что переданные суммы частей голосов и затемняющих чисел согласуются с обязательствами избирателей. Это достигается проверкой следующего равенства:

$$\prod_{j=1}^{m} (D_{j,k} \prod_{l=1}^{T} D_{l,j,k}^{l}) (\mathrm{mod} Q) = \prod_{j=1}^{m} B^{u_{i,j,k}} G^{w_{i,j,k}} (\mathrm{mod} Q) = B^{U_{i,k}} G^{W_{i,k}} (\mathrm{mod} Q). \quad (15)$$

Кроме того, полученные от счетных комиссий данные центр управления выборами предоставляет по запросам всем избирателям, что отражено в сообщении 3. $C \to M : \{D_{j,k}, D_{l,j,k}, U_{i,k}, W_{i,k}, SignC\}_{k_M}$.

Получив эти данные, избиратель по равенству (15) тоже может проверить корректность опубликованных результатов, кроме того, найдя свое обязательство в списке, он убедится что его голос учтен в конечном итоге.

Каждая из сторон процесса может определить итог, беря T значений $U_{i,k}$ и восстанавливая по ним окончательный результат с помощью интерполяционного многочлена Лагранжа. Дело в том, что $U_{i,k}$ – значение многочлена, представляющего сумму голосов, в точке i для k-го кандидата. А именно, решается система уравнений следующего вида:

$$U_{i,k} = \sum_{j=1}^{m} u_{i,j,k} = \sum_{j=1}^{m} R_{j,k}(i) = (\sum_{j=1}^{m} \upsilon_{j,k}) + (\sum_{j=1}^{m} r_{1,j,k})i + \Lambda + (\sum_{j=1}^{m} r_{T,j,k})i^T (\mathrm{mod} Q) \qquad (16)$$

В итоге получается сумма всех выбранных избирателями значений из множества {-1;1} для k-го кандидата. А соотнеся эту сумму с общим количеством проголосовавших и количеством кандидатов, за которых можно проголосовать, получается точный результат по количеству поданных голосов. Например, если h – количество подавших голоса избирателей, f – количество кандидатов, которые можно выбрать, то в процентном соотношении такое значение можно получить следующим образом:

$$\frac{h + \sum_{j=1}^{m} \upsilon_{j,k}}{2 * h * f} * 100\% \qquad (17)$$

Для доказательства того, что этот протокол отвечает всем требованиям, предъявляемым к протоколам электронного голосования, проведен формальный анализ протокола с использованием BAN-логики. В ходе анализа были получены результаты $C \mid\equiv U_{j,k}$ $N \mid\equiv U_{j,k}$ $M \mid\equiv U_{j,k}$, $M \mid\equiv [M \mid\sim v_{j,k}]$, $M \mid\equiv [M \mid\sim a_{j,k}]$, где N – счетная комиссия, M – избиратель, С – центр управления выборами. В терминах BAN-логики это означает, что все участники голосования верят итоговым данным по голосам, получаемым в результате работы протокола, и что избиратель M верит, что никто не узнает, что он высказал $v_{j,k}$ и $a_{j,k}$, соответственно.

В **третьей главе** дается общее описание подсистем, которые необходимы для функционирования системы электронного голосования, использующей разработанный протокол в условиях локальных вычислительных сетей. Для этого первоначально определяется совокупность функций, которые система должна выполнять в целом, для того, чтобы удовлетворять требованиям, предъявляемым к системам тайного электронного голосования. Затем в соответствии с выделенными функциями система разбивается на функционально независимые составляющие, в каждой из которых реализуются связанные функции системы. Структура системы имеет общий вид, представленный на рис. 1.

Разработанная структура вместе с протоколом могут использоваться для создания программ проведения тайного электронного голосования. Выбранные технологии реализации будут зависеть от конкретных условий использования системы.

В рамках диссертационной работы протокол голосования реализован в виде программного комплекса «Система защищенного электронного голосования», имеющего разработанную структуру и предназначенного для использования в локальной вычислительной сети на базе компьютеров под управлением операционных систем семейства Microsoft Windows.

Для реализации программы выбрано средство разработки Academic Edition Delphi 2007 for Windows 32 Professional. Каждая подсистема системы электронного голосования представляет собой независимую подпрограмму.

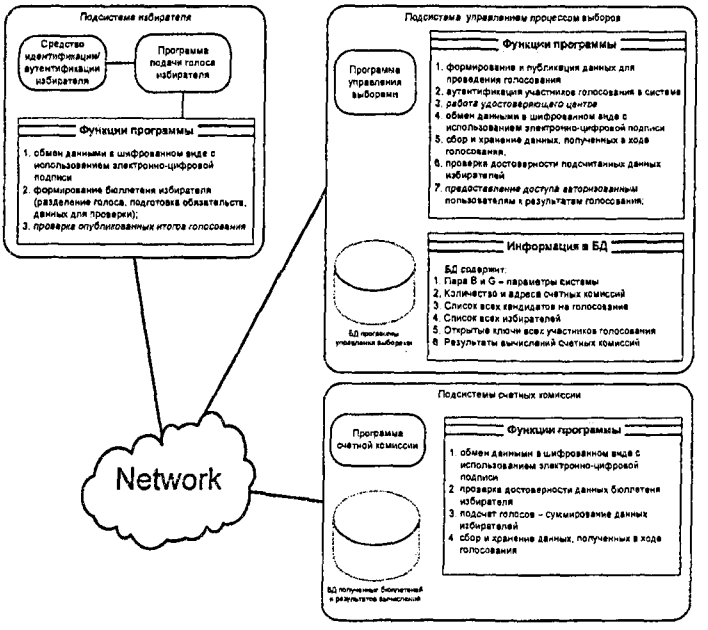

Рис. 1. Обобщенная структура программного комплекса

В голосовании принимают участие один центр управления выборами, несколько счетных комиссий и некоторое количество избирателей. Количество счетных комиссий и избирателей зависит от конкретных условий проведения выборов и может варьироваться в различных пределах. В связи с этим для обмена сообщениями между участниками голосования использовались технологии разработки трехзвенных приложений баз данных, позволяющие реализовывать интенсивный обмен данными между взаимодействующими подпрограммами.

Связь между подпрограммами осуществляется посредством технологии работы распределенных приложений DCOM. Серверные части приложений реализованы с использованием сервера Midas.

Разработанный программный комплекс испытывался на кафедре ЭВМ и Систем ВолгГТУ и используется для проведения голосований на собраниях акционеров в ЗАО «ЭнергоАльянс». Для организации выборов в конференц-зале компании для каждого акционера установлен персональный компьютер. Кроме того, установлен отдельный компьютер для работы подсистемы управления выборами, работа которого видна всем присутствующим через мультимедийный проектор. Все компьютеры объединены в сеть. Для проведения голосования, как правило, заводится от трех до пяти счетных комиссии, одна из которых работает на компьютере действующего председателя собрания, одна на компьютере вместе с подсистемой управления выборами и видна всем, и несколько на компьютерах акционеров. Для того чтобы изби-

ратель смог воспользоваться правом подать голос, ему необходимо авторизоваться в системе, выбрав свою учетную запись из списка и введя пароль. Пароль первоначально раздается в запечатанных конвертах, после чего избиратель может в программе для голосования изменить его на свой, чтобы его никто не знал, даже администратор центра управления выборами, который заводит в систему информацию об избирателях. После окончания процедуры подачи голосов каждая счетная комиссия запускает подсчет голосов и отправку результатов в центр управления выборами. После получения данных от всех счетных комиссий результаты голосования отображаются на мультимедийном проекторе в программе центра управления выборами, а также каждый избиратель может узнать их из программы голосования и убедиться в их корректности.

Кроме проведения тайного голосования созданный программный комплекс испытывался и используется для проведения анонимных социологических опросов в ВолгГТУ. Данные опросов используются на кафедре истории, культуры и социологии ВолгГТУ в ходе проведения практических занятий по курсу социологии и в ходе научных изысканий сотрудников кафедры. Для проведения опроса сотрудником кафедры подготавливается вся необходимая информация для организации такого соцопроса. Администратором центра управления создается новый соцопрос. Для работы системы заводится обычно две счетные комиссии, одна на кафедре истории, культуры и социологии, другая – в аудитории (кафедре), где проводится соцопрос. Для участия в соцопросе студенту необходимо воспользоваться программой для голосования. После проведения опроса информация счетной комиссии в аудитории (кафедре), где проводится соцопрос, уничтожается, в чем может убедиться каждый студент. Это является гарантией, что выбранные им варианты ответов останутся известны только ему.

Аналогичное применение программный комплекс нашел в компании ООО «Радеж» и используется для изучения мнения сотрудников по различным вопросам, касающимся всего персонала в целом, например, по вопросам места проведения корпоративных мероприятий (банкетов, соревнований).

В **четвертой главе** даются предложения по организации структурной модели возможной системы электронного голосования масштаба нашей страны. Условия функционирования такой системы электронного голосования, по сравнению с системой для локальных вычислительных сетей, другие, поэтому и ее структура имеет совершенно иной вид. Для работы системы требуются возможности сети Интернет. А значит и для организации работы ее составных частей необходимо использовать технологии, применяемые при работе в Интернете.

С учетом новых требований, предполагающих работу системы в масштабах целой страны, предлагается следующая обобщенная структура системы государственного электронного голосования (рис. 2):

1. Подсистема центральной избирательной комиссии управления выборами
2. Подсистема удостоверяющих центров

3. Подсистема счетных комиссий
4. Подсистема избирателя

Согласно российскому законодательству проводятся выборы четырех разных уровней:

1. Федеральный
2. Региональный
3. Административный центр
4. Местное самоуправление

За проведение выборов должны отвечать администрации соответствующих уровней. Таким образом, для проведения выборов на всех уровнях, то есть для того, чтобы система электронного голосования была действительно универсальной, необходимо создать центры управления выборами для каждого уровня. Предлагается создать центральную подсистему управления выборами федерального уровня и системы дочерних центров управления выборами региональных уровней. За проведения выборов на региональных уровнях, уровнях административного центра и местного самоуправления будут отвечать региональные центры управления выборами.

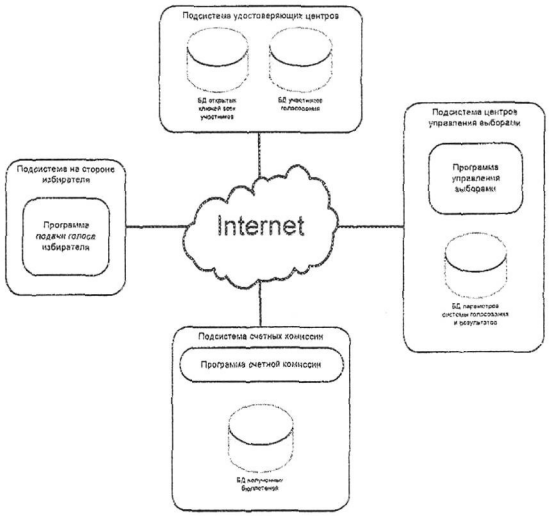

Рис. 2. Обобщенная структура системы электронного голосования

Структура центров управления выборами представляет собой дерево, корень которого – программа федерального центра управления выборами под управлением центральной избирательной комиссии. Федеральный центр управления выборами отвечает за управления выборами федерального уровня. Потомками федерального центра управления выборами являются региональные центры (РЦ) управления выборами. Схематичное изображение структуры федерального и региональных центров управления выборами приведено на рис. 3.

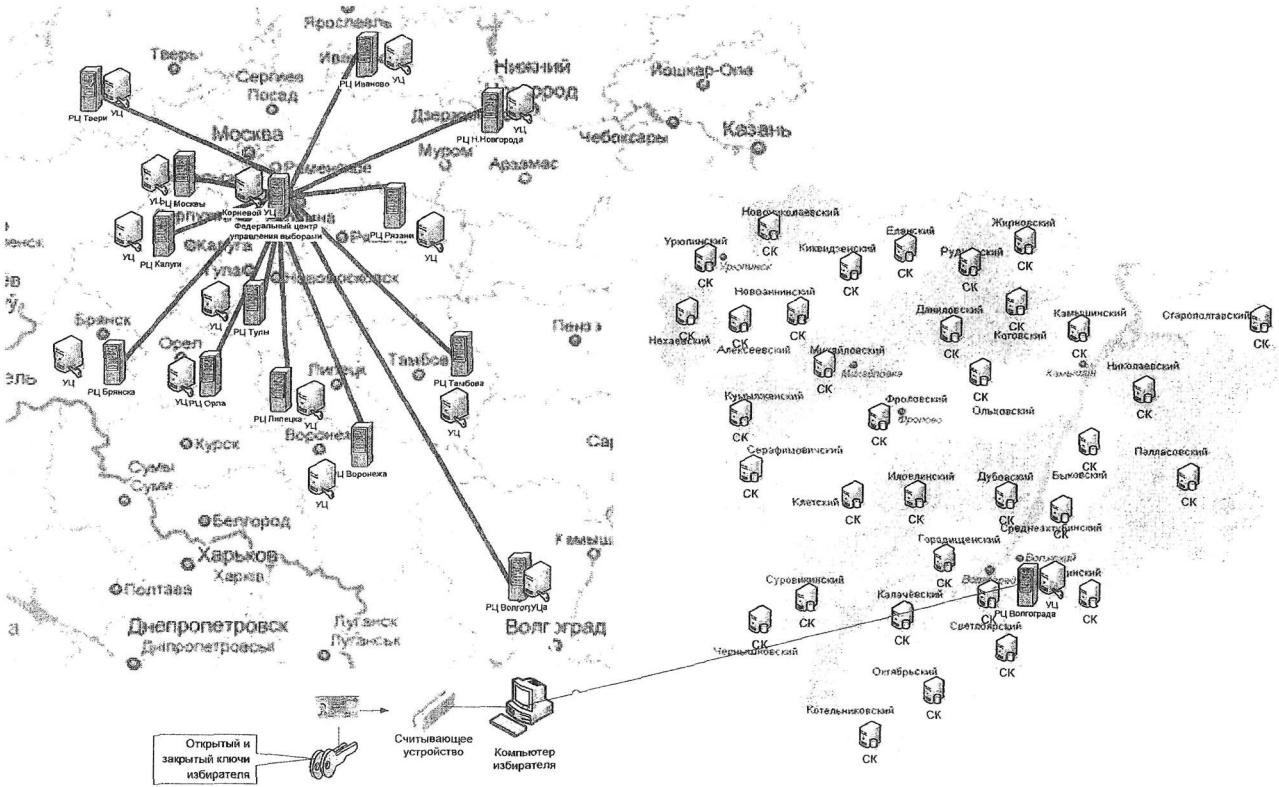

Рис. 3. Обобщенная структура системы электронного голосования масштаба государства

Дочерние программы управления выборами выполняют функции по организации выборов на региональном уровне, уровнях административного центра и местного самоуправления. При проведении выборов федерального масштаба региональные центры управления выборами дублируют данные главного центра управления выборами, для предоставления их избирателям своего региона. Это необходимо чтобы снизить нагрузку на главный центр управления выборами. Клиентское приложение избирателя для участия в выборах будет обращаться к региональному центру управления, отвечающему за организацию выборов по месту прописки избирателя. После окончания выборов региональный центр публикует данные выборов по территории, за которую он отвечает, и предоставляет данные федеральному центру управления выборами для подведения итогов по всей стране.

Подсистема удостоверяющих центров имеет территориально распределенную структуру в виде дерева. Главным является корневой удостоверяющий центр, а дочерние удостоверяющие центры представляют собой системы, территориально принадлежащие субъектам Российской Федерации, которые они обслуживают. Иначе говоря, дочерние удостоверяющие центры так же распределены с учетом региональных особенностей (рис. 3).

Счетные комиссии предлагается образовывать по территориальному принципу. А именно, для каждого района субъекта Российской Федерации предлагается завести по счетной комиссии, за работу которой будет отвечать районная администрация. Таким образом, жители каждого района будут иметь гарантии в сохранении тайны волеизъявления и достоверности публикуемых результатов голосования. Например, для волгоградской области структура подсистем счетных комиссий (СК) будет иметь вид, представленный на рис. 3.

Информацию о выборах счетные комиссии получают у центра управления выборами, полномочного для территории, на которой они функционируют.

Избирателю для участия в выборах необходимо иметь в своем распоряжении контейнер, содержащий его личную ключевую информацию. Это может быть ключевая дискета, таблетка Touch memory, флэш накопитель или что-нибудь другое. Однако наиболее подходящим решением является использование электронного паспорта, аналогично системе голосования Эстонии.

Для работы с электронным паспортом необходимо специальное считывающее устройство. Это считывающее устройство подключается к компьютеру, имеющему выход в интернет. На компьютере функционирует программа, выполняющая функции подсистемы избирателя. Эта программа соединяется с региональным центром управления выборами, который определяется в зависимости от места прописки избирателя.

Региональный центр в случае проведения выборов федерального уровня перед началом голосования запрашивает всю необходимую информацию у федерального центра управления выборами. Информация о счетных комиссиях, которым необходимо будет отправлять части голосов, при любых вы-

борах получается у региональных центров управления выборами. Структурная модель системы голосования вместе с подсистемой избирателя представлена на рис. 3.

По результатам проделанной работы получена структурная модель системы голосования масштаба государства, которая наряду с высоким уровнем автоматизации процесса голосования отвечает всем предъявляемым к системам голосования требованиям. Система имеет иную структуру, по сравнению с системой электронного голосования для локальной вычислительной сети.

Однако в разработанной модели имеются недоработки, связанные с невозможностью решить или исследовать в рамках диссертационной работы некоторые вопросы.

Во-первых, это необходимость перехода к государственному регистру населения, который на данный момент находится на стадии разработки, внедрения. Переход к государственному регистру населения сделает возможным использование электронных паспортов, которые необходимы для проведения электронного голосования с применением системы, имеющей разработанную структуру.

Во-вторых, необходимо исследовать возможное количество счетных комиссий, которые можно будет использовать в выборах. Количество счетных комиссий будет зависеть как от количества районов в области, так и от требуемых вычислительных ресурсов как на стороне избирателя, так и на стороне счетных комиссий. Так как эти данные возможно получить только в случае тестирования конкретной реализации системы, или же модели, построенной на данных, полученных опытным путем, то вопрос количества счетных комиссий остается не решенным.

В-третьих, в связи с большим количеством счетных комиссий особенно остро встает вопрос их безотказного функционирования. А именно, отдельной проработки требует вопрос их резервирования, что возможно только после получения опытных данных по функционированию системы в условиях сети Интернет.

В **заключении** обобщаются основные теоретические и практические результаты, полученные в диссертационной работе, выделяются возможные направления дальнейших исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В работе получены следующие теоретические и практические результаты:

1. Создан новый математический аппарат протокола тайного электронного голосования, отличающийся тем, что он отвечает всем предъявляемым к нему требованиям по соблюдению тайны голосования и достоверности результатов, позволяет производить выборы произвольной формы, а так же обеспечивает высокий уровень автоматизации процесса проведения голосования.

2. Выполнение требований, предъявляемых к созданному протоколу голосования, обосновано его формальным анализом, проведенным с использованием BAN-логики.

3. Создан программный комплекс «Система защищенного электронного голосования», предназначенный для использования в локальных вычислительных сетях, в котором реализован разработанный математический аппарат. На созданный программный комплекс оформлена и подана заявка № 2010616696 на свидетельство о регистрации в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам (Роспатенте).

4. Предложено использование созданного программного комплекса для проведения анонимных социологических опросов, что позволило обеспечить высокий уровень доверия к системе и результатам соцопросов со стороны опрашиваемых, а также предоставить возможность организаторам проводить соцопросы, ориентированные на определенный круг опрашиваемых.

5. Созданный программный комплекс применяется при проведении голосований на собраниях акционеров в ЗАО «ЭнергоАльянс».

6. Созданный программный комплекс используется для проведения анонимных социологических опросов на факультете экономики и управления ВолгГТУ и в компании ООО «Радеж».

7. Разработана структурная модель системы электронного голосования, которая наряду с высоким уровнем автоматизации отвечает всем, предъявляемым к системам электронного голосования требованиям и могла бы использоваться в государственных выборах в нашей стране.

Основные результаты диссертации изложены в следующих работах.

Статьи в изданиях, рекомендуемых ВАК РФ

1. Македонский, С.А. Система электронного голосования / С.А. Македонский, В.С. Лукьянов // Открытое образование : [по матер. XXXVI междунар. конф. и дискус. науч. клуба IT+SE`09, майская сессия, Ялта-Гурзуф]. - 2009. - Приложение к журн. - С. 126-128.

2. Македонский, С.А. Система электронного голосования / С.А. Македонский, В.С. Лукьянов // Открытое образование : [по матер. XXXVII междунар. конф. и дискус. науч. клуба IT+SE`10, майская сессия, Ялта-Гурзуф]. - 2010. - Приложение к журн. - С. 121-123.

3. Македонский, С.А. Формальный анализ протокола электронного голосования / С.А. Македонский, В.С. Лукьянов // Открытое образование : [по матер. XXXVII междунар. конф. и дискус. науч. клуба IT+SE`10, осеняя сессия, Ялта-Гурзуф]. - 2010. - Приложение к журн. - С. 39-48.

4. Македонский, С.А. Анализ систем проведения электронного голосования / С.А. Македонский, В.С. Лукьянов // Изв. ВолгГТУ. Серия "Актуальные проблемы управления, вычислительной техники и информатики в технических системах": межвуз. сб. науч. ст. / ВолгГТУ. - Волгоград, - Вып.9, (в печати).

5. Македонский, С.А. Универсальный протокол защищенного электронного голосования / С.А. Македонский, В.С. Лукьянов // Изв. ВолгГТУ. Серия "Актуальные проблемы управления, вычислительной техники и информатики в технических системах": межвуз. сб. науч. ст. / ВолгГТУ. - Волгоград - Вып.9, (в печати).

Статьи в российских журналах

6. Македонский, С.А. Применение протокола слепой подписи для проведения тайного голосования / С.А. Македонский, В.С. Лукьянов // Прикаспийский журнал: управление и высокие технологии. – 2009. - №4. - С. 7-11.

Статьи в сборниках международных и российских конференций

7. Македонский, С.А. Система электронного голосования / С.А. Македонский, В.С. Лукьянов // Инновационные технологии в управлении, образовании, промышленности "АСТИНТЕХ-2008": матер. всерос. науч. конф., 15-18 апреля 2008 г. / Астрахан. гос. ун-т и др. - Астрахань, 2008. - С. 186-188.

8. Македонский, С.А. Система электронного голосования / С.А. Македонский, В.С. Лукьянов // Инновационные технологии в управлении, образовании, промышленности "АСТИНТЕХ-2009": матер. всерос. науч. конф., 11-14 мая 2009 г. / Астрахан. гос. ун-т и др. - Астрахань, 2009. - С. 136-138.

9. Македонский, С.А. Система электронного голосования / С.А. Македонский, В.С. Лукьянов // Инновационные технологии в управлении, образовании, промышленности "АСТИНТЕХ-2010": матер. всерос. науч. конф., 11-14 мая 2010 г. / Астрахан. гос. ун-т и др. - Астрахань, 2010. – Том 1. - С. 159-161.

10. Македонский, С.А. Система электронного голосования / С.А. Македонский, В.С. Лукьянов // Проблемы обеспечения информационной безопасности в регионе : материалы III Регион. науч.-практ. конф., г.Волгоград, 20 апр. 2010 г. / Волгогр. гос. ун-т. - Волгоград, 2010. - С. 42-47.

Подписано в печать 24.11.2010 г. Заказ № 755 . Тираж 100 экз. Печ. л. 1,0
Формат 60 х 84 1/16. Бумага офсетная. Печать офсетная.

Типография ИУНЛ
Волгоградского государственного технического университета.
400131, г. Волгоград, просп. им. В.И. Ленина, 28, корп. №7