УДК 004.75

О.Ю. Пескова, И.Ю. Половко, С.В. Фатеева

ОБЗОР ПОДХОДОВ К ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ*

Проведен анализ существующих систем электронного голосования, а также методов обеспечения надежности и защищенности как самого процесса голосования, так и оценки его результатов, выделены наиболее интересные и перспективные из них. Представлены различные типы систем электронного голосования, их преимущества и основные проблемы, связанные с подобными системами. Основное внимание уделено дистанционным системам электронного голосования, позволяющим осуществлять голосование с использованием каналов передачи данных, таких, как каналы сети Интернет. Приведены примеры применения систем дистанционного электронного голосования в разных странах. Наиболее интересной и развитой представляется система электронного голосования Эстонии, подробно представленная в статье. Рассмотрены вопросы правового регулирования дистанционного электронного голосования, в частности описана Рекомендация Rec(2004)11 Комитета министров Совета Европы государствам-членам по правовым, организационным и техническим стандартам электронного голосования. Представлен ряд методов организации дистанционного голосования, и в том числе метод, построенный на подходах к bitcoin, авторы которого теоретически показали (а также уже продемонстрировали на практике реальных выборов), что богатые и общедоступные возможности биткоина можно использовать, среди прочего, в качестве своеобразной формы «углеродной датировки» для фиксации времени появления практически любой цифровой информации.

Электронное голосование; криптография; международное право; биткоины.

O.Yu. Peskova, I.Yu. Polovko, S.V. Fateeva

REVIEW OF APPROACHES TO THE ORGANIZATION OF ELECTRONIC VOTING

The main purpose of this article – to analyze existing electronic voting systems, and methods for ensuring the reliability and security of both the voting process and the evaluation of its results highlight the most interesting and promising ones. The article describes the various types of electronic voting systems, their advantages and problems associated with these systems The main attention is given to remote electronic voting systems allowing voting with the use of data channels, such as the Internet. Provides examples of using the remote electronic voting systems in different countries. The most interesting and developed is the Estonian e-voting system, presented in detail in the article. The problems of legal regulation of remote e-voting, in particular described recommendation Rec (2004) 11 of the Committee of Ministers to Member States on legal, organizational and technical standards for e-voting. Presents a number of methods of distance voting, including the method, built on the approaches to the bitcoin, whose authors could theoretically have shown (and have already demonstrated in practice, real elections), that the rich and widely accessible to bitcoin can be used, among other things, as a form of "carbon dating" for time-stamping of virtually any digital information.

Electronic voting systems; cryptography; international law; bitcoin.

В наше время все больше внимания уделяется процедурам голосования по самым разным вопросам, и прежде всего – связанным с решением общегосударственных проблем, с выборами законодательной и исполнительной власти. Поэтому активно развиваются системы электронного голосования разных типов. Термин «электронное голосование» (э-голосование; анг. electronic voting, e-voting) обозначает использование электронных средств голосования [1]. Впервые этот термин

* Работа поддержана грантом РФФИ 13-07-00244-а.

был введен в 1960-х гг. в США, где для голосования применялись специальные перфокарты, позволяющие компьютерной системе при помощи оптического сканирования считывать информацию о волеизъявлении избирателя [2]. В отличие от Америки, электронное голосование в Европе начали применять значительно позже – в начале 80-х гг. XX века.

В целом, можно выделить два основных вектора развития подобных систем – во-первых, системы технического обеспечения процедуры голосования (например, позволяющие произвести автоматический подсчет голосов по бумажным бюллетеням), и во-вторых, системы дистанционного голосования. Термин «стационарное э-голосование» (анг. polling place e-voting) используется для обозначения систем, при которых избиратель отдает свой голос в пределах избирательного участка под контролем членов избирательной комиссии; термин «дистанционное (удаленное) э-голосование» (анг. remote e-voting) используется в ситуации, когда избиратель голосует за пределами избирательного участка из любого месторасположения [1].

Дополнительные проблемы в случае удаленного голосования связаны, по нашему мнению, в первую очередь со следующими вопросами:

1. Идентификация и аутентификация участников голосования – строгая и однозначная.
2. Сложность контроля самостоятельности и доброй воли гражданина, отсутствия принуждения и манипуляций.
3. Обеспечение достоверности сообщений с результатом волеизъявления.
4. Необходимость гарантии корректного учета каждого голоса, причем только единократно.
5. Необходимость гарантии тайны волеизъявления гражданина на любой стадии обработки данных
6. Обеспечение возможности проверки процессов получения и подсчета голосов, а также пересчета голосов при необходимости дополнительного контроля
7. Традиционные уязвимости каналов связи, по которым информация о результатах голосования персоны будет передана в центр обработки данных.

В разных странах уже давно используются различные системы электронного голосования.

Наиболее яркий пример – Эстония, создавшая первую в мире систему электронного голосования [1, 3, 4]. Обсуждение возможностей удаленного голосования в Эстонии началось в 2001 г., а в 2002 г., была утверждена нормативная база для э-голосования. Тестирование инфраструктуры для интернет-голосования на местных выборах правительство Эстонии начало в 2005 г. Два года спустя она была использована на национальных выборах, а на выборах в Европейский парламент в 2009 г. через интернет были поданы 15 % эстонских голосов. В 2011 г. на выборах в национальный парламент страны это число выросло почти до 25 %.

Для проведения электронного голосования существует юридическая основа, заключающаяся в следующих законодательных актах:

- Акт о выборах в местные органы государственной власти, § 50;
- Акт о выборах в Riigikogu, § 44;
- Акт о выборах в Европейский парламент, § 43;
- Акт о Референдуме, § 37.

Была создана инфраструктура открытых ключей, основанная на использовании цифровых подписей и идентификационных карт, которыми обеспечен весь электорат страны (и которые используются при осуществлении финансовых операций, покупке билетов на общественный транспорт, поступлении в вузы и так далее).

Согласно эстонскому выборному законодательству, электронное голосование проводится в период с шестого по четвертый день до дня выборов, при этом предъявляются следующие требования [3]:

1. В дни предварительных выборов избиратели могут проголосовать, воспользовавшись электронной системой на Интернет – странице Национального Избирательного Комитета. Избиратель должен голосовать лично.

2. Избиратель должен подтвердить свою личность при помощи кода PIN1 идентификационной карты.

3. После успешной аутентификации избирателя ему будет представлен общий список кандидатов, баллотирующихся в избирательном округе, к которому относится избиратель по месту своего жительства.

4. Избиратель должен отметить на Интернет-странице кандидата, за которого он хочет проголосовать, и подтвердить свой выбор электронной подписью, используя код PIN2 идентификационной карты избирателя. На Интернет – странице отобразится сообщение о том, что голос принят.

5. Избиратель может переголосовать в период предварительного голосования с шестого по четвертый день до дня выборов:

- с помощью электронного голосования;
- проголосовав на избирательном участке.

Избиратель может проголосовать заново, и предыдущий голос будет удален. Эта возможность является прежде всего мерой против давления и манипулирования – избиратель, на которого было оказано незаконное влияние, может заново проголосовать, когда давление будет снято. При этом существует приоритет традиционного голосования: в случае, если избиратель придет на избирательный участок в день предварительного голосования и проголосует, то его/ее электронный голос будет аннулирован.

Основным средством обеспечения секретности голосования в электронной системе является ассиметричная криптография. Секретный компонент криптографической пары используется программой по подсчету голосов для расшифровки голоса. По завершении периода подачи жалоб секретный ключ уничтожается. В 2011 г. система шифрования была модернизирована до длины в 2048 бит.

Конфиденциальность и секретность электронного избирателя может быть подвергнута опасности при одновременном возникновении двух сбоев в системе безопасности: в случае, если в системе (или вне ее) появляется сторона, имеющая доступ как к секретному ключу системы, так и к голосам, заверенным цифровой подписью.

Секретный ключ может подвергнуться следующим двум опасностям:

- Компрометация ключа или открытие к нему общего доступа. Подобный инцидент предоставляет в распоряжение сторон электронные голоса, заверенные цифровыми подписями, что позволяет определить, кто за кого проголосовал, нарушая таким образом конфиденциальность избирателя.
- Повреждение. Секретный ключ может быть разрушен, утрачен или поврежден в результате технической ошибки. В подобных случаях расшифровка электронных голосов становится невозможной и теряются все электронные голоса. Это – очень серьезная опасность, и поэтому в системе необходимо одновременно использовать две криптографические пары.

Криптографическая пара создается в Аппаратном модуле системы безопасности (АМСБ) таким образом, что секретный ключ никогда не покидает модуль. Создание криптографической пары и использование секретного ключа поддерживается администраторами службы управления ключами, которых должно быть несколько. Рекомендуется схема «N из M», так как четверо из семи членов Национального Избирательно-

го Комитета должны присутствовать для проведения ключевых для обеспечения безопасности операций. Администраторы службы управления ключами имеют как материальные (например, карту-ключ), так и основанные на информации (ПИН-код) методы идентификации для установления сообщения с АМСБ.

Чтобы избежать обвинения в фальсификации выборов, Эстония раскрыла код электронной системы голосования. Тарви Мартенс (Tarvi Martens), архитектор эстонских цифровых документов и приложений для интернет-голосования, говорит, что опубликована лишь серверная часть исходного кода: «Мы не публикуем код ПО, находящегося на стороне клиента, чтобы создание поддельных клиентов не стало слишком простым».

В Австрии первый эксперимент с удаленным дистанционным голосованием проведен в мае 2003 г. параллельно с традиционным голосованием на выборах в Студенческий Совет в Венском университете экономики и бизнеса [1]. Система была построена на использовании системы идентификации граждан через электронные id-карты (Bürgerkarte). Избиратель должен был получить токен для э-голосования, который хранится на электронной id-карте. Подобные эксперименты (но по-прежнему юридически незначимые) были проведены еще несколько раз в различных университетах страны.

В 2003 году в канадской провинции Онтарио 12 муниципалитетов первыми в Северной Америке провели выборы в местные самоуправления и отделы среднего образования используя только электронные средства голосования (Интернет или телефон) [1]. Каждый из 100 000 зарегистрированных избирателей получил индивидуальный идентификационный номер и пароль, позволяющие ему проголосовать через Интернет либо телефон с тональным набором. Внедрение системы э-голосования позволило увеличить явку избирателей до 55 % в сравнении с обычным показателем 25–30 % на местных выборах. После этих выборов в Онтарио был создан Секретариат по делам обновления демократии (анг. Secretariat for Democratic Renewal), одной из задач которого стала выработка предложений по реформе избирательного процесса в Онтарио с использованием сети Интернет.

Во Франции согласно положениям Избирательного кодекса (ст. L 57-1), введенного законом от № 69-419 от 10 мая 1969 г., поправленного статьей 72 закона № 2005-102 от 11 февраля 2005 г. о равенстве прав и шансов, участии и гражданстве лиц с ограниченными возможностями, машины для голосования могут быть использованы в бюро по выборам в коммунах с численностью населения более 3500 жителей [1, 5]. Французский закон не допускает дистанционного электронного голосования для граждан, не проживающих за границей. Во Франции первый эксперимент по дистанционному голосованию был проведен в 2003 г.: была дана возможность участия граждан Франции, проживающих в США, в выборах своих представителей в Ассамблею граждан Франции, живущих за границей. Но в 2003 г. частная инициатива «Форум по правам Интернета» (фр. Forum des droits sur l'Internet) при поддержке правительства Франции опубликовала ряд рекомендаций, касающихся будущего электронного голосования во Франции. В этом отчете было сказано, что во Франции удаленное э-голосование использовать не следует, за исключением выборов делегатов AFE французскими экспатриантами, которые должны иметь возможность проголосовать через Интернет. В то же время рекомендация приветствует использование стационарного электронного голосования (например, через киоски для э-голосования на избирательных участках). Электронное голосование во Франции организуется на добровольной основе коммунами, список которых устанавливается в каждом департаменте префектом. Оборудование может быть куплено или взято в аренду коммунами, в этом случае они получают от государства субсидию в размере 400 евро за одну машину.

В Нидерландах избирательный закон с 1965 г. позволил коммунам организовать голосование иным образом, чем традиционные способы. Общепринятым электронное голосование стало в 90-е гг. XX века. На сегодняшний день более 90 % поданных голосов выражаются с помощью машин для голосования, в 448 из 458 коммун установлено электронное голосование. Более того, согласно экспериментальному закону 2003 г. о дистанционном голосовании, избиратели, проживающие и работающие за границей, имели возможность голосовать посредством Интернет [5].

Германия начала экспериментировать с электронным голосованием в 1999г – но в выборах неполитического характера (университеты, молодежные сообщества и т.п.) [1].

В Испании пилотные проекты по электронному голосованию проводились с 1995 года, а первый юридически незначимый тест с удаленным электронным голосованием был проведен в 2003 году в ходе парламентских выборов в Каталонии [1].

Швейцария выпустила ряд нормативных документов, а также экспертных отчетов о возможностях, рисках и выполнимости э-голосования, в начале 2000-х годов, и в первой половине десятилетия были проведены юридически значимые эксперименты в различных кантонах [1, 6, 7]. Кантон Женева в Швейцарии впервые в мире использовал удаленное голосование через сеть Интернет по полной схеме в 2003 году. Разработчики программы придумали способ исключения основного недостатка системы электронного голосования – отсутствия защищенной анонимности голоса, для чего всем гражданам страны присваивался уникальный номер, который знают только они сами.

Великобритания одной из первых, в 1997 г., начала активно заниматься проблемами электронного голосования, была создана специальная правительственная рабочая группа, были проведены пробные тесты на местных выборах в нескольких графствах [1, 2, 6, 8]. В мае 2003 г. избирательная комиссия Великобритании (the UK Electoral Commission) после проведения ряда пилотных проектов электронного голосования на местах с применением Интернета, сервиса коротких сообщений мобильных телефонов, цифрового телевидения в связи с выявлением ряда проблем рекомендовала правительству развивать и совершенствовать технические стандарты проведения электронного голосования для обеспечения возможности его успешного применения в будущем. Но по результатам пилотных проектов в 2004 г. избирательная комиссия сделала заключение, что избирательные технологии не следует включать в текущую программу модернизации избирательного процесса по причине неготовности на местах к данному процессу. В Великобритании и Ирландии было даже несколько судебных процессов за нарушение прав во время электронного голосования. Тем не менее, за десятилетие было проведено больше 150 пилотных проектов, хотя в первую очередь они были направлены на организацию стационарного электронного голосования.

В Финляндии проводился эксперимент по электронному голосованию на муниципальных выборах 2008 г., однако он провалился [9]. Тем не менее, в 2013 г. было принято о разработке новой системы электронного голосования, одной из задач которой декларируется повышение интереса молодежи к выборам.

В России тоже был проведен ряд экспериментов по дистанционному голосованию [7, 8, 10]. В октябре 2008 г. был проведен первый эксперимент: голосование через интернет протестировали во время выборов в местные органы власти в городе Новомосковске Тульской области. Они проходили с помощью специальных компакт-дисков, которые были распространены среди избирателей. В проводимом параллельно с обычными "бумажными" выборами голосовании участвовали 61,8 % избирателей из числа тех, кто пришел на "экспериментальные участки". При этом

явка избирателей на участки, где проводилось тестирование, была больше, чем на все остальные в среднем примерно на 10 %. С 2009 г. разрабатываются проекты по электронному голосованию с использованием мобильных телефонов. Тем не менее, в российской практике в рамках законодательства о выборах – законе №67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» определены порядок применения голосования, а также термин «электронное голосование»: «Электронное голосование – голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием средств автоматизации ГАС «Выборы». Но при этом все системы дистанционного голосования называются системами дистанционного электронного опроса. Понятие «опрос» не является четко формализованным и может более широко применяться.

Развитие систем электронного голосования привело к необходимости выработки нормативно-правовой базы этого процесса, в том числе и на международном уровне.

В сентябре 2000 г. Европейская Комиссия запустила проект под названием КиберГолос (анг. CyberVote), цель которого заключалась в том, чтобы «продемонстрировать возможность проведения в полной мере проверяемых выборов, гарантирующих абсолютную тайность голосов, при использовании стационарных и мобильных Интернет-терминалов» [1]. К участию в проекте были привлечены партнеры из бизнес-сектора (EADS Matra Systèmes & Information из Франции, Nokia Research Centre из Финляндии, British Telecommunications из Соединенного Королевства), учреждения образования (K.U.Leuven Research & Development из Бельгии, Технический университет Эйндховена в Нидерландах) и потенциальные пользователи (Вольный ганзейский город Бремен в Германии, г. Исси-ле-Мулино во Франции, район Стокгольма Чиста в Швеции).

Первой международной межправительственной организацией, которая серьезно занялась проблемой отсутствия международно-правового регулирования процедур электронного голосования, стал Совет Европы (СЕ), впервые в истории международного права установивший региональные международно-правовые стандарты электронного голосования [2].

В 2003 г. начала функционировать созданная под эгидой СЕ Многопрофильная специальная экспертная рабочая группа по правовым, организационным и техническим стандартам электронного голосования (Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enable voting) [2]. Рабочее название группы IP1-S-EE, она была учреждена и функционировала в рамках комплексного проекта СЕ «Демократические институты в действии» (Making Democratic Institutions Work). В группу вошли государства – члены СЕ, интересы которых были представлены специалистами избирательных комиссий или министерств внутренних дел (в ряде государств за проведение выборов отвечают именно они), а также руководители Технического комитета по услугам в области организации выборов и проведения голосования (Election and Voter Services Technical Committee) Организации по разработке и систематизации информационных стандартов (далее – OASIS). В компетенцию этой группы входила разработка единых межгосударственных стандартов процедур электронного голосования, а также разработка проекта стандартов электронного голосования для его дальнейшего утверждения Комитетом министров СЕ. 30 сентября 2004 г. проект Рекомендации был утвержден Комитетом министров СЕ и получил официальное название Рекомендация Rec(2004)11 Комитета министров СЕ государствам-членам по правовым, организационным и техническим стандартам электронного голосования. Этот документ стал первым в области международно-правового регулирования стандартов электронного голосования. Рекомендация состоит из преамбулы и трех приложений:

- Приложение I – правовые стандарты (legal standards),
- Приложение II – организационные стандарты (operational standards),
- Приложение III – технические требования (technical requirements).

Преамбула определяет 9 основных целей применения электронного голосования:

1) предоставление возможности избирателям голосовать дистанционно вне места нахождения избирательного участка;

2) упрощение процесса голосования;

3) содействие участию в голосовании гражданам, проживающим или находящимся за границей;

4) расширение доступа к процессу голосования избирателей с ограниченными возможностями, для которых представляется затруднительной личная явка на избирательный участок и использование установленного там оборудования для голосования;

5) увеличение явки избирателей посредством внедрения дополнительных способов / каналов голосования;

6) модернизация процесса голосования в соответствии с развитием общества и ростом использования новых технологий;

7) сокращение суммарных затрат на проведение выборов и референдумов;

8) повышение надежности результатов выборов и ускорение процесса подсчета голосов избирателей;

9) обеспечение повышенного качества обслуживания электората посредством предоставления дополнительных способов / каналов голосования.

Рекомендация определяет, что электронное голосование должно быть таким же надежным, безопасным, как демократические выборы и референдумы, проводимые без привлечения каких-либо электронных средств или устройств. В преамбуле Рекомендации государствам-членам предлагается пересмотреть внутреннее законодательство, относящееся к вопросу электронного голосования, в соответствии с разработанными в ней стандартами. В документе определена вся необходимая терминология.

Приложение I – правовые стандарты – включило в себя условия, гарантирующие при проведении электронного голосования соблюдение фундаментальных принципов избирательного права, таких как всеобщее избирательное право, равное избирательное право, свобода волеизъявления избирателя, тайное голосование. В числе прочего сформулировано требование, что интерфейс электронной системы голосования должен быть понятным избирателю, легким в использовании и доступным лицам с ограниченными возможностями. Кроме того, определены следующие условия выполнения требований к системам электронного голосования:

- относительно равного избирательного права – условие о том, что каждый электронный бюллетень избирателя должен быть посчитан только один раз, система электронного голосования не должна допускать мошенничества и попыток подать голос более одного раза;
- относительно свободы волеизъявления – условие о необходимости исключать любое сторонне влияние на принятие избирателем решения в процессе осуществления голосования, о возможности со стороны избирателя изменить свой выбор на любой стадии процесса электронного голосования до того момента, как голос был отдан;
- относительно тайны голосования – условие, гарантирующее, что в ходе применения электронной системы голосования невозможно будет установить связь между идентификационными данными избирателя и тем волеизъявлением, которое он выразил в процессе электронного голосования.

Правовые стандарты Рекомендации закрепляют также процедурные гарантии применения электронного голосования, следование которым решает проблему недоверия избирателей к данной процедуре, основные из которых – следующие:

1) право избирателей апробировать внедренный способ электронного голосования до того момента, как он будет использован;

2) введение мониторинга системы электронного голосования со стороны независимого органа, уполномоченного на то властями, отвечающего за корректность и надежность работы системы голосования;

3) предотвращение любых несанкционированных попыток вторжения в электронную систему голосования;

4) защита конфиденциальности внесенных в систему электронного голосования данных относительно голосов избирателей, а также сведений, идентифицирующих личность голосующих.

Приложение II к Рекомендации – организационные стандарты – включает в себя критерии, позволяющие сделать вывод о том, насколько корректно была организована процедура электронного голосования. Задача этих стандартов – устранить основные ошибки, возникающие на этапе организации процесса электронного голосования, следствием чего является ущемление прав избирателей и нарушение принципов проведения демократических выборов. Для этих целей Приложение II рекомендует государствам – членам СЕ соблюдение следующих основных условий:

1) электронный голос не может быть отдан избирателем до официального уведомления о проведении выборов или референдума;

2) избиратель должен иметь возможность проверить информацию, которая содержится о нем в электронном реестре избирателей, и потребовать ее изменения в случаях недостоверности;

3) электронная система голосования должна быть свободна от любой информации, которая может повлиять на выбор избирателя;

4) рассекречивание содержания голосов избирателей до момента закрытия процесса голосования запрещено;

5) система электронного голосования должна обеспечивать возможность ее аудита;

6) представитель уполномоченного органа власти, отвечающего за организацию выборов, а также независимые наблюдатели должны присутствовать при подсчете голосов, отданных при помощи электронных средств.

Приложение III к Рекомендации – технические требования – содержит информацию о передовых технологических решениях, разработанных исследователями в области информационных технологий и рекомендуемых СЕ для применения в процессе электронного голосования. Например, закрепляется использования специального языка программирования систем электронного голосования – Election Markup Language. Именно данный стандарт – спецификация языка программирования – рекомендуется для применения в электронных системах голосования в государствах – членах СЕ как наиболее надежный и защищенный.

Кроме того, в Приложении III документа даны рекомендации относительно технических критериев проведения электронного голосования:

1) электронная система голосования должна защищать информацию аутентификации пользователей для того, чтобы несанкционированные источники не могли вторгаться, перехватывать, модифицировать или иным образом получать доступ к защищенной информации;

2) должна быть обеспечена целостность и проведена проверка подлинности происхождения информации, передаваемой с одного этапа электронного голосования на другой;

3) должен существовать процесс сертификации, позволяющий проверять и сертифицировать любой компонент информационной и коммуникационной технологии электронного голосования в соответствии с техническими требованиями, описанными в настоящей Рекомендации.

После принятия Рекомендации было принято решение о проведении каждые 2 года специальных совещаний по пересмотру и развитию политики применения систем электронного голосования.

Существует ряд методов, предназначенных для повышения надежности и защищенности электронного голосования, разрабатываются новые подходы, в том числе использующие нестандартные технологии.

Принципиальное улучшение существовавших прежде методов тайного голосования обеспечивает криптография с открытым ключом, которая позволяет организовать такую систему голосования, в которой корешок бюллетеня, оставляемый у избирателя, является полностью анонимным (с его помощью третьему лицу нельзя установить или доказать, за кого именно был отдан голос) и в то же время избиратели могут гарантированно убедиться, что их бюллетень правильно учтен при подсчетах в финальных итогах голосования. Подобного рода криптографические системы для выборов часто называют E2E или «end-to-end verifiable» (т.е. насквозь проверяемое) голосование [11]. Существует ряд подобных систем, созданных авторитетными в области криптографии специалистами, например, Punchscan (Дыркоскан), изобретенной Дэвидом Чомом, автором концепции «цифровых наличных» и целого ряда криптографических протоколов, или системы 3Ballot (Трехчастевой бюллетень) криптографа Рональда Райвеста, известного, в частности, такими алгоритмами как RSA, RC4, RC5, MD5. Система Scantegrity из этого ряда особо интересна тем, что в своем нынешнем виде (Scantegrity II) она является итогом совместного творчества уже упомянутых Чома и Райвеста, а также целого коллектива аспирантов и студентов из четырех университетов США и Канады (включая создателей CommitCoin Кларка и Эссекса).

Ну кроме того, Scantegrity – пока что единственная E2E-система, которую реально и уже дважды успешно применяли на выборах государственной власти (муниципальные выборы в органы управления округа Takoma Park, штат Мэриленд, США).

Очень любопытным представляется предложение использовать структуры биткоинов (BitCoin) для организации дистанционного голосования [11]. На международной криптографической конференции Financial Cryptography 2012 двое канадских ученых, Джереми Кларк и Александр Эссекс, представили свою исследовательскую работу «CommitCoin – ‘углеродная датировка’ обязательств с помощью системы Bitcoin» (CommitCoin: Carbon Dating Commitments with Bitcoin, by Jeremy Clark and Aleksander Essex), в которой авторы теоретически показали (а также уже продемонстрировали на практике реальных выборов), что богатые и общедоступные возможности биткоина можно использовать, среди прочего, в качестве своеобразной формы «углеродной датировки» для фиксации времени появления практически любой цифровой информации. В контексте электронных выборов эта технология может стать полезным инструментом для гарантированной защиты от жульничества и подделки итогов голосования.

Монеты-биткоины конкретного человека зарегистрированы по адресам, которые представляют собой буквенно-цифровые последовательности, выступающие в качестве идентификаторов данного пользователя в пиринговой сети. Когда имеет место транзакция – пересылка биткоинов с одного адреса на другой – то она ши-

роковещательно сообщается в сеть, чем создается публичная запись транзакции. Поскольку пользователь генерирует свои адреса сам, Кларк и Эссекс установили, что к нужному виду биткоин-адреса можно сконвертировать и заранее подготовленные сообщения. Например, для случая выборов, таким сообщением является особый список, который перед началом голосования в виде таблицы увязывает имена кандидатов с теми случайными кодами, что присвоены им в избирательных бюллетенях. Криптография преобразований данных в Bitcoin устроена так, что пересылка на этот адрес минимальной доли биткоина позволила бы держателю данного списка сделать две вещи: сохранить таблицу в виде публичной записи и при этом не раскрывать содержимое таблицы. Впоследствии, когда выборы закончены и результаты подсчитаны, та же самая доля биткоина пересылается обратно на исходный адрес – для верификации результата. Криптографическими методами адреса сгенерированы так, что любой человек при желании имеет возможность по публичным записям этих транзакций повторить те же самые преобразования, убедившись в том, что данные никто не подменил. То есть сверить сигнатуру открыто опубликованной после выборов «секретной таблицы» с той, что была закодирована до начала голосования; и убедиться, что публикация обязательств была сделана именно до, а не после выборов. Ученые показали, что манипуляции с данными выборов, как и любая попытка подделки публичной записи о биткоин-транзакциях, оказываются вычислительно чрезвычайно сложной задачей.

В заключение хотелось бы отметить, что системы электронного голосования продолжают активно совершенствоваться и с технической точки зрения, и с точки зрения обеспечения защиты информации в процессе голосования и обработки голосов, давая возможность организации дистанционного голосования с помощью любых каналов связи и любых платформ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Электронное голосование в фокусе [Электронный ресурс] // URL: http://aceproject.org/ace-ru/focus/e-voting (дата обращения: 10.03.2014).
2. Фонд развития электронной демократии. Стандарты совета Европы в области электронного голосования [Электронный ресурс] // URL: idemocracy.ru/projects/articles/43-стандарты-совета-европы-в-области-электронного-голосования.html (дата обращения: 10.03.2014).
3. Национальная Избирательная Комиссия Эстонии Обзор системы электронного голосования [Электронный ресурс] // URL: http://mexnap.info/articles.php?article_id=291 (дата обращения: 10.03.2014).
4. Эстонцы раскрыли код своей революционной системы электронных выборов [Электронный ресурс] // URL: http://corp.cnews.ru/news/top/index.shtml?2013/07/15/535367 (дата обращения: 10.03.2014).
5. *Масловская Т.С.* Электронное голосование: опыт зарубежных стран [Электронный ресурс] // URL: http://www.gosbook.ru/node/12744 (дата обращения: 10.03.2014).
6. Зарубежный опыт использования системы электронного голосования [Электронный ресурс] // URL: http://allvoices.ru/jelektronnye-vybory/zarubezhnyj-opyt-ispol-zovanija-sistemy-jelektronnogo-golosovanija.html (дата обращения: 10.03.2014).
7. Реализация системы электронного голосования в России [Электронный ресурс] // URL: http://allvoices.ru/jelektronnye-vybory/realizacija-sistemy-jelektronnogo-golosovanija-v-rossii.html (дата обращения: 10.03.2014).
8. Электронные голосования [Электронный ресурс] // URL: http://saferunet.org/adult/news/675/ (дата обращения: 10.03.2014).
9. Финские власти разрабатывают новую систему электронного голосования для выборов [Электронный ресурс] // URL: http://fontanka.fi/articles/13162/ (дата обращения: 10.03.2014).

10. *Кибкало А.А., Ляпер В.С., Субботин А.Г., Задорожный В.В.* Перспективные системы электронного голосования [Электронный ресурс] // URL: http://www.i-tc.ru/press/publications/binder7.pdf (дата обращения: 10.03.2014).
11. *Киви Берд.* Сделаем это по-честному [Электронный ресурс] // URL: http://kiwibyrd.org/2013/11/24/122/#more-1149 (дата обращения: 10.03.2014).

Статью рекомендовал к опубликованию к.т.н. М.Н. Казарин.

Пескова Ольга Юрьевна – Южный федеральный университет; e-mail: poy@tgn.sfedu.ru; 347922, г. Таганрог, ул. Чехова, 2; тел./факс: 88634371905; кафедра безопасности информационных технологий; к.т.н.; доцент.

Половко Иван Юрьевич – e-mail: i.y.polovko@gmail.com; кафедра безопасности информационных технологий; к.т.н.; ассистент.

Фатеева Светлана Владимировна – e-mail: svetlana.fateeva@rambler.ru; кафедра безопасности информационных технологий; студентка.

Peskova Olga Yur'evna – Southern Federal University; e-mail: poy@tgn.sfedu.ru; 2, Chekhov street, Taganrog, 347922, Russia; phone/fax: +78634371905; the department of security in data processing technologies; cand. of eng. sc.; associate professor.

Polovko Ivan Yur'evich – e-mail: i.y.polovko@gmail.com; the department of security in data processing technologies; cand. of eng. sc.; assistant professor.

Fateeva Svetlana Vladimirovna – e- mail: svetlana.fateeva@rambler.ru; the department of security in data processing technologies; student.

УДК 681.3

К.А. Катков, Е.К. Катков

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ СПУТНИКОВЫХ РАДИОНАВИГАЦИОННЫХ СИСТЕМ ПРИ ИСКУССТВЕННЫХ ИОНОСФЕРНЫХ ВОЗМУЩЕНИЯХ

Целью исследования является уменьшение погрешности местоопределения потребителей спутниковых радионавигационных систем в условиях намеренного создания искусственных возмущений ионосферы на трассе распространения навигационных радиосигналов. В случае возникновения сильных ионосферных возмущений навигационные радиосигналы неминуемо будут подвержены искажениям, которые приведут к многократному увеличению погрешности измерения псевдодальностей до соответствующих навигационных космических аппаратов. Это, в свою очередь, приведет к резкому возрастанию погрешности местоопределения в навигационной аппаратуре потребителей. В работе представлен разработанный алгоритм вторичной обработки навигационных данных, позволяющий за счет многократного измерения псевдодальности в условиях наличия локальной области повышенной ионизации в выбранном рабочем созвездии НКА снизить погрешность местоопределения. Также представлен алгоритм решения навигационной задачи в условиях дефицита навигационных космических аппаратов, когда искусственные возмущения ионосферы делают невозможным прием навигационной информации от большинства видимых аппаратов.

Спутниковые радионавигационные системы; искусственные возмущения ионосферы, вторичная обработка навигационных данных; информационная безопасность спутниковых радионавигационных систем.