Электронное голосование: методы, риски и проблемы

О.Ю. Пескова, С.В. Фатеева

Южный федеральный университет, г. Таганрог
poy@tgn.sfedu.ru

Аннотация

В статье рассмотрены возможные риски и проблемы систем электронного голосования, и в первую очередь – дистанционного. Проведен анализ рисков дистанционного электронного голосования, представлена их классификация, подробно описаны различные группы рисков. Рассмотрены существующие методы и средства организации электронного голосования.: электронный бюллетень Бисмарка, Scantegrity, система электронного голосования Эстонии. Представлена общая классификация подобных систем, описан опыт их использования в разных странах. Описаны проблемы, связанные с организацией электронного голосования, и существующие решения.

Введение

Подведение итогов выборов как в России, так и в других странах нередко заканчивалось громкими скандалами, связанными с фальсификацией итогов голосования. В связи с этим резко возрос интерес к новым технологиям тайного голосования – и прежде всего к электронному голосованию, которое разделяется на стационарное и дистанционное.

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. В отличие от него, термин «дистанционное/удаленное э-голосование» (анг. remote e-voting) используется в ситуации, когда избиратель голосует за пределами избирательного участка из любого месторасположения.

Одной из самых перспективных технологий считается дистанционное электронное голосование через сеть Интернет или иную информационно-коммуникационную сеть передачи данных.

На сегодняшний день реализации электронного голосования во многом мешает стереотип о ненадежности результатов информационных систем. Нами было проведен анализ систем электронного голосования: рассмотрен мировой опыт создания таких систем, исследована ситуация в России, сформулированы проблемы, возникающие при реализации электронного голосования, и предложены направления путей их решения.

1. Опыт использования в разных странах

Австрия. Весной 2004г. федеральное Министерство внутренних дел созвало рабочую группу по проблемам э-голосования с целью изучения и составления отчета о его различных аспектах. Первый, юридически незначимый эксперимент с удаленным голосованием был проведен в мае 2003г. параллельно с традиционным голосованием на выборах в Студенческий Совет в Венском университете экономики и бизнеса (ВУ). Прототип системы э-голосования был создан в ВУ Проф. Проссером и исследовательской группой под его руководством e-Voting.at. За основу была взята система идентификации граждан через электронные id-карты (Bürgerkarte). До дня выборов избирателю необходимо было подать заявку о получении токена, который будет храниться на электронной id-карте. В день выборов избиратель, чтобы подтвердить свое право голоса, предоставляет только лишь токен. В дополнение к этому та же проектная группа провела второй (вновь не являющийся юридически значимым) тест своей системы э-голосования параллельно с традиционным голосованием на президентских выборах 25 апреля 2004г.

Бельгия. В Бельгии из особенностей применяемых технологических решений стоит особо выделить следующие:

- используется моноблок с сенсорным экраном, оптическое перо и считыватель смарт-карт;
- избиратель имеет возможность, либо подтвердить свой первоначальный выбор, либо отменить его и произвести голосование заново;
- когда выбор подтвержден, избиратель получает свою магнитную карту, и после этого никакое изменение сделанного выбора уже невозможно.

Бразилия. Электронные устройства для голосования состоят из двух частей: устройство для идентификации избирателя и «электронная урна»,

Технологии информационного общества в науке, образовании и культуре: сборник научных статей. Материалы XVII Всероссийской объединенной конференции «Интернет и современное общество» IMS-2014, Санкт-Петербург, 19 - 20 ноября 2014 г.

которая имеет связь с технологическим центром и состоит из экрана и цифровой клавиатуры, на которой избиратель должен набрать цифровой код кандидата. Идентификация производится только с помощью карты избирателя - документа, который гражданин обязан получить по достижении им 18-летнего возраста. Без карты избирателя в Бразилии, нельзя, например, получить водительское удостоверение, поступить в ВУЗ, получить пенсию, поэтому такую карту можно считать универсальной и достаточно удобной.

Великобритания. Первые эксперименты по внедрению электронного голосования в Великобритании были начаты в 2001. В ходе них было проведено более 150 пилотных проектов в 100 округах, охвачено 6,4 миллиона избирателей. реализовано 17 централизованных проектов электронного голосования - интернет-киоски, интерактивное телевидение, голосование по телефону, и посредством смс-сообщений. При этом 14 проектов касались интернет-голосования. В рамках их голосование могло осуществляться с любого компьютера с применением персонального пароля, получаемого одновременно с идентификационной получили в специальном консультативном документе, где особо отмечалась их эффективность. В 2002 году в ряде районов было разрешено голосование через интернет (с домашних компьютеров) и с использованием мобильных телефонов (посредством смс-сообщений). На муниципальных выборах в Ливерпуле и в Шеффилде в экспериментальном порядке было разрешено голосование через Интернет, в в 2003 также в Шеффилде и в Сент-Олбанс.

Германия. Германия начала экспериментировать с электронным голосованием в 1999 г. Экспериментальное э-голосование проводилось в выборах неполитического характера: в университетах (Оснабрюк, Бремерхафен), в местных совещательных органах (молодежные сообщества и советы пожилых граждан), а также в профсоюзах в государственном и частном секторе. Система интернет-голосования, которая использовалась в большинстве тестов в Германии, была разработана Исследовательской группой по интернет-голосованию.

Испания. В Испании первый эксперимент по электронному голосованию проводился в 2004 году в связи с выборами 14 марта, при этом голосование осуществлялось уже после официальных выборов в бумажной форме. Голосование производилось либо с помощью SMS, либо с использованием персонального компьютера с доступом в Интернет (компьютеры имелись, в том числе и на избирательных участках) и устройством, способным считывать информацию со смарт-карты.

Канада. В период 5-10 ноября 2003г. в канадской провинции Онтарио 12 муниципалитетов из графства Прескотт и Рассел и графства Стормонт, Дандас и Гленгарри первыми во всей Северной Америке провели выборы в местные самоуправления и отделы среднего образования используя только электронные средства голосования. Каждый избиратель 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 (Secretariat for Democratic Renewal), задачей которого стало выработать предложения по реформе избирательного процесса в Онтарио.

Нидерланды. В большинстве общин Нидерландов голосование проводится на избирательных участках в электронной форме. Во время выборов в Европейский Парламент в 2004г. граждане, находящиеся за пределами государства в день выборов и подавшие заявку о дистанционном э-голосовании, могли отдать свой голос через Интернет или телефон. В ходе многолетнего общенационального обсуждения политические партии, муниципалитеты и Центральная Избирательная комиссия Голландии в итоге посчитали использование электронного голосования в ходе выборов целесообразным, в свете соотношения прилагаемых средств и предполагаемого позитивного результата. Поэтому Избирательный Совет, во взаимодействии с Ассоциацией голландских муниципалитетов, организовали разработку программного обеспечения (OSV) для проведения выборов и голосования. Впервые OSV было использовано на выборах в Европейский парламент 4 июня 2009 года.

Норвегия. В Норвегии первые эксперименты, связанные с внедрением электронного голосования были проведены на муниципальных выборах в нескольких районах 15 сентября, 26 и 27 октября 2003 года. Была использована идентификация с помощью смарт-карты. Далее проводилась двухступенчатая система голосования: сначала голосование за список кандидатов, а затем, в рамках этого списка, уже за конкретных кандидатов.

США. Для повышения уровня доверия избирателей к электронному голосованию в ряде штатов были приняты решения о замене сенсорных машин для голосования на сканирующие электронные средства для голосования (таким образом, избирателям предоставляется возможность удостовериться в своем электронном выборе при помощи бумажного носителя). В 41 штате применяются оптические комплексы для электронного голосования, наряду с сенсорными, включая 17 штатов, где они используются на всех без исключения избирательных участках. Голосование посредством использования сети Интернет применяется только в графстве Окалооза (остров Окалооза), штат Флорида. Широкая дискуссия насчет выполнимости э-голосования

развернулась после эксперимента SERVE, который был разработан для участия экспатриантов в голосовании на президентских выборах США в ноябре 2004г. Проект был приостановлен весной 2004г. на основании заключения 4 членов группы оценки, поддерживаемой Департаментом Обороны. Эти эксперты призывали к немедленному свертыванию программы SERVE, так как считали Интернет и персональные компьютеры недостаточны безопасным медиумом для голосования.

Франция. Во Франции интернет-голосование применяется исключительно для граждан, находящихся за границей с 2003 года, а само электронное голосование ориентировано исключительно на машины для голосования на избирательных участках. В 2007 году во Франции впервые были использованы электронные машины для голосования с сенсорным экраном и функцией подтверждения выбора на президентских выборах (на парламентских выборах впервые они использовались в июне 2006 года). Эти выборы оппозицией впоследствии были охарактеризованы негативно, хотя официально они и считалась законными и легитимными.

Швеция. В Швеции используются специальные карты идентификации избирателей, высылаемые по почте. Однако само голосование осуществляется с помощью обычных бумажных бюллетеней. Таким образом, был создан комбинированный вариант «бумажного» и «электронного» голосования, появившийся после критических оценок электронного голосования Шведской избирательной комиссией.

Швейцария. Используется полностью автоматизированная система, направляющая избирателя на специализированный сайт. Перед референдумом каждый избиратель может, предъявив паспорт, взять в ближайшем почтовом отделении карточку для электронного голосования, содержащую уникальный номер, который может совпасть один раз на 5 миллиардов избирателей, и секретный код, скрытый под непрозрачным защитным слоем. На сайте электронного голосования необходимо ввести номер карточки. Только теперь избиратель допускается на сервер, где проводится само голосование: поставить галочки напротив нужных вариантов референдума, ввести секретный PIN-код и данные своего паспорта и получить электронное подтверждение голоса, которое в дальнейшем может быть проверено в администрации кантона.

Эстония. В Эстонии нам интересен в первую очередь именно опыт интернет-голосования. Здесь для увеличения активности избирателей вообще и повышения интереса среди молодых избирателей в частности, а также в целях глобальной модернизации процедуры голосования была реализована система цифровой подписи и достаточно эффективная и быстрая система проверки ее подлинности. В основе системы интернет-голосования в Эстонии лежит использование персонального документа, удостоверяющего личность (идентификационной карточки), который принимается для удостоверения личности в сети Интернет и совершения электронной цифровой подписи. В целях предотвращения покупки и продажи голосов, а также иного влияния на волеизъявление избирателей, допускалось проголосовать с использованием электронной формы несколько раз, но последний голос считался окончательным. и только он и учитывался.

Проект ЕС КиберГолос. В сентябре 2000г. 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». 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).

Первый эксперимент с новой системой состоялся 11 декабря 2002г. во французском городе Исси-ле-Мулино. Второй эксперимент был проведен 13-15 января 2003г. в Бременском университете в Германии. Опция электронного голосования была доступна в ходе выборов трех представительных органов университета: совета университета, совета департаментов университета и студенческого совета. Последнее испытание было проведено в районе Стокгольма Чисте при участии пожилых избирателей. Привлечь избирателей старше 55 лет к пользованию системой э-голосования потребовало много усилий. Проект КиберГолос завершился в июле 2003г. [1]

2. Анализ рисков дистанционного электронного голосования

2.1. Общая классификация

Несмотря на очевидные преимущества дистанционного голосования перед традиционным, оно имеет свои недостатки, способные серьезным образом повлиять на ход и результаты выборов. Данная форма голосования содержит определенные риски, которые на основе анализа их содержания можно разделить на следующие группы (рис. 1):

– риски, связанные с необходимостью обеспечения важнейших принципов избирательного права;

- риски, связанные с доверием избирателей к процедуре дистанционного электронного голосования;
- риски, связанные с несовершенством технологии дистанционного электронного голосования в области защиты информации и сложности самой процедуры голосования;
- риски, связанные с технической реализацией проекта

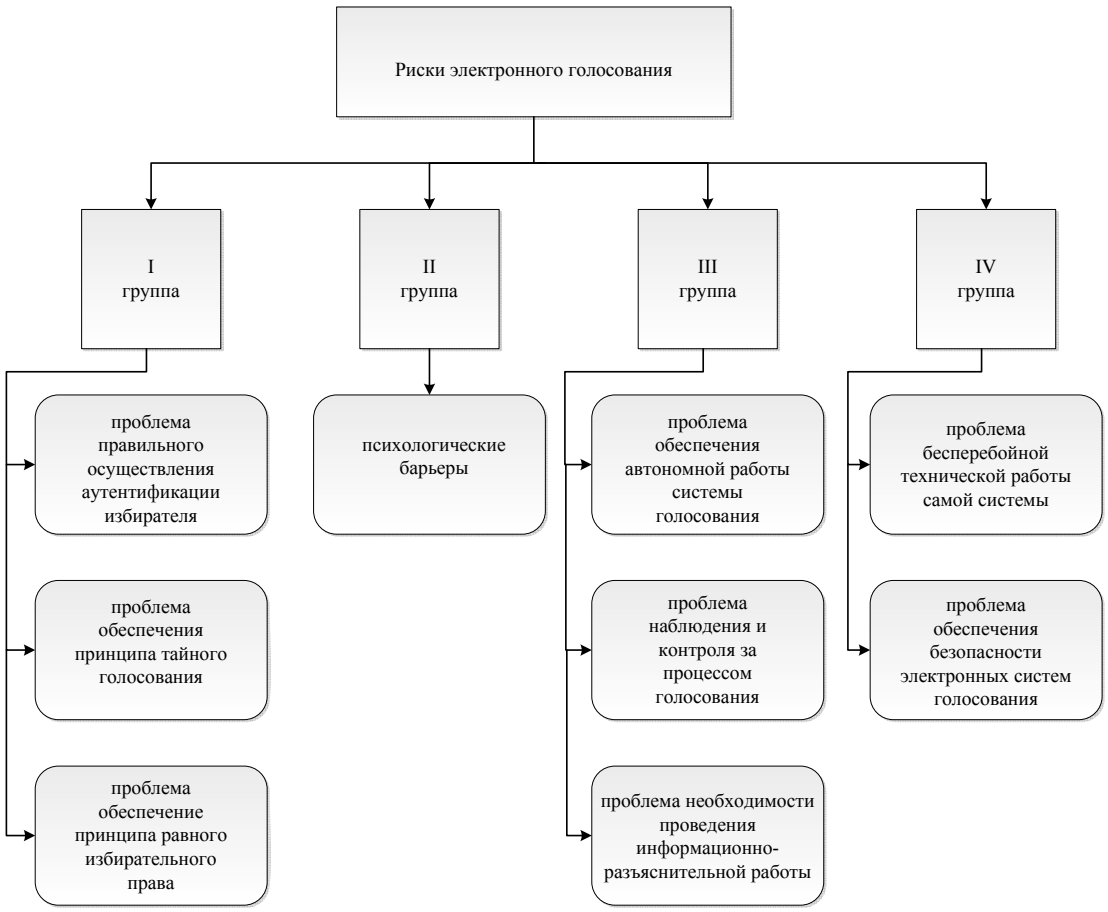

Рис. 1. Риски и проблемы

2.2. Риски первой группы

Остановимся на анализе первой группы рисков, в рамках которой остро встает проблема правильного осуществления аутентификации избирателя (обеспечение принципа личного голосования). При голосовании с помощью мобильного телефона возможность такой идентификации при настоящем уровне развития технологий практически отсутствует. Несмотря на то, что для предотвращения повторного голосования одним человеком или использования чужой SIM-карты каждому избирателю присваивается уникальный код, который действует однократно, гарантий того, что с телефона и SIM-карты голосует именно то лицо, которому выдан код, нет никаких. При голосовании непосредственно через Интернет и с помощью социальной электронной карты рассматриваемую проблему предлагается решить путем внедрения системы электронной цифровой подписи (ЭЦП). Избиратель может либо заранее единовременно получить ключ ЭЦП для доступа на сервер для голосования на всех последующих выборах, либо получать ключи электронной цифровой подписи каждый раз накануне выборов. В первом варианте проблема заключается в том, что длительный период хранения резко снижает надежность подобных ключей. Они могут быть либо похищены в базе данных избирательной комиссии, либо у самого избирателя, а соответственно есть вероятность начала спекулятивной торговли такими ключами, превращения его в некий специфический объект

подкупа избирателей. При применении второго варианта пропадает основное преимущество данной формы голосования – удобство, так как за день до голосования избиратель должен лично посетить помещение, в котором расположена избирательная

комиссия, зарегистрироваться и получить ключ для доступа. Зарубежной практикой был найден другой выход - использование индивидуальной идентификационной карты (ID-карты), позволяющей ставить электронную цифровую подпись. Преимущество ID-карты по сравнению с указанными выше вариантами в том, что данное решение имеет универсальный характер, несколько степеней защиты, выдается один раз и не позволяет голосовать за другого избирателя, т.к. избиратель идентифицирует себя, указав свой секретный код, дату и место рождения. \

К проблеме аутентификации избирателя тесно примыкает и проблема обеспечения принципа тайного голосования, на которую обращено особое внимание в Рекомендациях Совета Европы. Социологические исследования, проведенные одновременно с экспериментами по электронному голосованию, наглядно демонстрируют обеспокоенность избирателей возможностью нарушения тайны их голосования. При привычной схеме выборов для соблюдения тайны голосования достаточно убедиться, что бюллетень не подписан вашей фамилией и что в кабине для голосования не присутствуют посторонние лица. При применении систем дистанционного электронного голосования избиратели уже не могут самостоятельно удостовериться, что информация, позволяющая идентифицировать их личность, не была прикреплена к электронному бюллетеню при отправке на сервер голосования. На практике выработаны достаточно универсальные подходы к решению данного вопроса. Так, например, в Швейцарии используется подход, обеспечивающий тайну голосования отсутствием поименного списка избирателей, содержащего идентифицирующие личность данные, а лишь наличием списка, содержащего номера действительных карточек для голосования. Другой способ, представляющийся более предпочтительным, заключается в использовании т.н. серверов деперсонификации, которые стирают информацию, индивидуализирующую избирателя. Данный способ получил широкое распространение при проведении экспериментов по электронному голосованию в России. Наряду с указанными способами, широко применяется и технология «перемешивания» электронного ящика для голосования, т.е. электронные бюллетени считываются не по мере их поступления, а в произвольном порядке.

Обеспечение принципа равного избирательного права при применении рассматриваемой формы голосования имеет свои специфические черты. И, в первую очередь, эти особенности связаны с необходимостью существования определенных технических предпосылок для голосования у самого избирателя. Так, например, избиратель должен иметь мобильный телефон определенных технических характеристик или иное устройство с выходом в Интернет [2].

Таким образом, данная ситуация делает пока невозможным введение электронного голосования дистанционным способом в качестве универсальной формы голосования, однако и при использовании его в качестве дополнительного способа на выборах в целом проблема равенства еще более обостряется, т.к. возникает возможность подачи избирателем голоса более чем одним каналом для голосования. Поэтому возникает необходимость формирования некой единой базы данных о проголосовавших, которая обновляется в режиме реального времени.

Таким образом, риски, обозначенные при классификации в первой группе, могут быть минимизированы при наличии воли законодателя во внесении необходимых изменений в правовые акты и в результате разработки и внедрения определенных технологий..

2.3. Риски второй группы

Для многих людей, не знакомых с принципами работы дистанционных технологий, это будет вопрос веры. Да и в целом доверие к электронным средствам голосования также одна из актуальнейших проблем, на необходимость решения которой, указывается в п. 20 Рекомендаций Совета Европы. Преодолеть психологические барьеры для использования технологий дистанционного электронного голосования будет весьма непростым делом, что обуславливает выделение данной проблемы в отдельную группу рисков. Согласно инициативному опросу, проведенному в сентябре-октябре 2008 года по федеральной выборке, лишь треть россиян (34%) в целом положительно относится к идее интернет - голосования (из них 24% - скорее, положительно, 10% - безусловно положительно). Половина сограждан (48%) негативно относится к такому нововведению (среди лиц пожилого возраста такая цифра составляет около 70%) [2].

Однако проведенные подобным же образом исследования в Эстонии показали, что рассматриваемое отношение не зависит от пола, уровня дохода, политических пристрастий. Исследователями была установлена зависимость от возраста и уровня образования избирателей. При этом было особо отмечено, что данная зависимость отражает лишь структуру пользователей Интернета и по мере распространения технологий и вхождения их в повседневную жизнь людей она будет снижаться. Таким образом, решение данной проблемы представляется делом времени..

2.4. Риски третьей группы

Перед предоставлением статьи в оргкомитет При применении систем дистанционного электронного голосования, как и любой электронной системы, остро встает вопрос необходимости защиты данных, который тесно связан с обеспечением возможности избирателя отследить, правильно ли учтен его голос, что в совокупности составляет третью группу

рисков. Следует особо отметить, что именно этот вопрос в наибольшей степени волнует потенциальных участников дистанционного электронного голосования. Возможность фальсификации результатов выборов значительно облегчается тем, что при отсутствии избирательного бюллетеня «материальным» носителем волеизъявления является исключительно информация, которая как таковая может быть легко изменена. Если также учесть большую опасность применения хакерских атак, то электронное голосование на выборах при самом неблагоприятном сценарии имеет весьма большие шансы стать мощным инструментом политических манипуляций, одним из действенных способов узурпации власти. В связи с чем перед разработчиками стоит достаточно сложная задача обеспечить автономную работу системы дистанционного голосования, пресекающую каждую попытку вмешательства в его функционирование. В настоящий момент широкое распространение имеет криптографическая защита.

В отношении вопроса правильности учета голоса избирателя существует норма Рекомендации Совета Европы:«дистанционная система электронного голосования не должна позволять избирателю иметь возможность получать доказательство содержания поданного голоса». Данное положение направлено на обеспечение одного из важнейших принципов выборов – тайны голосования, но в то же время она лишает возможности избирателя удостовериться в правильности учета его голоса. Однако эти нормы являются лишь рекомендациями.

Это обстоятельство указывает на еще одну проблему - проблему наблюдения и контроля за процессом голосования. При удаленном электронном голосовании объективно невозможно обеспечить наблюдение и контроль за непосредственным процессом подачи голоса, а также его подсчета. Однако рассмотренными методиками подобный контроль в ограниченной «индивидуальной» форме, но реализуется.

Барьером является также сложность процедуры голосования и вытекающая из нее проблема необходимости проведения информационно-разъяснительной работы по доведению до избирателей сведений о технологии. Вполне реальной представляется ситуация, когда вследствие либо неправильного использования самими избирателями технических устройств, либо ошибок разъяснительной работы будут иметь место нарушения избирательных прав, заблуждение граждан в вопросе своего волеизъявления [2].

2.5. Риски четвертой группы

Кроме проблемы собственно определенных действий, направленных на обеспечение защиты данных, проблема далеко не бесперебойной технической работы самой системы также является актуальной, в связи с чем представляет собой четвертую группу рисков.

Данное обстоятельство вызвано в первую очередь несовершенством самой технологической базы всех электронных систем, а также отсутствием единого подхода и универсальных требований к качеству и безопасности самих систем дистанционного электронного голосования.

Ярким примером уязвимости систем для Интернет – голосования стала система SERVE, созданная по заказу Пентагона для голосования через Интернет тех граждан Соединенных Штатов Америки, что находятся за рубежом. Результаты экспертизы оказались неудовлетворительными. Новая пентагоновская система, как указано в отчете, «предоставляет злоумышленникам чересчур много возможностей вмешиваться в процесс честного и аккуратного голосования, причем такими способами, которые потенциально невозможно выявить» [2].

Отечественный опыт в этом вопросе также является весьма интересным. Так, именно опасения в области безопасности вынудили ЦИК РФ отказаться от дальнейшей работы в отношении такого характерного для ранней отечественной практики способа, как голосование с использованием CD-дисков.

Обеспокоенность проблемой обеспечения безопасности электронных систем голосования подтверждается как многими научными исследованиями (в частности университета De Montfort University), так и проведенными социологическими исследованиями. Данные обстоятельства предопределяют необходимость международной сертификации систем электронного голосования, а также введения положения об обязательном проведении предварительного аудита такого оборудования, что нашло свое отражение и в Рекомендациях Совета Европы.

Рассмотренные в настоящей главе возможные риски электронного голосования дистанционным способом говорят не о проблемности самого дистанционного электронного голосования как формы выражения волеизъявления избирателей, а лишь об определенных технических, а также финансовых сложностях

3. Существующие методы электронного голосования

3.1. Идея электронного бюллетеня Бисмарка и его аналог система Бена Адида

Идея электронного бюллетеня или система Prêt à Voter была предложена профессором Питером Райаном (Peter Y.A.Ryan) и разработана группой исследователей из университета Суррея в Гилфорде, Великобритания.

Бюллетень делится на две части. В левой части указывается список кандидатов. Правая часть состоит из пустых полей, в одном из которых избиратель должен поставить знак, обозначающий его выбор. Рядом с полями печатается QR-код

бюллетеня, где зашифрован уникальный случайный набор чисел — пин-код. Сделав выбор, избиратель разрывает его по перфорации на две части. Левая часть с кандидатами остается у избирателя, а правая часть бюллетеня сканируется или опускается в избирательную урну.

Для подсчета голосов с бюллетеня считываются и передаются в центральную базу данных два числа: порядковый номер проставленной «галочки» и пин-код с QR-кода, который является специальным ключом, помогающим расшифровать, что означает выбор в соответствующем квадрате бюллетеня.

К моменту подсчета голосов сформируется база данных, состоящая из чисел и отдельных частей общего ключа, то есть каждого пин-кода, участвовавшего в голосовании. Чтобы ее расшифровать потребуется сложить все части ключей. При этом, определенные части ключей будут находиться у партий. Если партии согласны с ходом выборов, то они предоставляют для проведения подсчетов свои части ключей. После этого все ключи собираются вместе, складываются, и расшифровываются результаты голосования.

Анонимность голосования является, с одной стороны, сильной стороной бюллетеня Бисмарка, а с другой является его серьезной уязвимостью по причине сложности в доказательстве собственного выбора, кроме того, анонимность записей в центральной базе позволяет администратору внести туда сколько угодно «нужных» полей.

Тем не менее, данный метод способен обеспечить прозрачность, конфиденциальность, честность и безопасность подсчета голосов избирателей. [3].

Аналогом бюллетеня Бисмарка является система Бена Адида, основанная на паре ключей — секретного и публичного, по аналогии с системами банкоматов [4].

Для такой системы были определены следующие требования:

- система публичных/частных ключей: голосующие зашифровывают голос, кандидаты — расшифровывают;
- генерируемые случайные ключи: для каждого голосующего генерируется случайный ключ, так что голоса за одного кандидата от разных людей не являются идентичными в зашифрованном виде.

В такой системе можно использовать любой алгоритм шифрования, подобный RSA, который основан на использовании пары публичный-частный ключ

Само голосование может происходить так, если используется принцип доказательства с нулевым разглашением знаний:

- Избиратель проверяет бюллетень. Голосующий выбирает два любых бюллетеня, соскребает случайные числа (публичный ключ) с одного из них и сканирует двумерный штрих-код чтобы удостовериться, что указанный там порядок кандидатов соответствует зашифрованной информации. Этот бюллетень перестает быть действительным, а избиратель использует второй.
- Избиратель делает выбор.
- Отрывает левую часть.
- Уничтожает публичный ключ.
- Сканирует бюллетень.

Отсканированные бюллетени публикуются на вебсайте. Проголосовавший может проверить, был ли его голос учтен, и если был — все ли прошло без ошибок.

Данная система была опробована на выборах в локальные органы самоуправления в университетах MIT, Harvard, Unversite Catholique de Louvain (25000 избирателей), University of Ottawa. 3 ноября 2009 года эта система применялась на выборах в Takoma Park, Maryland, USA.

3.2. Система электронного голосования Scantegrity и ее улучшение с помощью CommitCoin

На международной криптографической конференции Financial Cryptography 2012 двое канадских ученых, Джереми Кларк и Александр Эссекс, представили свою исследовательскую работу под названием «CommitCoin – ‘углеродная датировка’ обязательств с помощью системы Bitcoin».

В этой работе исследователи теоретически показали (а также уже продемонстрировали на практике реальных выборов), что возможности БитКойна можно также использовать в качестве своеобразной формы «углеродной датировки» для фиксации времени появления практически любой цифровой информации. В конкретном же контексте электронных выборов эта технология оказывается весьма полезным инструментом для защиты от жульничества и подделки итогов голосования.

Монеты-биткойны конкретного человека здесь зарегистрированы по адресам, которые представляют собой случайного вида буквенно-цифровые последовательности, выступающие в качестве идентификаторов данного пользователя в пиринговой сети. Когда имеет место транзакция – пересылка битмонет с одного адреса на другой – то она широковещательно сообщается в сеть, чем создается публичная запись транзакции. Поскольку пользователь Bitcoin генерирует свои адреса сам, Кларк и Эссекс установили, что к нужному виду Биткойн-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 биткойна – совсем небольшая транзакция – 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 биткойна 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.

Опираясь на математически просчитанную безопасность системы Bitcoin, ученые показали, что здесь манипуляции с данными выборов, как и любая попытка подделки публичной записи о биткойн-транзакциях, оказываются вычислительно чрезвычайно сложной задачей. Потому что для жульничества вам здесь понадобилось бы больше вычислительных мощностей, чем имеет вся остальная часть сети BitCoin вместе взятая. На данной особенности, собственно, и построено обеспечение безопасности этих цифровых наличных.

CommitCoin не является собственно инструментом электронного голосования, скорее, обеспечивая лишь один из многих методов обеспечения честных и насквозь проверяемых выборов. Как говорят об этом сами создатели технологии: «Пример подлинно проверяемого голосования может дать технология выборов, на 95% состоящая из системы Scantegrity и на 5% – из подсистемы CommitCoin. Мы только лишь добавляем некоторое количество дополнительной верификации для одной из конкретных фундаментальных основ Scantegrity».

Подобного рода криптографические системы для выборов ныне часто называют E2E или «end-to-end verifiable» (т. е. насквозь проверяемое) голосование. Scantegrity – это одна из таких систем, но есть и другие, созданные чуть ранее весьма авторитетными в области криптографии специалистами, вроде системы Punchscan (Дыркоскан), изобретенной Дэвидом Чомом, автором концепции «цифровых наличных» и целого ряда криптографических протоколов, широко применяемые ныне в электронной коммерции, или системы 3Ballot (Трехчастевой бюллетень) знаменитого криптографа Рональда Райвеста.

Система Scantegrity из этого ряда особо интересна тем, что в своем нынешнем виде (Scantegrity II) она – пока что единственная E2E-система, которую реально и уже дважды успешно применяли на выборах государственной власти

Одна из главных особенностей системы Scantegrity заключается в том, что она специально создана для усовершенствования уже существующих процедур голосования и работает как бы «поверх» них.

В основу Scantegrity положена система голосования с оптическим сканированием бюллетеней – на сегодняшний день это доминирующая технология выборов в США. E2E-надстройка, реализованная системой Scantegrity, работает так. Здесь избиратель вместо обычной ручки использует особый фломастер, который проявляет уникальный код, напечатанный внутри кружка невидимыми чернилами. Когда этот бюллетень пропускается через обычный оптический сканер, тот просто определяет, какой именно из кружков против кандидатов был закрашен – то есть все как раньше.

Всякий избиратель, желающий проверить, что его голос учтен и подсчитан правильно, при выборах записывает тот код, который был проявлен в кружке бюллетеня, в сочетании с уникальным серийным номером бюллетеня. Позднее проголосовавший может проверить свой серийный номер на веб-сайте избирательной комиссии и убедиться, что он поставлен в соответствие тому коду, который был внутри помеченного им кружка. Здесь этот код, хотя он и вывешен на веб-сайте для всеобщего обозрения, уже никак не привязан к имени кандидата, за которого был отдан голос.

Вся система выстроена и математически рассчитана таким образом, что если всего лишь 2 процента избирателей проверят и подтвердят свои коды, то статистически оказывается практически невозможным, чтобы подделка результатов голосования прошла невыявленной (на реальных выборах в Мэриленде свои номера и коды сверили через интернет около 4% избирателей).

Перед выборами избирательная комиссия готовит набор «битовых обязательств» таблиц, которые – при их сведении вместе – связывают коды бюллетеней и имена кандидатов. Но при этом данные связи не могут быть установлены или вычислены по любой из этих таблиц, взятых по отдельности. Затем комиссия открыто публикует набор цифровых сигнатур, которые фиксируют все позиции этих таблиц, но при этом реальное содержание списков не раскрывается.

На финише, когда процедура выборов закончена, избирательная комиссия открыто публикует содержательную часть информации из таблиц-обязательств (те коды, что были проявлены на всех зарегистрированных в выборах бюллетенях) вместе с криптоключами, которые верифицируют подлинность этих данных. Но при этом частично раскрытое содержание таблиц скрывает достаточно информации, чтобы сохранять анонимность избирателей. Однако данные таблицы раскрывают вполне достаточно информации для всякого, кто заинтересован в проверке честности голосования и выявлении возможных подделок результатов.

Хотя высокая криптографическая стойкость системы Scantegrity к манипуляциям данными и к подделке итогов выборов просчитана очень тщательно, но и у нее есть недостатки. Например, система недостаточно защищена от предварительного сговора нескольких партий, желающих убрать сильного и потому нежелательного для остальных кандидата. В таких условиях теоретически становится возможен сценарий жульничества с «перебросом» голосов – например, когда , при итоговом подсчете бюллетеней происходит «сбой» программы, в результате которого происходит обмен голосов между лидером и аутсайдером.

Поскольку конструкция подсистемы CommitCoin позволяет обеспечивать «углеродную датировку» сообщений, запущенных в сеть BitCoin, избиратели после подсчетов имеют возможность удостовериться, что данные таблиц-обязательств для выборов были зафиксированы до того, как началось голосование, а не после. Как сказал Джереми Кларк, система «CommitCoin позволяет проверяющим не доверять вообще никому» [3].

3.3. Система электронного голосования Эстонии

Система электронного голосования Эстонии состоит из следующих компонент:

- списки избирателей;
- списки кандидатов;
- результаты волеизъявления избирателей.

В результате же она дает:

- итоговую сумму голосов избирателей, воспользовавшихся электронной системой голосования;
- список избирателей, воспользовавшихся электронной системой голосования.

Система включает в себя следующие элементы.

Избиратель – избиратель со своим ПК. Создает зашифрованный и подтвержденный цифровой подписью голос и отправляет его в Центральную Систему.

Центральная Система (ЦС) – компонент системы, подотчетный Национальному Избирательному Комитету (НИК). Получает и обрабатывает голоса, в результате чего получает общие результаты электронного голосования.

Система управления ключами (СУКл) – создает криптографическую пару (криптографические пары) системы и управляет ей (ими). Открытые ключи интегрируются в прикладные программы избирателей, секретные ключи передаются в программу подсчета голосов. По завершении периода подачи жалоб секретный ключ уничтожается.

Система контроля (СК) – разрешает споры и жалобы, используя зарегистрированные данные из ЦС.

ЦС также зависит от двух других сторон:

- составителя списков избирателей (Система учета населения);
- составителя списков кандидатов (сам НИК).

Теперь рассмотрим компоненты ЦС:

Сервер, пересылающий голоса (СПГ) идентифицирует личность избирателя при помощи идентификационной карты, предоставляет избирателю список кандидатов и получает зашифрованный и подтвержденный цифровой подписью электронный голос, который голос немедленно отсылается на сервер хранения голосов и подтверждение, полученное оттуда, направляется избирателю.

Сервер хранения голосов (СХГ) принимает электронные голоса от СПГ и хранит их. После закрытия избирательных участков предварительного голосования аннулирует двойные голоса, голоса избирателей, не имеющих право голосовать, а также получает и обрабатывает данные о погашении электронных голосов. В заключение он отделяет внутренние конверты от внешних и подготавливает их для работы программы подсчета голосов.

Процедуры электронного голосования:

А. Управление ключами. Методика управления ключами и используемая схема безопасности являются одним из ключевых элементов системы, от которого зависит соответствие основным требованиям к системе (конфиденциальность и секретность голосования). Создается криптографическая пара системы. 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. Несмотря на то, что эти данные в системе разделены, риск, тем не менее, остается.

Секретный ключ может подвергнуться следующим двум опасностям:

- Компрометация ключа или открытие к нему общего доступа – стороны получают в свое распоряжение 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.

Б. Голосование и хранение голосов. Голосование проводится во время предварительных выборов. Когда завершается предварительное голосование, ЦС прекращает обмен информацией с внешним миром.

Голосование представляет собой обмен данными между избирателем и СПГ. СПГ запрашивает в местных базах данных списки избирателей и кандидатов и в заключение отсылает голос в СХГ. СПГ – это единственный компонент ЦС, к которому существует прямой доступ через Интернет – все остальные компоненты защищены внутренним брандмауэром, и доступ к ним возможен только через СПГ.

Процесс голосования заключается в следующем.

1. Избиратель через HTTPS-протокол получает доступ к СПГ и удостоверяет свою личность с помощью идентификационной карты.

2. СПГ отправляет запрос в базу данных избирателей, используя личный идентификационный код (ЛИК) избирателя, и получает информацию о принадлежности его к определенному избирательному округу. Если избиратель не имеет право голосовать, то выводится соответствующее сообщение, и он направляется в службу X-tee, где избиратель может проверить свой статус по отношению к праву голосовать.

3. СПГ запрашивает в СХГ информацию о том, голосовал ли уже данный избиратель. Если ответ положительный, то избиратель об этом информируется.

4. СПГ отправляет запрос, используя данные из базы данных избирателей, и получает список кандидатов избирательного округа, к которому относится избиратель.

5. Избиратель выбирает кандидата.

6. Прикладная программа избирателя просит подтвердить свой выбор.

7. Прикладная программа зашифровывает голос и случайное число открытым ключом ППГ. Избиратель подписывает криптограмму (далее: голос) своей цифровой подписью.

8. Прикладная программа избирателя передает конверт, подписанный электронной подписью, в СПГ, который проверяет формальную правильность полученного материала и тот ли человек, который удостоверил свою личность в начале сеанса, поставил цифровую подпись.

9. СПГ направляет полученный голос в СХГ. СХГ получает доступ на сервер подтверждения действительности и получает сертификат, подтверждающий действительность цифровой подписи, который затем добавляется к подтвержденному голосу.

10. В случае успешного проведения процедуры СХГ отсылает СПГ подтверждение, что голос получен. Избирателю также доставляется соответствующее сообщение. В системном журнале (LOG1) делается запись о том, что голос получен.

Избиратель может голосовать несколько раз. Все голоса передаются через СПГ в СХГ. После окончания электронного голосования СПГ прекращает все процессы передачи информации.

В. Удаление и сортировка голосов. Прикладная программа СХГ является центральным компонентом на этапе удаления и хранения голосов. Результатом этого процесса являются голоса (зашифрованные номера кандидатов, от которых отделены цифровые подписи) и список избирателей, воспользовавшихся электронной системой голосования.

После завершения предварительных выборов двойные голоса немедленно удаляются. В расчет принимается только последний из голосов, поданных одним избирателем.

Каждый удаленный голос фиксируется в системном журнале (LOG2) указывается причина, где причиной может быть:

- несколько голосов, поданных одним избирателем;
- участие в предварительных выборах;
- переголосование в день выборов.

После удаления двойных голосов формируются списки электронных избирателей, которые отправляются на избирательные участки одновременно с конвертами предварительных выборов.

Следующий этап – этап аннулирования голосов. В первую очередь в запросах отмечаются избиратели, проголосовавшие как с помощью электронной системы, так и на досрочных выборах традиционным способом. Избиратели, проголосовавшие с помощью электронной системы, могут, если захотят, переголосовать на избирательном участке до 17.00. По истечении этого времени избирательные участки прекращают вносить изменения в требования на аннулирование, подписывают их как документ и отсылают в окружную избирательную комиссию. Она составляет электронный список из данных, предоставленных избирательными участками, ставит цифровую подпись (в комиссии должны присутствовать как минимум два человека, которые могут поставить электронные подписи) и отправляет список в НИК.

НИК, в свою очередь, подготавливает сводный список из полученных, подписывает его электронной подписью (снова необходимо как минимум двое человек) и направляет в СХГ. Последний проверяет цифровую подпись, сохраняет список аннулирований и выполняет аннулирование (с записью в системном журнале LOG2).

Когда завершен период аннулирования, внешние конверты отделяются от внутренних, т.е. цифровые подписи отделяются от заверенного содержимого (голосов). Из цифровых подписей извлекаются личные идентификационные коды, которые используются для отправки запросов в базу данных избирателей.

Внешние конверты вскрываются, т.е. цифровые подписи удаляются, а остаются криптограммы, зашифрованные открытым ключом ППГ (т.е.

голоса). Цифровые подписи хранятся отдельно без содержания – это «список избирателей, воспользовавшихся системой электронного голосования».

Г. Подсчет голосов. Подсчет голосов производится в Программе подсчета голосов, не являющейся частью сети. Для подсчета голосов секретный ключ системы активируется администраторами СУКл в соответствии с установленными процедурами управления ключами.

Голоса расшифровываются с помощью секретного ключа (ключей). Расшифрованный голос проверяется по списку кандидатов на предмет возможности голосования за этого кандидата в данном избирательном округе. Если номер кандидата неверен, голос объявляется недействительным. В системном журнале LOG4 делается соответствующая запись.

Действительные голоса суммируются по кандидатам и избирательным округам и записываются в системном журнале LOG 5.

Результаты электронного голосования добавляются к результатам обычного голосования.

Программа контроля позволяет определить, что произошло с голосом, отмеченным определенным ЛИК. Возможны следующие варианты:

голос принят – запись в LOG1;

голос аннулирован, т.к. избиратель проголосовал на избирательном участке в течение предварительных выборов – запись в LOG2;

голос аннулирован, т.к. избиратель проголосовал в день выборов – запись в LOG2;

голос аннулирован, т.к. кандидат, чей номер был отмечен в бюллетене, не баллотировался в данном избирательном округе – запись в LOG3, и дополнительно соответствующий хэш (голос) записывается в LOG4;

голос засчитан – запись в LOG3 и соответствующий хэш (голос) записан в LOG5.

К программе контроля в основном прибегают при рассмотрении жалоб. Кроме того, программа контроля имеет возможность проверять журналы на полноту содержащейся информации: LOG2 и LOG3 вместе должны соответствовать содержимому LOG1; LOG4 и LOG5 вместе должны соответствовать содержимому LOG3. [6].

3.4. Проблемы и существующие решения

Каждая проблема, связанная с той или иной стороной дистанционного электронного голосования, находит свое решение. Предложим следующий список основных проблем и их решений:

1. Проблема правильного осуществления аутентификации избирателя (обеспечение принципа личного голосования). Для систем голосования с помощью мобильного телефона было предложено использовать уникальный код, который присваивался каждому избирателю, для предотвращения повторного голосования одним человеком или использования чужой SIM-карты. Но все равно данная технология не дает никаких гарантий того, что голосует именно то лицо, которому выдан код.

Для систем голосования с помощью социальной карты или через Интернет решили использовать электронную цифровую подпись, заменяющую собой собственноручную подпись гражданина и служащей дополнительным способом защиты содержащейся информации. Однако встал вопрос о хранении и получения такой ЭЦП, но для данной проблемы одним из решений оказалось использование индивидуальной идентификационной карты (ID-карты), с помощью которой пользователь может однажды лично голосовать без потери своих данный и защитив при этом свой голос.

2. Проблема обеспечения принципа тайного голосования. Для решения этой проблемы было предложено несколько вариантов решения. Например, не использовать поименный список избирателей, содержащий идентифицирующие личность данные, а заменить его списком, содержащим только номера действительных карточек для голосования. Другим решением стало использование серверов деперсонификации, которые стирают информацию, индивидуализирующую избирателя. Также широко применяется и технология «перемешивания» электронного ящика для голосования, т.е. электронные бюллетени считываются не по мере их поступления, а в произвольном порядке.

3. Проблема обеспечение принципа равного избирательного права. Эта проблема требует определенных технических предпосылок для голосования у самого избирателя. Например, мобильный телефон определенных технических характеристик или другое устройство с выходом в Интернет. Также должна существовать единая база данных о проголосовавших, которая обновляется в режиме реального времени и ПО, способное обрабатывать голоса пользователей.

4. Психологические барьеры и проблема необходимости проведения информационно-разъяснительной работы. Данная проблема вполне объяснима, так как вполне реальной представляется ситуация, когда вследствие либо неправильного использования самими избирателями технических устройств, либо ошибок разъяснительной работы будут иметь место нарушения избирательных прав, заблуждение граждан в вопросе своего волеизъявления, а в следствии этого недоверие и отверждение использования подобных систем. Таким образом следует подготовить грамотных специалистов, которые смогли бы провести информационно-разъяснительные работы среди различных слоев населения и уже через несколько лет количество пользователей систем дистанционного голосования начнет увеличиваться в арифметической прогрессии.

5. Проблема наблюдения и контроля за процессом голосования. При использовании систем дистанционного электронного голосования невозможно на данный момент обеспечить полное наблюдение и контроль за непосредственным процессом подачи и подсчета голосов. Однако есть возможность осуществить «индивидуальный» контроль при помощи своей индивидуальной идентификационной карты (ID-карты).

6. Проблема бесперебойной технической работы самой системы. Данная проблема обозначает две самые уязвимые точки, это центры голосования (предоставление, хранение, подсчет голосов) и конечные устройства, с которых пользователь голосует, выбирая одну из систем голосования. Для ее решения на уровне центров будет достаточным установление оборудования бесперебойного питания или независимыми генераторами электричества.

7. Проблема обеспечения безопасности электронных систем голосования. Данные проблема предопределяет необходимость международной сертификации систем электронного голосования, а также введения положения об обязательном проведении предварительного аудита такого оборудования.

В итоге оказалось, что не все проблемы нашли свое практическое решение, некоторые из них отразились в рекомендация

Литература

[1] Электронное голосование прогнозы [Электронный ресурс]. // ACE [сайт]. URL: http://aceproject.org/ace-ru/focus/e-voting/countries (дата обращения: 15.10.2014).

[2] С.А. Бажуков Дистанционное электронное голосование как альтернативная форма голосования на выборах // "Вестник избирательной комиссии архангельской области". 2011. №1. с.3-16

[3] Бюллетень Бисмарка как метод электронных выборов [Электронный ресурс]. // Идеи электронного правительства для Беларуси [сайт]. URL: http://e-gov.by/themes/egov-obzor/byulleten-bismarka-kak-metod-elektronnyx-vyborov (дата обращения: 15.10.2014).

[4] Ben Adida Advances in Cryptographic Voting Systems [Электронный ресурс] // MASSACHUSETTS INSTITUTE OF TECHNOLOGY [сайт]. URL: groups.csail.mit.edu/cis/theses/adida-phd.pdf (дата обращения: 15.10.2014).

[5] Выборы: сделаем это по-честному [Электронный ресурс] // 3DNews Daily Digital Digest [сайт]. URL: http://www.3dnews.ru/624551/ (дата обращения: 15.10.2014).

[6] НИК Эстонии. Обзор системы электронного голосования [Электронный ресурс]. // Механизм народовластия [сайт]. URL: http://mexnap.info/articles.php?article_id=291 (дата обращения: 15.10.2014).

Electronic Vote: Methods, Risks and Problems

O.Y. Peskova, S.V. Fateeva

In article possible risks and problems of systems of electronic vote, and first of all - remote, are considered. Risk analysis of remote electronic vote is carried out, their classification is presented, various groups of risks are in detail described. The article discusses the existing methods and systems of implementing electronic voting: electronic bulletin by Bismarck, Scantegrity, an electronic voting system in Estonia. The general classification of similar systems is presented, experience of their use in the different countries is described It describes the problems related to the organization of electronic voting, and the existing solutions. The ways of development of existing systems