Научная статья
УДК__004.057.4
DOI: 10.17072/1993-0550-2022-4-61-67

Построение модели протокола электронного голосования с возможностью проверки результата избирателями

Эмма Александровна Нехорошева[1], Александр Петрович Шкарапута[2]
[1, 2]Пермский государственный национальный исследовательский университет, Пермь, Россия
[1]emmanekhorosheva@vk.com
[2]shkaraputa@psu.ru, https://orcid.org/ 0000-0002-0593-6663

Аннотация. В данной статье предложена модель протокола электронного голосования, с возможностью мониторинга результата со стороны избирателей. Центральной идеей такой модели является появление механизма связи электронных бюллетеней с результатами голосования в единую цепь, с помощью криптографических преобразований, на базе криптографических систем с открытым ключом. Такой механизм не допускает появления "лишних" бюллетеней, позволяет отслеживать результат своего голоса конкретным избирателем в этой цепи и приводит к невозможности произвести неправильный подсчет голосов, без нарушения целостности цепи. Рассмотрено три протокола электронного голосования: Фудзиока–Окамото–Охта, протокол с одной центральной комиссией на базе протокола ANDOS, протокол с одной центральной комиссией на базе слепой подписи. Протоколы были исследованы на предмет достоинств и недостатков, а также на возможность модификации с целью добавления новых функций. Выбран оптимальный протокол для включения в него механизма связи голосов в единую цепь. В результате разработана новая система электронного голосования на основе протокола с Центральной избирательной комиссией на базе слепой подписи. Приведена схема, объясняющая работу этой системы.

Ключевые слова: *электронное голосование; голосование; протокол; цепь; Фудзиока–Окамото–Охта; ANDOS; центральная избирательная комиссия*

Для цитирования: *Нехорошева Э. А., Шкарапута А. П.* Построение модели протокола электронного голосования с возможностью проверки результата избирателями // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 61–67. DOI: 10.17072/1993-0550-2022-4-61-67.

Статья поступила в редакцию 10.10.2022; одобрена после рецензирования 10.11.2022; принята к публикации 11.11.2022.

Research article

Building a Model of Electronic Voting Protocol With the Possibility of Verification of the Result by Voters

Emma A. Nekhorosheva[1], Alexander P. Shkaraputa[2]
[1, 2]Perm State University, Perm, Russia
[1]emmanekhorosheva@vk.com
[2]shkaraputa@psu.ru, https://orcid.org/0000-0002-0593-6663

Abstract. This article proposes a model of electronic voting protocol, with the possibility of monitoring the result by the voters. The central idea of such a model is the emergence of a mechanism for linking electronic ballots with the results of voting in a single chain, with the help of cryptographic transformations, based on cryptographic systems with a public key. Such a mechanism prevents "superfluous" ballots from appearing, makes it possible to track the result of one's vote by a particular voter in this chain, and makes it impossible to make an incorrect vote count, without violating the integrity of the chain. Three electronic voting protocols were examined: the Fujioka–Okamoto–Ohta protocol, the protocol with one central commission based on the ANDOS protocol, and the protocol with one central commission based on the blind signature. The protocols were investigated for merits and demerits, as well as for the possibility of modification to add new features. The optimal protocol was selected to include a mechanism for linking votes into a single chain. As a result, a new electronic voting system based on a protocol with the Central Election Commission based on a blind signature was developed. A scheme explaining the operation of this system is given.

Keywords: *electronic voting; voting; protocol; chain; Fujioka–Okamoto–Ohta; ANDOS; central election commission*

For citation: *Nekhorosheva E. A., Shkaraputa A.P.* Building a Model of Electronic Voting Protocol With the Possibility of Verification of the Result by Voters // Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2022;4(59):61–67. (In Russ.). DOI: 10.17072/1993-0550-2022-4-61-67.

The article was submitted 10.10.2022; approved after reviewing 10.11.2022; accepted for publication 11.11.2022.

Введение

Электронное голосование – термин, определяющий различные виды голосования, охватывающий как электронные средства голосования (электронная демократия), так и электронные средства подсчета голосов. Разновидностью электронного голосования являются интернет-выборы [1].

На протяжении всей истории человечества голосование и выборы имели важную роль в развитии общества. В далеком прошлом первобытные люди выбирали правителей, используя бобы разных цветов, но сейчас, в современном обществе с массой новых и развивающихся технологий, голосование должно становиться все более надежным, защищенным от постороннего вмешательства, удобным и честным. Однако на данный момент опыт использования электронного голосования имели только 14 стран на муниципальном уровне, и только 11 на национальном [2].

Остальные страны используют высокотехнологичные, дорогостоящие, утвержденные документально, но все те же "бобы": огромная часть работы на разных этапах выполняется людьми, требуется много времени на проведение голосования и подсчет голосов, существует огромное количество возможностей изменить, удалить или вовсе добавить нужные злоумышленнику голоса. Системы голосования и выборов до сих пор принадлежит тем, кому это выгодно.

Несмотря на это, технологии все же развиваются и появляются новые современные способы решения проблемы, например, использование интернет-выборов. Однако использование технологий более высокого уровня требует тщательного подхода к защите информации. Если при бумажном голосовании между избирателем и его выбором стоит только бланк и урна, то при дистанционном голосовании нужно преодолеть подключение к ресурсу, регистрацию, аутентификацию, минуя все программные и аппаратные угрозы несанкционированного доступа, и только тогда добраться до заветного бюллетеня. Но это еще не все: бюллетень не должен быть изменен или удален на пути к системе подсчета голосов, а раз эта система еще дальше от избирателя, значит угроз еще больше.

На данный момент есть несколько протоколов электронного голосования, которые близки к идеалу, но у всех есть большой минус – отсутствие возможности просмотра списка проголосовавших и не проголосовавших. Без этого невозможно определить, как идет голосование, доказать его честность. Избиратель оказывается как бы в "информационном вакууме", ему остается только доверять или не доверять системе.

Целью данной статьи была разработка механизма улучшения существующих протоколов и повышение уровня контроля процесса голосования со стороны голосующих.

Для пояснения работы этого механизма можно рассмотреть простейший пример – как даже традиционный метод голосования можно было бы модернизировать, используя механизм связи между предметами для голосования (в том числе бюллетенями).

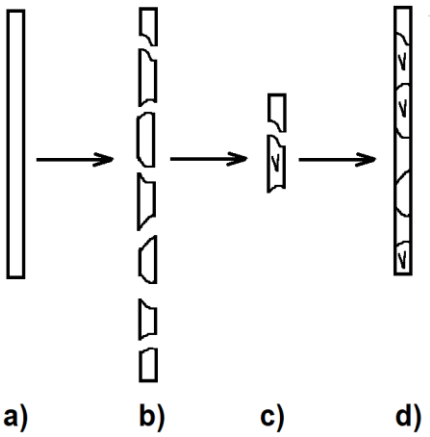

Рис. 1. *Демонстрация работы механизма связи предметов для голосования в единую цепь на примере традиционного голосования*

Предположим, что у нас имеется некий целостный предмет (например, деревянная палка, рис. 1a) и мы хотим его использовать в голосовании, как это раньше делалось с черепками или теми же бобами. Далее приведем "протокол" улучшенного традиционного голосования:

1. Разобьем предмет на несколько частей, так, чтобы каждая часть была уникальной рис. 1b).
2. Раздадим части голосующим, так, чтобы никто не знал, какая часть кому достанется (этот вопрос решается обычным перемешиванием и вытягиванием вслепую).
3. После получения своей части, голосующий ставит на ней необходимый знак рис. 1c).
4. Соберем части с сохранением анонимности, после чего восстановим исходный предмет.

Из приведенного примера очевидно, что в данном случае невозможно добавить другие части, не относящиеся к предмету (палке). Каждый голосующий может проверить результат, осмотрев итоговую цепь. В случае попытки исключить какой-то голос, цепь рассыпается. Все это ведет к тому, что применение механизма "связи" существенно уменьшает махинации, как при самом голосовании, так и при подсчете голосов.

Современные возможности позволяют применить этот механизм и в электронном голосовании.

1. Электронное голосование

По словам Брюса Шнайера [3, с. 103], одного из крупнейших экспертов в области информационной безопасности, идеальный протокол электронного голосования должен обладать следующими критериями:

1. Голосовать могут только те, кто имеет право.
2. При подсчете результатов голосования для каждого избирателя учитывается не более одного голоса.
3. Никто не может узнать, за кого проголосовал конкретный избиратель (т.е. должна обеспечиваться анонимность голосования).
4. Никто не может проголосовать за другого.
5. Никто не может тайно изменить чей-то голос.
6. Избиратель может проверить, что его голос учтен при подведении итогов голосования.
7. Каждый знает кто голосовал, а кто нет.

Желательны также два дополнительных свойства:

8. Избиратель может изменить свое мнение (т.е. аннулировать свой бюллетень и проголосовать заново) в течение заданного периода времени.
9. Если избиратель обнаруживает, что его голос засчитан неправильно, он может подать протест.

В данной работе были рассмотрены три протокола голосования:

1. Протоколы двух агентств Фудзиока–Окамото–Охта.
2. Протокол голосования с одной Центральной комиссией на базе протокола ANDOS.
3. Протокол голосования с одной Центральной комиссией на базе "слепой" подписи.

Необходимо отметить, что во всех существующих как электронных, так и бумажных протоколах голосования есть уязвимость – возможность покупки голосов. Поскольку исправить это нельзя, этот факт будет игнорироваться.

2. Обоснования выбора базового протокола

Для того чтобы реализовать возможность просмотра списка голосовавших, нужно создать условия, при которых избиратель сможет удостовериться в правильности и неподдельности предоставленных данных. Для этого был предложен механизм связи голосов, чтобы каждый последующих голос зависел от предыдущего. В таком случае любой избиратель в любой точке «цепи» сможет проследить наследование значений от самого первого звена до собственного голоса и последующих звеньев.

В ходе рассмотрения протоколов для предложенной модификации и их анализа были сделаны следующие выводы:

1. Протокол голосования с одной Центральной комиссией на базе протокола ANDOS имеет серьезные недостатки: проблемы с масштабируемостью и возможность использования голосов зарегистрировавшихся, но еще не проголосовавших людей.

2. Протокол голосования с одной Центральной комиссией на базе "слепой" подписи имеет оптимальное количество участников и почти все критерии идеального протокола голосования.

3. Протокол двух агентств Фудзиока–Окамото–Охта самодостаточен, защищен от несанкционированного доступа, однако подразумевается, что будет добавлена еще одна сторона – "Цепь", а протокол сам по себе уже имеет три стороны. В данном контексте можно считать данный протокол перегруженным и неподходящим для преобразования.

Протокол голосования с одной Центральной комиссией на базе "слепой" подписи и протоколы двух агентств Фудзиока–Окамото–Охта похожи по характеристикам, однако протокол голосования с одной центральной комиссией имеет меньше участников информационного обмена, что позволяет добавить еще одного и не слишком сильно усложнить систему и общение между сторонами при этом. Новый протокол будет строиться на базе именно этого протокола.

3. Объяснение логики работы системы

Используемые в протоколах обозначения:

ЦИК – центральная избирательная комиссия;

ЦСК – центр сертификации ключей;

B – бюллетень;

ID – уникальный номер (идентификатор), однозначно связанный (ассоциируемый) с конкретным избирателем;

M – уникальный номер (метка), который нельзя сопоставить с конкретным избирателем. Генерируется разово, специально для процедуры голосования;

kpub, kpriv – открытый и закрытый ключи для асимметричного шифрования. Открытый ключ доступен всем желающим и однозначно связан с ID ищбирателя;

ken, kdec – асимметричные ключи зашифрования и расшифрования. В отличие от предыдущей пары ключей, ken (аналог kpub) хранится в тайне;

ksecr – секретный ключ для симметричного или асимметричного шифровани;

DS (англ. digital signature) – электронная цифровая подпись, ЭЦП;

h(X) – функция хеширования сообщения X;

encrypt(k, X) – функция зашифрования ключом k сообщения X;

decrypt(k, X) – функция расшифрования ключом k сообщения X;

sign(k, X) = encrypt(k, X) – функция создания ЭЦП ключом k для сообщения X;

unsign(k, X) = decrypt(k, X) – функция проверки ЭЦП ключом k для сообщения X;

blind({r, k}, X) = encrypt({r, k}, X) – процедура зашифрования методом слепой подписи с помощью «закрывающего множителя» r и ключа k сообщения X;

unblind({r-1, k}, X) = encrypt({r-1, k}, X) – процедура расшифрования методом слепой подписи с помощью «раскрывающего множителя» r-1 и ключа k сообщения X;

{} – набор данных;

* – множество однотипных данных;

= – расчет значения по определенному алгоритму;

== – сравнение значений;

защищенный канал – канал связи, который устойчив к прослушиванию и вмешательству или по которому информация передается в зашифрованном виде;

анонимно – передача информации таким образом, чтобы получатель не мог определить отправителя.

Ниже приведена выбранная для модификации схема протокола голосования с Центральной избирательной комиссией на базе "слепой" подписи (рис. 2).

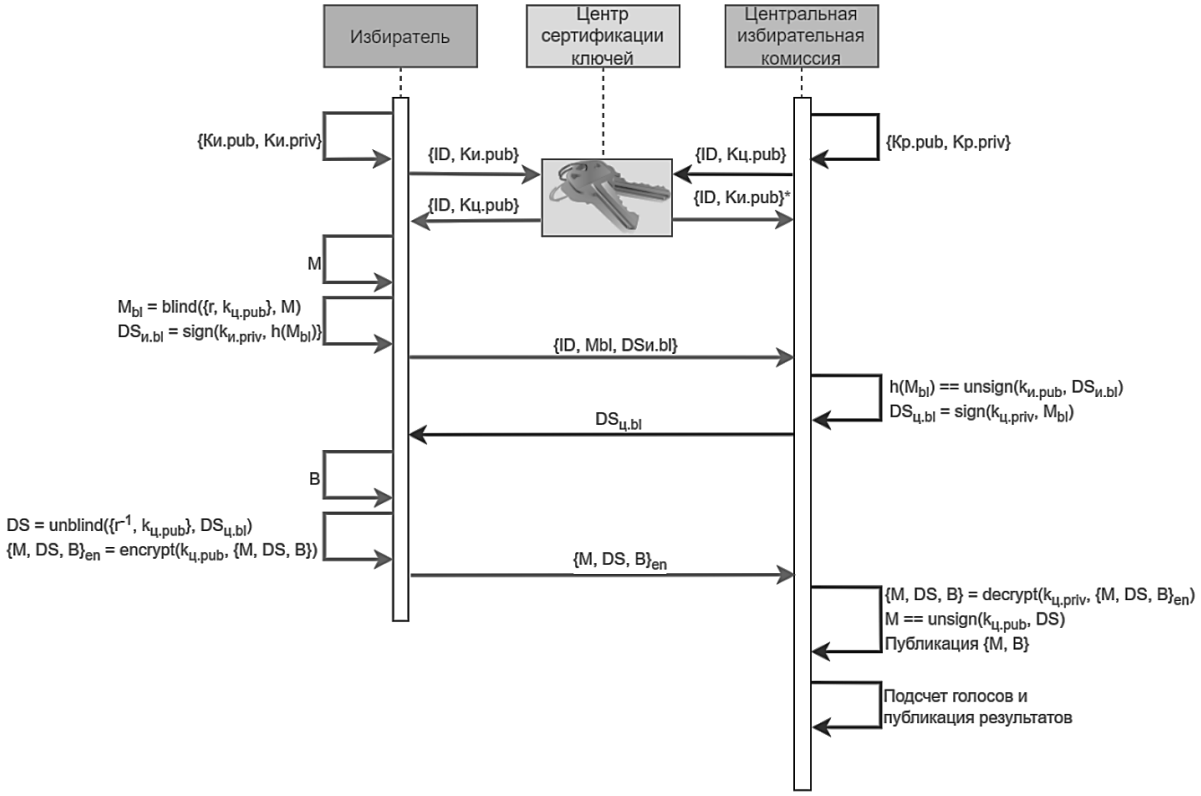

Рис. 2. *Схема протокола голосования с ЦИК на базе "слепой" подписи*

Этот протокол взят из редакции В.В. Анисимова [1]. "Слепая" подпись в данном случае применяется не к бюллетеню, как это описано у Соломаа [4], а к уникальной метке M. Данная поправка позволяет обеспечить 3-е свойство идеального голосования – анонимность избирателя.

Шаг 1. Центральная избирательная комиссия (далее – ЦИК) публикует список всех правомочных избирателей, создает пару ключей для асимметричного шифрования {kp.pub, kp.priv}; публикует открытый ключ kp.pub в Центр сертификации ключей.

Шаг 2. Избиратель создает пару ключей для асимметричного шифрования {ки.pub, ки.priv} и публикует открытый ключ ки.pub в ЦСК (публикация ключа является в данном случае регистрацией на конкретного избирателя с присвоенным ему ID); генерирует уникальную метку M: скрывает содержимое метки Mbl = blind({r, кц.pub}, M); ки.priv подписывает содержимое метки DSи.bl = sign(ки.priv, h(Mbl)} и посылает ЦИК свой ID, скрытую метку Mbl и ЭЦП к ней DSи.bl.

Шаг 3. ЦИК с помощью открытого ключа избирателя ки.pub проверяет его ЭЦП к скрытой метке h(Mbl) == unsign(ки.pub, DSи.bl) с целью аутентификации избирателя С помощью своего закрытого ключа кц.priv подписывает скрытую метку DSц.bl = sign(кц.priv, Mbl); посылает избирателю "слепую" ЭЦП DSц.bl к скрытой метке Mbl.

Шаг 4. Избиратель снимает "закрывающий множитель" r со "слепой" подписи комиссии DSц.bl и получает ЭЦП комиссии DS = unblind({r-1, кц.pub}, DSц.bl) к метке M; делает свой выбор в бюллетене B, с помощью открытого ключа ЦИК кц.pub шифрует в виде единого файла метку M, ЭЦП к ней DS и бюллетень B {M, DS, B}en = encrypt(кц.pub, {M, DS, B}). Шифрование выполняется, чтобы при посылке данного набора информации никто не смог бы подменить бюллетень, анонимно посылает зашифрованный файл {M, DS, B}en в ЦИК.

Шаг 5. ЦИК с помощью кц.priv расшифровывает файл {M, DS, B} = decrypt(кц.priv, {M, DS, B}en); с помощью кц.pub проверяет свою подпись DS к метке M == unsign(кц.pub, DS); публикует {M, B} для того чтобы избиратель убедился, что его голос учтен; подводит подсчет голосов; публикует результаты голосования.

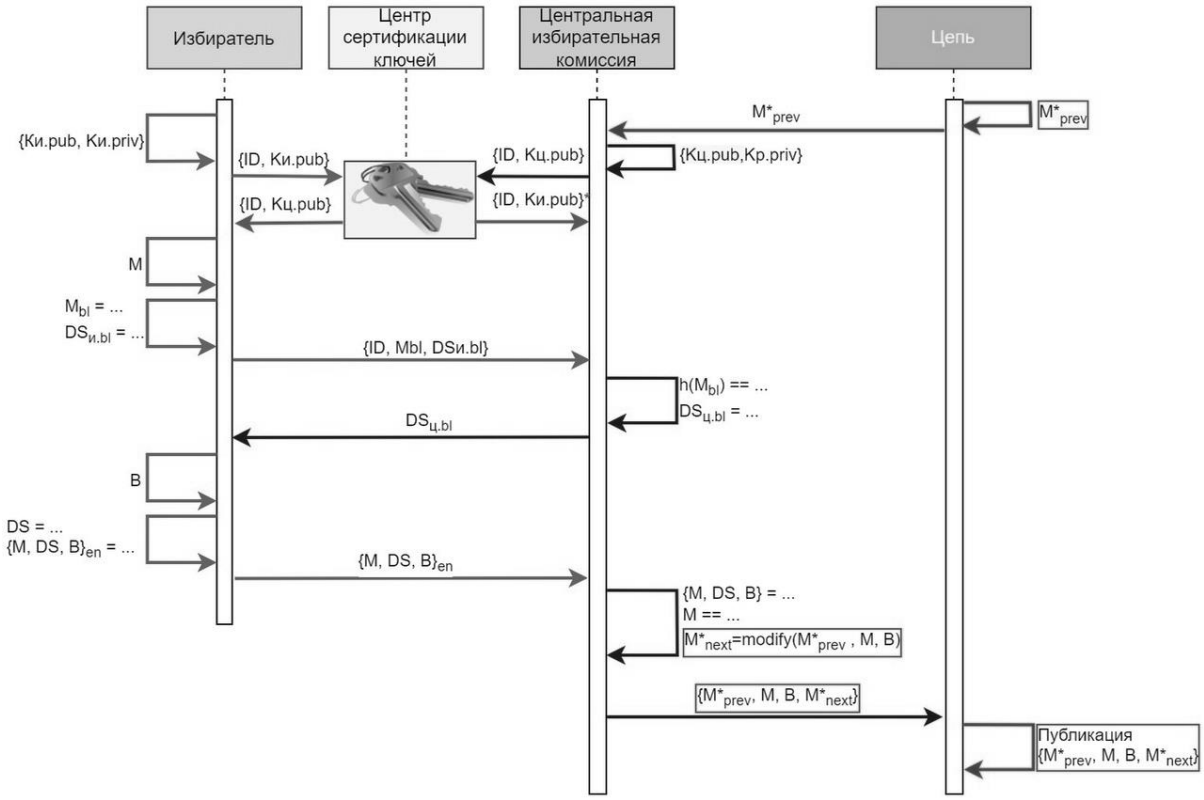

Рис. 3. *Схема протокола электронного голосования с "Цепью"*

Данный протокол обладает всеми свойствами "идеального голосования": защищен от постороннего вмешательства, добавляется третье звено – ЦСК – для контроля ключей со сторон избирателя и ЦИК, "слепая" подпись обеспечивает анонимность.

Недостатками данного протокола являются возможность покупки голосов и отсутствие возможности просмотра списка избирателей.

На рис. 3 представлена новая система на базе протокола голосования с ЦИК на базе "слепой" подписи – Схема протокола электронного голосования с новой стороной – "Цепью".

Обозначения на схеме:

M^*_{prev} – хеш предыдущего блока голосования;

modify(M^*_{prev},M,B) – функция получения хеша от значения , полученного от предыдущего блока, метки избирателя и бюллетеня;

M^*_{next} – модифицированная метка, результат работы функции modify().

Публикация ({M^*_{prev},M,B, M^*_{next}}) – публикация M^*_{prev}, M,B,M^*_{next} избирателя для того чтобы он мог убедиться, что его голос учтен.

Тело голосования остается таким же, однако добавляется предварительный и заключительный шаг для каждой итерации голосования.

Предварительный шаг: наследование результата хеш-функции от предыдущего блока M^*_{prev}. При наследовании избиратель не знает, кем являлся предыдущий избиратель, он получает от него только модифицированную метку.

Заключительный шаг: после того, как избиратель сделал выбор в бюллетене он модифицирует свою метку также с помощью хеш-функции (причем в ее параметр входит и предыдущее значение M^*_{prev}) и передает результат M^*_{next} в "Цепь". Это значение вновь используется в следующем звене как исходное значение M^*_{prev}.

Избиратель может изменить свой голос только до построения цепи. После ее построения все голоса являются связанными.

Так как публикуется ({M^*_{prev},M,B, M^*_{next}}) для каждого избирателя, то каждый избиратель может посчитать результат голосования, проследить, встроен ли его голос в "Цепь" и даже проследить целостность цепи от начала и до конца.

4. Достоинства системы

"Цепь" позволяет подтвердить, что все голоса всех проголосовавших учтены и намеренного удаления чьего-либо голоса не было. У избирателей есть возможность удостовериться, что их голоса учтены и попали в "Цепь".

Перед началом голосования публикуются списки правомочных избирателей, которые зарегистрировались в системе. Это сокращает возможность ЦИК добавлять новых людей в процессе голосования и пользоваться их правом голоса, и избиратель может быть уверен, что все, кто есть в цепи – реальные люди.

Поскольку в цепи публикуются только метки и бюллетени, избиратели могут узнать, кто проголосовал, только если голосовавшие раскроют свои метки. Но даже так избиратели не узнают, за кого именно отдал голос другой избиратель.

Даже если злоумышленник перехватит блок на пути к "Цепи", он не сможет поменять выбор в бюллетене – так как это отразится в результате хеш-функции.

Заключение

В данной работе, для повышения контроля над электронным голосованием со стороны избирателей, разработана система электронного голосования, в основе которой лежит механизм связи голосов в единую "Цепь". Для выбора базового протокола электронного голосования было произведено сравнение протоколов: на базе ANDOS, протокола Фудзиока–Окамота–Охта и протокола с Центральной избирательно комиссией на базе слепой подписи, относительно возможности добавления нового функционала. Сравнение показало, что оптимальным выбором протокола, на основе которого можно построить новый, будет протокол с ЦИК на базе "слепой" подписи.

Новый протокол голосования удовлетворяет свойствам идеального голосования [3, с. 103] и у избирателей появляется больше контроля над процессом выборов.

Список источников

1. *Учебная* и научная деятельность Анисимова Владимира Викторовича. URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema15/tema15_3#p1532 (дата обращения: 9.11.2022).
2. *Electronic* voting by country. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.885e82f0-626929b5-b6657333-74722d776562/https/en.wikipedia.org/wiki/Electronic_voting_by_country, (дата обращения: 22.04.2022).
3. *Шнайер Б.* Прикладная криптография, второе издание, 2002. 103 с.
4. *Solomaa A.* Public-Key Cryptography. Springer-Verlag, 1990.

References

1. *Educational* and scientific activity of Vladimir Viktorovich Anisimov. URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema15/tema15_3#p1532 (accessed: 09.10.2022). (In Russ.).
2. *Electronic* voting by country. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.885e82f0-626929b5-b6657333-74722d776562/https/en.wikipedia.org/wiki/Electronic_voting_by_country, (accessed: 22.04.2022).
3. *Schneier* Bruce. Applied Cryptography, second edition, 2002. 103 p. (In Russ.).
4. *Solomaa A.* Public-Key Cryptography. Springer-Verlag; 1990.

Информация об авторах:

Э. А. Нехорошева – студент 5 курса механико-математического факультета Пермского государственного национального исследовательского университета (614068, г. Пермь, ул. Букирева, 15), emmanekhorosheva@vk.com;

А. П. Шкарапута – кандидат физико-математических наук, доцент кафедры информационной безопасности и систем связи механико-математического факультета Пермского государственного национального исследовательского университета (614068, г. Пермь, ул. Букирева, 15), shkaraputa@psu.ru, AuthorID 69440.

Information about the authors:

Э. А. Nekhorosheva is a 5th year Student of the Faculty of Mechanics and Mathematics, Perm State University (15, Bukireva street, Perm, 614068), emmanekhorosheva@vk.com;

A. P. Shkaraputa – Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Information Security and Communication Systems, Faculty of Mechanics and Mathematics, Perm State University (15, Bukireva street, Perm, 614068), shkaraputa@psu.ru, AuthorID 69440.