ЭССЕ

“Электронное голосование”

Клюжев А.
группа 917.

Голосование, несомненно, является неотъемлемым атрибутом нашей жизни. С выборами мы встречаемся постоянно, начиная от голосования на каком-нибудь сайте с анекдотами или за любимую песню на концерте и заканчивая таким серьёзным делом, как выборы депутатов в государственную думу или выбора президента. До недавнего времени выборы депутатов или президента проводились привычным для народа методом – изъявлением своей воли голосованием на избирательном участке, посредством заполнения бумажного бюллетеня. А вот с голосованием на сайте встречались не многие. Это уже непросто голосование, а одна из разновидностей т.н. **электронного голосования**. Теперь, в связи с бурным развитием сетевых технологий, стало возможным задуматься о реализации подобных выборов в глобальном масштабе. Но голосовать в Internet за анекдоты и за президента – две огромные разницы – требования к безопасности и защите информации во втором случае значительно больше, чем в первом. При этом далеко не все люди смогут голосовать через Internet, поэтому реализация подобного проекта является делом чрезвычайно сложным и дорогим, как в физическом плане, так и с точки зрения защиты информации. Подходя серьёзно к решению проблемы выборов посредством электронного голосования, оказывается, что для полноценного проведения выборов требуется грамотно локализировать местоположения систем голосования, осуществить между ними связь, отвечающую требованиям безопасности, как информации, так и, естественно, людей. По типам локализации принято разделять системы голосования на три типа:

(1) расположенные на избирательных участках;

(2) расположенные в некоторых специальных местах – киосках;
(представляет собой некоторое подобие банкомата)

(3) расположенные в местах удалённого доступа, примерами которых являются обычные телефоны.

В том или ином случае голосование происходит посредством т.н. “машин для голосования”, а результаты обрабатываются специальными “машинами для подсчёта результатов”.

Что же представляют собой системы голосования? *(примечание: информация о видах голосования взята в Интернете по ссылке* **[01]**) В зависимости от места установки системы голосования, она представляет собой определённый программно-аппаратный комплекс, предназначенный для проведения, контроля, подсчета, сохранения и передачи по сети или вывода на печать или устройства отображения информации сведений о процессе голосования или его итогах. Алгоритм работы комплекса и построение применяемых технологий определяется специальным регламентом проведения мероприятий на объекте, т.е. в месте установки системы. Оборудование и программное обеспечение к нему изготавливается, дорабатывается и поставляется, как в виде отдельной системы, так и интегрированной в состав конференц - системы объекта, например такого, как государственная дума. Состав и функциональные возможности системы определяются техническим заданием заказчика и базируются на универсальных модулях и базовом программном обеспечении.

Огромное значение имеют виды голосования. Система голосования должна обеспечивать проведение **Количественного, Открытого, Закрытого, Поименного, Рейтингового и Альтернативного** голосования в соответствии с регламентом. Существует мнение, что эти устоявшиеся в практике голосования определения видов голосования не совсем корректны. Так, например: имеются Альтернативное и Тайное (Закрытое) виды голосования. Но разве Альтернативное голосование само по себе не может быть Открытым, Тайным или Поименным?

Чтобы разобраться в этом для начала надо выделить характерные черты этих терминов.

Поименное — такое голосование, при котором в протоколе голосования кроме итоговых результатов голосования приводятся поименные списки индивидуальных результатов голосования присутствующих делегатов.

Тайное — такое голосование, при котором информация о привязке качества волеизъявления к фамилии депутата отсутствует.

Открытое голосование. С этим понятием имеются наибольшие сложности. Чтобы было легче выделить отличительные черты этого вида голосования, обратимся к истории, ко временам, когда голосовали поднятием руки. В этом случае присутствующим в зале было видно как голосуют другие участники совещания, а в протокол заносились только итоговые результаты голосования. Так вот именно эти признаки наличия информации об индивидуальных волеизъявлениях для присутствующих и наличие в протоколе только итоговых результатов голосования являются отличительными чертами данного вида голосования, т.е. при голосовании с мест нужно выводить на групповой монитор не только итоги голосования, но и поименные итоги голосования, не занося их в протокол. К особенностям открытого электронного голосования необходимо также отнести меньший конформизм, т.к. результаты голосования становятся доступными присутствующим после окончания процедуры голосования, а не в ее процессе. Из приведенных отличительных признаков данных видов голосования нетрудно увидеть, что они никак не зависят от процедур голосования, а лишь определяют доступность к информации об индивидуальных волеизъявлениях депутатов. Таким образом, все наиболее часто применяемые виды голосования можно классифицировать по следующим основным признакам:

(1) по доступности информации о индивидуальных волеизъявлениях депутатов голосования подразделяются на **Поименное, Открытое, Тайное (Закрытое)**;

(2) по количеству выбираемых вопросов решения голосования подразделяются на **Одновариантные и Многовариантные**.

К одновариантному виду голосования относится:

Количественное голосование, при котором депутаты могут выбирать "За", "Против" или "Воздержался" по отношению к варианту предложенного решения.

К видам голосования с многовариантным выбором относятся:

Альтернативное голосование, когда депутат может отдать голос только за один из предъявленных вариантов голосуемого вопроса. Подсчет голосов и предъявление результатов голосования производится одновременно по всем вариантам вопроса, поставленного на голосование;

Рейтинговое голосование – ряд последовательных количественных голосований, в которых может принять участие каждый депутат. Результат предъявляется по окончании голосования по всем вариантам вопроса.

Рассмотренные признаки классификации являются независимыми, – мы имеем матрицу 3 x 3 возможных видов голосования и, следовательно, возможно прийти к идентичности понятий данного вопроса у исполнителя работ и заказчика и определить какие виды голосования необходимо реализовать при создании систем голосования.

	Поименное	Открытое	Тайное
Количественное	+	+	+
Альтернативное	x	x	+
Рейтинговое	x	x	+

Таким образом, выводы приведены в таблице, где знаком "+" помечены те виды голосования, которые должны быть реализованы в системах голосования, знаком "x" помечены те виды голосования, которые реально не требуются для систем голосования.

Возвращаясь к выбору президента, мы видим, что разрешение вопроса электронного голосования здесь реализуется с некоторыми трудностями. Голосуя за президента посредством бумажного бюллетеня, голосование является Тайным Альтернативным. Голосуя за президента электронным образом, система должна знать, что голосуете именно вы, и голосуете в первый раз. Ваша идентификация, собственно, психологически и ставит под сомнение смысл слова Тайный. Огромные проблемы возникают также с предварительной регистрацией избирателей, и созданием самих мест электронного голосования, в зависимости от их типа локализации.

Напомним типы локализации мест установки системы голосования:

(1) расположенные на избирательных участках;
(2) расположенные в некоторых специальных местах – киосках;
(представляет собой некоторое подобие банкомата)
(3) расположенные в местах удалённого доступа, примерами которых являются обычные телефоны.

Проведём небольшой сравнительный анализ некоторых свойств для этих трёх типов.

Расположение избирательных мест относительно избирателей:

(1) удобно;
(2) более удобно;
(3) самое удобное;

Цена на установку места и подведение сети:

(1) большая (~25.000 $ за 1 систему);
(2) самая большая (? – подобные системы только разрабатываются);
(3) самая маленькая (…Internet…☺);

Цена на обслуживание:

(физическая охрана, охрана соблюдения закона о голосовании, один из пунктов которого запрещает агитацию во время выборов, и т.п.)

(1) большая;

(2) самая большая;

(3) самая маленькая;

Возможность функционирования без дополнительного оператора.

(1) пока отсутствует;

(опыты, проведённые в США **[02][03]**, показали, что независимо от надёжности системы и регистрации (требовалось предварительное посещение мест регистрации и получение специальной карты) машины для голосования давали достаточно частые сбои)

(2) пока отсутствует;

(3) существует;

Надёжность защиты информации:

(1) самая высокая

(разрабатываются более дешёвые системы идентификации посредством сканирования сетчатки глаза и отпечатков пальцев);

(2) высокая;

(3) наименьшая;

(огромное количество вирусов, специальных маскирующихся программ, большие возможности для хакеров);

Преимущества перед системой голосования бюллетенями:

Все системы: - получение результатов в реальном времени;

- физическое удобство.

Таким образом, на первый взгляд кажется, что самым удобным для избирателя является всё-таки голосование посредством сети Интернет. Но помимо того, что этот способ является самым незащищённым в процессе голосования, неясен также на первый взгляд и процесс регистрации участников голосования. Посмотрим, что же всё-таки возможно предпринять, чтобы создать компромисс между защищённостью и удобством, где удобство подразумевает в себе не только физический аспект, но и включает в себя также определённую степень доверия избирателей к системе голосования через Интернет. *(примечание: далее некоторый материал базируется на частичном переводе статей расположенных по Интернет-адресам указанных в ссылках к* **[13]** *и* **[14]**) Рассмотрим ключевые проблемы, которые нужно решить при реализации выборов через Интернет:

(1) Неудобство голосования.

(2) Трудный доступ для избирателей-инвалидов.

(3) Избиратели, находящиеся за границей, часто не получают избирательные бюллетени или получают избирательные бюллетени слишком поздно, чтобы проголосовать.

(4) Жёсткие рамки голосования по времени и местоположении.

(5) Регистрация может быть запутанная, и обновление регистрационной информации может занимать много времени.

(6) Информация о выборах и кандидатах может быть труднодоступна.

Возникает главный вопрос: повысит ли явку избирателей решение всех этих проблем? Иначе, проведение выборов через Интернет окажется бессмысленным, несмотря на кажущееся удобство.

Далее возникают технологические проблемы и проблемы безопасности информации. Несмотря на то, что следует разработать системы защиты от атак хакеров, нужно решить ряд не менее важных проблем безопасности информации. Должны быть изобретены методы, обеспечивающие в полной мере секретность, поддающуюся проверке, и что наиболее важно при этом, избиратель должен доверять системе. Следующее препятствие – точность системы голосования при сборе и подсчёте голосов. Наконец, есть проблема идентификации и проверки избирателя. Должны быть развиты системы, гарантирующие, что именно тот избиратель голосует, и что он голосует именно один раз. Какие же методы защиты возможно применить в голосовании через Интернет.

(1) Личный номер идентификации (PIN-код) или пароль.

Это основной механизм, который должен использоваться, чтобы гарантировать уникальность избирательного бюллетеня избирателя. Должны быть приняты меры защиты пароля от различных атак. Однако системы паролей часто компрометируются. Кроме того, нет никакой гарантии, что избиратели не будут использовать свои пароли совместно с другими людьми. И всё-таки, носителем уникальной информации может служить компьютерный чип или CD-ROM выданный избирателю на этапе регистрации. Но это в некотором смысле неудобно, так как требует явки избирателя на участок регистрации заранее, но в срок, значительно превышающий время самих выборов. Но и здесь могут возникнуть трудности. Что если устройство сломано или утеряно !!!

(2) Кодирование.

Эта технология должна использоваться, чтобы защитить цифровые избирательные бюллетени и пароли, поскольку они путешествуют через Интернет. Криптографические протоколы также должны использоваться, чтобы сохранить тайну избирательного бюллетеня и предотвратить некоторые типы мошенничества. Однако, такие системы все еще могут быть уязвимы к атакам и должны быть тщательно исследованы перед использованием в общественных выборах.

(3) Цифровая подпись.

Системы цифровой подписи могут использоваться, чтобы подтвердить подлинность документов и проверить, что документ был подписан в цифровой форме , используя специфический ключ. Избирательные власти могут подписывать цифровые формы избирательного бюллетеня так, чтобы избиратели знали, что они получили подлинный избирательный бюллетень. Избиратель может подписывать цифровой "конверт избирательного бюллетеня" так, чтобы избирательные власти знали, что зарегистрированный избиратель “бросает” избирательный бюллетень. Однако, важно то, что цифровые ключи, должны быть определённым образом защищены, чтобы предотвратить мошенничество. Это наводит на мысль о том, что технология цифровой подписи является ключом к обеспечению процесса голосования через Интернет. Цифровые подписи обеспечивают лучший уровень защиты в электронных сделках. Хоть они и не недороги, а вопросы финансирования важны. Если бы правительство обеспечило цифровую подпись для всех избирателей, стоимость была бы очень высока. Также существуют несколько "классов” или уровней защиты цифровых подписей. Некоторые цифровые подписи получаются без того, чтобы требовать любую личную идентификацию, в то время как другие требуют высоких уровней идентификации, включая личные интервью.

(4) Смарт-карты:

Смарт-карта – кредитная карточка, содержащая маленький компьютерный чип. Такие карты могли бы быть отправлены избирателям с предопределёнными заранее избирательными бюллетенями, также как и ключами кодирования. Здесь, помимо потенциальных проблем защиты с картами непосредственно, имеет место проблема обычного почтового воровства.

(5) Биометрические идентификаторы.

Распознавание Голоса, распознавание отпечатка пальца, и подобные биометрические методы могли бы использоваться, чтобы удостовериться в том, что только зарегистрированные избиратели голосуют. Избиратели не были бы способны дать свои пароли другим людям, а также такие методы принесут дополнительную защиту сетевой системы голосования. Однако, использование этих методов может поднимать проблемы секретности.

Но всё-таки весьма удобно, когда *(примечание: далее некоторый материал базируется на частичном переводе статьи расположенной по Интернет-адресу указанному в ссылке* к **[04]**), несколькими щелчками мыши, мы можем подать неофициальный голос за какого-нибудь депутата, выразить своё мнение относительно разнообразия важных и не очень важных проблем, проголосовать за свои любимые сайты, и делать свои оценки относительно кино или музыки и т.д. и т.п. Эти опросы забавны, и многие даже полезны, но всё-таки немногие поддерживают уровни защиты и секретности, которая требуется, чтобы производить, например, правительственные выборы в многих демократических странах. Одновременно достижение защиты и

секретности в электронных опросах - проблема, которая должна быть решена, если Internet должен будет использоваться для серьезных крупномасштабных обзоров и выборов. Поскольку всё большее количество людей обращается к Internet, электронное голосование, вероятно, станет все более и более обращением к географически распределенным организациям, которые в настоящее время проводят выборы посредством бюллетеней. Электронные выборы имеют потенциал, будучи более дешевым и требующими меньшее количество времени, чем выборы бюллетенями. В конечном счёте, электронное голосование стимулирует решение участия избирателя в правительственных выборах. Однако, если нет тщательно разработанной электронной системы голосования, то избиратели могут быть легко компрометированы, таким образом нарушаются результаты или секретность избирателей. Каковы же действительно хорошие характеристики системы электронного голосования.

При проектировании электронной системы опроса, необходимо рассмотреть пути, которыми задачи голосования могут быть выполнены с помощью электроники без того, чтобы жертвовать секретностью избирателя или предоставлять возможности для мошенничества. Чтобы определять, исполняет ли система эти задачи хорошо, полезно развить набор критериев для оценки работы. Далее - набор тех желательных характеристик для электронных систем опроса, которые включают характеристики большинства систем, описанных в электронной литературе по голосованию.

Точность.

Система точна, если:

(1) не существует возможности изменить голос;

(2) не существует возможности устранить утвержденный голос из заключительного числа поданных голосов;

(3) не существует возможности включить недопустимый голос в заключительное число поданных голосов.

В наиболее точных системах заключительное число голосов должно быть абсолютно точным или потому, что никакие погрешности не могут быть внедрены или потому, что все внедрённые погрешности могут быть обнаружены и исправлены. Частично точные системы могут обнаруживать, соответствующие погрешности, но не всегда.

Демократия.

Система является демократической, если:

(1) она позволяет голосовать только избирателям, имеющим право голоса;

(2) она гарантирует, что каждый, имеющий право голоса избиратель, может голосовать только один раз.

Секретность.

Система конфиденциальна, если:

(1) ни избирательные власти, ни кто-либо еще не могут увязать какой-либо избирательный бюллетень с тем самым избирателем, который его бросил (Тайное голосование);
(2) никакой избиратель не может доказывать, что он или она голосовали специфическим способом.

Второй фактор секретности важен для предотвращения скупки голоса и вымогательства. Избиратели могут продавать свои голоса, только если они способны доказать покупателю, что они фактически голосовали согласно его пожеланиям . В то время как некоторые могут доказывать, что в демократическом и капиталистическом обществе нет ничего плохого в том, чтобы добровольно продавать свои голоса, большинство людей, вероятно, согласилось бы, что люди никогда не должны так делать.

Проверяемость.
Система считается поддающаяся проверке, если любой может независимо проверить то, что все голоса были подсчитаны правильно. Более слабое определение проверяемости, используемое некоторыми авторами, говорит о том, что система, поддающаяся проверке это та система, которая позволяет избирателям проверять их собственные голоса и исправить любые ошибки, которые они могли бы найти без нанесения ущерба секретности. Системы, менее поддающиеся проверке, могли бы позволить выявлять ошибки, но не исправлять их, или могли бы позволить проверку процесса сторонним представителям, но не индивидуальными избирателями. Традиционные системы голосования вообще учитывают только минимальную проверку сторонними представителями стороны.

Удобство.
Система считается удобной, если она позволяет избирателям выносить свои голоса быстро, в одном сеансе, и с минимальным оборудованием или специальными навыками.

Гибкость.
Система считается гибкой, если она допускает разнообразные форматы вопроса избирательного бюллетеня, включая открытые законченные вопросы. Гибкость также важна для кандидатов дополнительно внесённых в список и для некоторых исследовательских вопросов. Некоторые криптографические протоколы голосования являются жёсткими, так как они допускают только “однобитовое” голосование, т.е. голосование типа да/нет.

Подвижность.
Система считается подвижной, если нет никаких ограничений в местоположении, из которого избиратель может подавать голос. Одна из причин, заинтересовывающая людей – это причина передвижных электронных систем голосования.

Участие избирателей могло бы увеличиваться, если бы люди могли легко подавать свои голоса с компьютеров в своих домах, офисах, школах, библиотеках и т.д. Конечно, для правительственных выборов необходимо было бы сохранить централизованные места голосования для людей, которые не будут иметь доступа к компьютерам по-другому. Свойство самой подвижности - главный вкладчик в некоторые из проблем, связанные с проектированием безопасной и конфиденциальной электронной системы голосования. Позволяя избирателям подавать свои голоса фактически в любом месте, происходит так, что расширяется множество людей, участие в голосовании которых было бы нежелательно.

Рассмотрим теперь основные протоколы, используемые в системах электронного голосования. “Основные протоколы” означает факт того, что системы электронного голосования и протоколы до сих пор разрабатываются, и их определённые типы могут быть применены в зависимости от требований регламента выборов, направленных на обеспечение определённого уровня технической поддержки и систем информационной безопасности. Итак:

Простой протокол

Простой протокол голосования функционирует так, что для того, чтобы выполнить вышеупомянутые требования не требуется использовать какие-либо криптографические методы. Такой протокол требует, чтобы избиратель предъявил на рассмотрение электронному валидатору электронный избирательный бюллетень с приложенным номером идентификации избирателя. (Валидатор – некий электронный прибор, проверяющий действительность чего-либо, а номер выдаётся избирательной коммисией во время регистрации, которая проводится за некоторое время до выборов). Валидатор использует номер идентификации, чтобы проверить избирателя в списке зарегистрированных избирателей. Далее валидатор снимает номер идентификации и посылать избирательный бюллетень электронному счётчику. Он производит соответствующую запись результата голосования и добавляет их к общему числу.

Хотя этот простой протокол гибок, передвижной, и удобен, но имеет несколько серьёзных проблем. Во-первых, избиратели могли наполнить “урну” для избирательных бюллетеней, используя номера идентификации других избирателей. Во-вторых, хотя валидатор программа, как предполагается, не читает или делает запись содержания избирательного бюллетеня, избиратели действительно не могут убедиться в том, что валидатор – программа, которая не нарушает таким образом их секретность. В-третьих, нет никакого способа гарантировать, что валидатор не изменяет избирательные бюллетени перед посылкой их к счётчику или воспроизводит избирательные бюллетени, которые фактически никогда не были представлены избирателями. В-четвертых, нет никакого способа гарантировать, что счётчик точно делает запись голосования.

Мы можем решить проблему избирателей, наполняющих урну для избирательных бюллетеней, требуя избирателей подписать их избирательные бюллетени цифровыми подписями. Здесь возможно использование программы типа PGP. Таким образом, если

секретный ключ избирателя не был компрометирован, то мы можем быть уверены в том, что избиратели не используют другие номера идентификации. Кроме того, мы можем предотвратить валидатор от нарушения секретности избирателей при наличии избирателей, которые зашифруют свои избирательные бюллетени ключом счётчика. Таким образом, валидатор не будет способен читать или изменять избирательные бюллетени. Однако, если валидатор и счётчик объединятся, и валидатор получит секретный ключ счётчика, то секретность может быть компрометирована. Таким образом, мы нуждаемся в более сложном подходе к включению криптографических методов в такую электронную систему голосования.

Протоколы одного и двух агенств.

Нурми, Салома и Сантин **[05] [06]**, являясь одними из разработчиков протоколов электронного голосования, предложили подход, который решает многие из проблем, упомянутых выше. В этом протоколе электронный валидатор раздаёт уникальный секретный признак идентификации каждому избирателю, только до процедуры выбора . Далее валидатор посылает счётчику список всех уникальных признаков идентификации, без отчета о соответствующих ему избирателях. Каждый избиратель посылает счётчику свой уникальный признак идентификации и зашифрованный файл, содержащий копию уникального признака и утвержденный выбором избирательный бюллетень. В этот момент счётчик может удостовериться, что уникальный признак идентификации действителен, но зашифрованный файл не может быть исследован на содержание избирательного бюллетеня. Счётчик издает зашифрованный файл (так, чтобы избиратель имел доказательство того, что файл был представлен на рассмотрение вовремя), и избиратель отвечает, посылая счётчику ключ, необходимый для дешифрования файла. Когда выборы закончены, счётчик издает список всех избирательных бюллетеней участвовавших в голосовании и соответствующие зашифрованные файлы. Здесь избиратели могут подтвердить, что их голоса были посчитаны правильно. Любой избиратель, который находит ошибку, может возразить, предоставляя зашифрованный файл и ключ дешифрования снова. Поскольку зашифрованный файл был издан ранее, счётчик не может отрицать факт того, что он его не получал.

Протокол двух агентств, поддающийся проверке индивидуальными избирателями (в отличие от простого протокола), однако, это все еще имеет несколько проблем. Наиболее важно что, он не защищает секретность избирателей, если счётчик и валидатор объединятся в “тайном сговоре”. Таким образом, если эти два агентства собираются работать вместе, то это могло бы также быть, как одно агентство.

Протокол одного агентства идентичен протоколу двух агентств, если бы не процедура распределения признака. В протоколе одного агентства, признаки распределены счётчиком (нет валидатора) используя систему ANDOS (All-or-Nothing Disclosure Of Secrets – бескомпромиссное раскрытие тайн) (*примечание: см. разделы* **4.13, 23.9** *в* **[11]**) – протокол для реализации тайны тайн. Это решает проблему сговора; однако,

ANDOS – протокол – весьма сложный в вычислительном отношении комплекс и хорошо не масштабируется.

Протокол Нурми, Салома и Сантина не будет в состоянии удовлетворять второй части требования секретности и части требования точности, рассмотренных выше.

Протоколы слепой подписи.

Когда Дэвид Чаум **[07]** сначала представил концепцию слепых подписей в 1982 году, он предложил то, что слепые подписи могли бы использоваться для секретных выборов. Десятью годами позже, Фуджиока, Окамото, и Охта **[08]** развивали практическую схему голосования, которая использует слепые подписи, чтобы решить проблему сговора, свойственную протоколам подобным протоколу двух агентств без сильного увеличения полной сложности протокола.

Слепые подписи – это класс цифровых подписей, которые позволяют документу быть подписанными без того, чтобы показать его содержание. Эффект подобен размещению документа и листа копирки внутри конверта. Если кто-то подписывает внешнюю сторону конверта, он также подписывает документ во внутренней части конверта. Подпись остается приложенной к документу, даже когда он удален из конверта.

В протоколе Фуджиока, Окамото и Охта, избиратель подготавливает избирательный бюллетень со своим выбором, который он сделал, шифрует его секретным ключом, и маскирует его (*примечание: см. раздел* **5.3** *в* **[11]**). Далее избиратель подписывает избирательный бюллетень и посылает его валидатору. Валидатор проверяет, что подпись принадлежит зарегистрированному избирателю, который еще не голосовал. Если избирательный бюллетень действителен, валидатор подписывает избирательный бюллетень и возвращает его избирателю. Избиратель удаляет маскировку, раскрывая таким образом зашифрованный избирательный бюллетень, подписанный валидатором. Далее избиратель посылает в результате полученный подписанный, зашифрованный избирательный бюллетень счётчику. счётчик проверяет подпись на зашифрованном избирательном бюллетене. Если избирательный бюллетень действителен, счётчик размещает его в списке, который будет издан после всего голосования. После того, как список издан, избиратели проверяют, что их избирательные бюллетени находятся в списке и посылают счётчику ключи дешифрования, необходимые, чтобы открыть их избирательные бюллетени. Счётчик использует эти ключи для дешифрования избирательных бюллетеней и добавляет голос к общему числу. После выборов счётчик издает ключи дешифрования наряду с зашифрованными избирательными бюллетенями так, чтобы избиратели могли независимо проверить выбор.

Cranor и система Ситрона – Sensus **[09]**, основаны на схеме Фуджиока, Окамото, и Охта. Главное различие между этими схемами появляется после того, как избиратель представил зашифрованный избирательный бюллетень счётчику. В Sensus-протоколе, счётчик отвечает, посылая квитанцию избирателю. Избиратель может представить ключ дешифрования немедленно после получения этой квитанции, полностью завершая процесс голосования в одну сессию. Sensus-система использует программу-опросчик, которая исполняет все криптографические функции и функции “сделки” с программами

выбора при защите избирателя. Испытания, проводимые с выполнением опытного образца Sensus указывают, что полный процесс голосования может быть закончен в пределах нескольких минут.

Sensus-протокол - один из немногих электронных протоколов голосования, который фактически был осуществлен. Другая разновидность протокола Фуджиока, Окамото и Охта, была осуществлена Давенпортом, Ньюбергером и Вудордом **[10]** и использовалось, чтобы провести студенческие выборы.

Sensus-протокол обладает большинством желательных характеристик; однако, он также будет не в состоянии исправить некоторые проблемы, свойственные протоколам одного и двух агенств. Возможно наиболее важная проблема состоит в том, что администратор выбора (в этом случае валидатор) может подавать голоса за воздержавшихся избирателей. Эти недействительные голоса могут быть обнаружены непосредственно воздерживающимися избирателями или ревизором, который проверяет подписи по всем представленным запросам валидатора. Однако, нет никакого способа идентифицировать недействительные избирательные бюллетени и удалять их – если номера недействительных голосов обнаружены, выбор должен будет быть повторен. Если избиратели, которые желают воздержаться, представят чистые избирательные бюллетени, этой проблемы можно избежать.

Существуют ещё несколько простых и достаточно сложных (к примеру, голосование без избирательной комиссии) протоколов электронного голосования, описание которых можно найти в книге Брюса Шнайера “Прикладная криптография” в главе 6 - “Эзотерические протоколы”. (*примечание: см.* **[11]**).Теоретически они, конечно, очень привлекательны, но реализовать их на практике пока мешает либо недостаточная защищённость, либо сложность реализации, хотя компромисс – одна из методик крупномасштабных электронных выборов - существует (*примечание: см. ссылку 585 в* **[11]**).

Заключение.

Ни один из протоколов, обсужденных здесь, не удовлетворяет критерию верифицируемости полностью потому, что ни один из них не может быть проверен любой заинтересованной стороной. Те, кто позволяют избирателям проверять, что их собственные голоса были подсчитаны правильно, удовлетворяют критерию в значительной степени. Однако, система проверки, которая полагается на избирателей, берущих на себя какие-то действие после выборов, вряд ли может быть целиком реализована.

Важно, что безопасность и соображения секретности должны быть приняты во внимание при проектировании электронных систем голосования. В дополнение к обычным мерам безопасности, которые должны быть, система голосования, имеет уникальные черты, которые возникают в результате желания поддержать секретность избирателя. Хотя ни один из протоколов голосования, представленных здесь, не удовлетворяет всем

желаемым свойствам полностью, некоторые удовлетворяют им, достаточно хорошо, чтобы быть столь же хорошими или даже лучше, чем традиционные системы голосования, которые они вполне могут заменить.

Несмотря на то, что электронные правительственные выборы ещё далеко, профессиональные и социальные организации уже начали проводить обзоры и выборы с помощью электроники. В то время как большинство этих выборов в настоящее время игнорирует средства секретности в электронной почте и программном обеспечении браузеров, которое может легко соединять с криптографическим программным обеспечением, путь к безопасным и частным электронным выборам в ближайшем будущем уже открыт.

Библиография и ссылки:

[01] http://www.tarusa.ru/~pactp/gol/index.html

[02] **"Report of National Workshop of Internet Voting." March 2001.**
http://www.pirp.harvard.edu/pubs_pdf/green/green_Vot-spln.pdf

[03] Anthony T. Green
"Decisions About Voting Technologies: The Issues." June 2001.
http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf

[04] Cranor, L.
"**Electronic Voting. Computerized polls may save money, protect privacy." 1996.**
http://www.acm.org/crossroads/xrds2-4/voting.html

[05] Nurmi, H., Salomaa, A., and Santean, L.
"Secret ballot elections in computer networks." **1991.**
Computers and Security, 36, 10 (1991), pp. 553-560.

[06] Salomaa, A.
"Verifying and recasting secret ballots in computer networks." 1991.
New Results and New Trends in Computer Science,
Springer-Verlag, Berlin. 1991, pp. 283-289.

[07] Chaum, D.
"Blind signatures for untraceable payments." 1983.
Proceedings of Crypto 82,
Plenum Press, New York. 1983, pp. 199-203.

[08] Fujioka, A, Okamoto, T., and Ohta, K.
"A practical secret voting scheme for large scale elections." 1993.
Advances in Cryptology - AUSCRYPT '92,
Springer-Verlag, Berlin. 1993, pp. 244-251.

[09] Cranor, L.F. and Cytron, R.K.

“ Design and Implementation of
a Security-Conscious Electronic Polling System.” February 1996.
Washington University Computer Science Technical Report WUCS-96-02.

[10] Davenport, B., Newberger, A., and Woodard, J.
“Creating a secure digital voting protocol for campus elections.”
Unpublished paper. **1995.**
http://www.princeton.edu/~bpd/voting/

[11] Брюс Шнайер
“Прикладная криптография”
http://www.3ka.mipt.ru/vlib/books/Programming/ComputerScience/Applied_Cryptography/applied_cryptography.htm

[12] **Electronic Voting Bibliography**
http://theory.lcs.mit.edu/~cis/voting/greenstadt-voting-bibliography.html

[13] Patricia Tarabelsi
“Internet Voting: Security, Experimentation and Innovation”
http://www.reformamericainc.org/paper-edem.shtml

[14] Thomas Bryer
“Internet Voting: Security, Experimentation and Innovation”
October 11 and 12, 2000.
http://www.reformamericainc.org/paper-evoting.shtml

Литература по теории электронного голосования:

(1) **Tartu University**
Faculty of Mathematics and Informatics
Institute of Computer Science
Chair of Software Engineering
Oleg Murk ’2001
“Designing Electronic Voting”
Bachelor’s Thesis
http://www.cs.ut.ee/~olegm/

(2) **Tartu University**
Faculty of Mathematics
Institute of Computer Science
Chair of Theoretical Computer Science
Oleg Murk ’2001
“Electronic Voting Schemes”
Semester Work
http://www.cs.ut.ee/~olegm/

(3) Michael J. Radwin ’December, 1995
“**An untraceable, universally verifiable voting scheme”**
Seminar in Cryptology
Professor Phil Klein

http://www.radwin.org/michael/projects/voting.html

(4) Bruce Sneier **“Applied Cryptography”**
(Брюс Шнайер **“Прикладная криптография”**)
(*примечание:*см.**[11]**