№ 5 (190)

Раздел I. Информационные технологии и защита информации

УДК 004.422 DOI 10.23683/2311-3103-2017-5-6-15

Л.К. Бабенко, И.А. Писарев, О.Б. Макаревич

ЗАЩИЩЕННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ С ИСПОЛЬЗОВАНИЕМ СЛЕПЫХ ПОСРЕДНИКОВ*

Наша жизнь всё больше связывается с интернетом. Естественно коснется она и политики. В этом плане уже сейчас существует множество предложений и практических реализаций по решению проблем электронного голосования. При этом одним из важных вопросов проведения выборов является обеспечение защищенности информации в системе. Мы предлагаем рассмотреть систему проведения электронного голосования с использованием современных достижений криптографии на всех этапах функционирования системы. Основной прием, который использован при формировании защищенного протокола передачи информации между серверами системы, представляет собой шифрование разными ключами разных частей передаваемой разным получателям информации. Мы назвали этот протокол протоколом на основе слепых посредников. Основываясь на этом протоколе возможно построение системы электронного голосования, в которой будут соблюдены основные требования, а именно то, чтобы в голосовании могли участвовать только определенные люди и что нельзя сопоставить открытые персональные данные людей с голосом. Система отличается комплексностью выполнения всех необходимых функций электронного голосования, обоснованностью введения средств защиты информации на всех этапах: подготовки, регистрации, голосования, подсчета голосов. Приведена общая схема проведения электронного голосования. Описаны базовые приемы для обеспечения проведения электронного голосования, а именно: безопасность передаваемых конфиденциальных данных, распределение секретных ключей, аутентификация сторон, проверка передаваемых данных на целостность, временной контроль передаваемых данных. Разработаны алгоритмы, реализующие четкую последовательность действий на каждом этапе. На базе разработанных алгоритмов реализована система электронного голосования на языке программирования C# .Net Framework, состоящая из набора оконных приложений, взаимодействующих между собой через сеть. Показана эффективность разработанной системы. Отмечены направления усовершенствования системы.

Электронное голосование; криптографическая защита; .Net; система.

L.K. Babenko, I.A. Pisarev, O.B. Makarevich

PROTECTED ELECTRONIC VOTING SYSTEM WITH THE USE OF BLIND INTERMEDIARIES

Our life is more and more connected with the Internet. Naturally, it concerns politics as well. In this regard, there are already many proposals and practical implementations for solving electronic voting problems. At the same time, ensuring the security of information in the system is an important issue in the conduct of elections. We propose to consider the possibility of voting using modern achievements of cryptography at all stages of the system functioning. The main technique used to create secure protocols between the servers of the system is the encryption of various keys of different parts of

* Работа выполнена при финансовой поддержке РФФИ грант № 15-07-00597.

the information transmitted to different recipients. We called this protocol a protocol based on blind intermediaries. Basing on this protocol it is possible to built the system of electronic voting where all necessary requirements are taken into account, namely a possibility of participating in voting only for certain people and an impossibility to match the opened personal data of people with their vote. The system is characterized by the complex performance of all necessary functions for the protection of rights at all stages: preparation, registration, voting, counting of votes. The general scheme of voting is given. The basic techniques for providing system voting are described, namely: security of confidential data transmitted, distribution of secret keys, authentication of the parties, verification of the transmitted data for integrity, temporal control of the transmitted data. Algorithms implementing a clear sequence of actions at each stage have been developed on the basis of C # .Net Framework, consisting of a set of window applications interacting with each other across the network. The efficiency of the developed system is shown. Areas of improvement of the system are noted.

Electronic voting; cryptographic protection; .Net; system.

Введение. Разработка алгоритмов проведения выборов актуальная проблема. Электронные выборы значительно превосходят по надежности и эффективности традиционные алгоритмы. На данный момент существует множество алгоритмов, базирующихся на современных принципах, однако все они не позволяют полностью обеспечить безопасность и честность выборов, а ряд алгоритмов не пригодны для использования на практике [1–7]. Таким образом, актуальными являются разработки, которые с одной стороны были бы просты в реализации, и с другой стороны – обеспечивали бы хорошую надежность, честность и самое главное максимально снижали бы влияние человеческого фактора. В данной статье предлагается система, построенная с применением современных криптографических алгоритмов, обеспечивающая высокую защищенность и приемлемую скорость работы. Главное достоинство разработки – комплексность решаемых вопросов, завершенность структурных единиц, детальная проработка основных этапов функционирования.

Этапы проведения электронного голосования. Проанализировав существующие публикации то теме организации электронных выборов, мы можем перечислить основные этапы их проведения [8–21].

1. **Подготовка.**

На данном этапе формируется база данных потенциальных голосующих, которая включает в себя их персональные данные, например паспортные, биометрические данные и прочие данные, по которым можно идентифицировать личность голосующего. Формируется бюллетень, в котором перечисляются кандидаты и некоторые данные о них.

2. **Регистрация и анонимизация.**

На данном этапе голосующему предоставляется функционал, позволяющий ввести ему свои персональные данные, произвести считывание (если необходимо) его биометрических данных, обеспечить безопасную передачу этих данных на удаленный сервер с базой данных, сформированной на этапе 1. В случае наличия такого набора данных для голосующего в базе данных обеспечить его анонимным токеном доступа, который в большинстве случаев представляет собой анонимный идентификатор пользователя в виде случайно сгенерированных данных фиксированной разрядности. На этом этапе очень важно обеспечить невозможность сопоставить открытые персональные данные голосующего с его анонимным токеном доступа.

3. **Голосование.**

На данном этапе голосующий заполняет бюллетень и отправляет его вместе со своим анонимным токеном доступа на сервер для голосования. В случае если такой токен доступа присутствует в базе данных, то голос принимается, а пользователю предоставляется некоторый функционал, который позволит после окончания голосования проверить, что его голос учтен после окончания голосования. На этом этапе необходимо обеспечить невозможность определения предварительной статистики голосов, а так же исключить возможность «вброса» голосов.

4. Подсчет и проверка голосов.

На данном этапе производится подсчет голосов. Результаты публикуются в общем доступе, а голосующему предоставляется функционал, позволяющий проверить ему свой голос.

Базовые приемы для обеспечения проведения электронного голосования. Одна из важных задач в ходе проведения электронного голосования это обеспечение безопасной передачи конфиденциальных данных на сервер. Её можно решить с помощью использования стойкого симметричного шифра, лучше всего, например, в режиме сцепления блоков. Это обеспечит надежную защиту данных в процессе передачи.

Для осуществления шифрования с помощью симметричного шифра обе стороны должны иметь общий секретный ключ. Одним из способов распределения ключа является использование протоколов прямого взаимодействия партнеров для выработки общего сессионного ключа. Они позволяют двум сторонам, используя незащищенный канал связи выработать общий сессионный ключ, который можно использовать для шифрования данных в процессе их передачи между сторонами.

В процессе передачи важно чтобы обе стороны доверяли друг другу и знали, что это именно та сторона, с которой и желает общаться другая сторона. Обеспечить это возможно благодаря использованию аутентификации сторон. Одним из способов обеспечения аутентификации сторон является использование механизма «Запрос-ответ», когда случайное число, добавляется в некоторые части сообщений для проверяемого, последний при этом должен возвратить значение функции от этого числа как от аргумента.

В процессе передачи необходимо производить контроль целостности передаваемых данных. Одним из способов обеспечения контроля целостности является комбинация шифрования в режиме распространяющегося сцепления блоков и случайного числа, расположенного в конце сообщения.

Передаваемые данные должны быть актуальными по времени. Данные, передаваемые в определенный промежуток времени должны быть обработаны за выделенный отрезок времени, и их повторное использование в другое время должно быть невозможно. Одним из вариантов обеспечения контроля передачи данных по времени является контроль сессии на стороне сервера по времени. Сервер принимает соединение клиента на некоторое время, и в случае если оно не завершится успешно, обрывает соединение.

Необходимо, чтобы каждый пользователь был сопоставлен с его некоторым «электронным» эквивалентом. В большинстве случаев это достигается путем использования уникальных идентификаторов или иных случайных данных. В данной работе каждому пользователю изначально сопоставлен набор хэшей, а затем производится его сопоставление с уникальным идентификатором.

Система электронного голосования в общем случае должна выполнять два фундаментальных требования: в голосовании могут принимать участие только пользователи, которые занесены в специальную базу данных, и сопоставить голос пользователя с его открытыми персональными данными должно быть невозможно. Выполнение этих фундаментальных требований осуществляется путем использования предложенного авторами принципа слепых посредников.

Слепые посредники. Поясним работу принципа «слепые посредники», используя схему, изображенную на рис. 1.

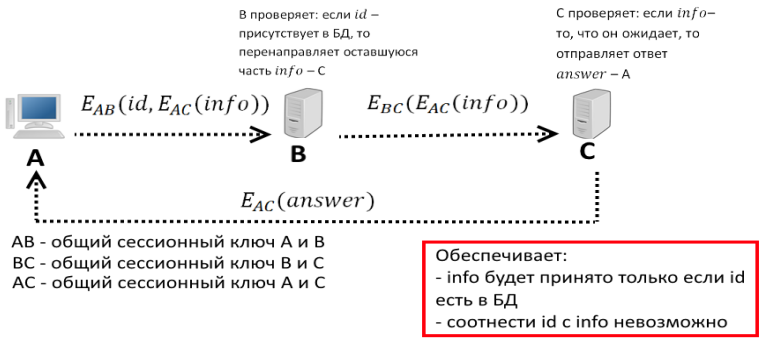

Рис. 1. Схема на основе слепых посредников

Имеются 3 взаимодействующие стороны A, B, C. С помощью протокола выработки общего секретного ключа осуществляется генерация сессионного ключа AB, BC, AC. A шифрует некоторую информацию info на ключе AC, прилагает к этому идентификатор id, шифрует на ключе AB и посылает это сообщение B. B и является в данном случае слепым посредником, поскольку он может расшифровать только первую часть сообщения с id, а оставшуюся часть с info не сможет. Он принимает сообщение, расшифровывает, проверяет наличие id в БД и в случае успеха перенаправляет оставшуюся часть сообщения, шифрованную ещё раз на ключе BC стороне C. C принимает сообщение, расшифровывает info, шифрует ответ answer на ключе AC и посылает его A. Данный принцип обеспечивает то, что: info будет принято только если id есть в БД и то, что соотнести id с info невозможно. Тем самым на основе данного принципа можно построить систему электронного голосования, где выполняются главные требования, чтобы в выборах могло участвовать только строгое количество людей, и одновременно с этим невозможно было сопоставить их голос с какими либо данными или идентификаторами.

Система электронного голосования на основе слепых посредников. Архитектура системы основана на использовании следующих компонентов: клиентское приложение для голосующего V, 3 серверных приложения, которые будут расположены на разных физических машинах: «Сервер аутентификации» AS (authentication server), «Сервер обработки» PS (processing server), «Сервер учета голосов» VS (voting server), приложение-шифровальщик для паспортной базы данных и бюллетени DBE (database encryptor). Общая схема взаимодействия компонентов представлена на рис. 2.

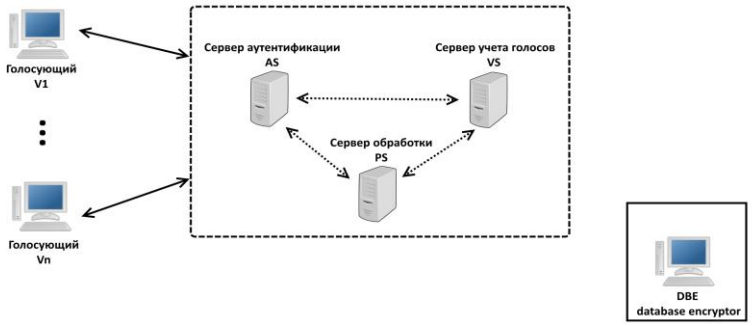

Рис. 2. Общая схема взаимодействия компонентов системы

Этап подготовки.

На данном этапе производится составление базы данных голосующих и бюллетеней (Все серверы выключены, работа производится на изолированной от сети машине с помощью компонента DBE).

На данном этапе присутствует человеческий фактор. Поля БД включают в себя данные, по которым можно идентифицировать личность. На данный момент используются паспортные данные граждан. База подгоняется под формат хранения для компонента DBE, а именно: от каждого набора полей берется хэш, в итоге представление одного человека в базе будет в виде набора хэшей. Хэш функция на данный момент используется SHA-512. Хэши берутся от набора полей, чтобы практически полностью исключить их совпадение при одинаковом значении поля в паспорте и чтобы усложнить обращение данных обратно в строковое представление (рис. 3). После чего база шифруется на некотором ключе DBPass с помощью приложения-шифровальщика DBE.

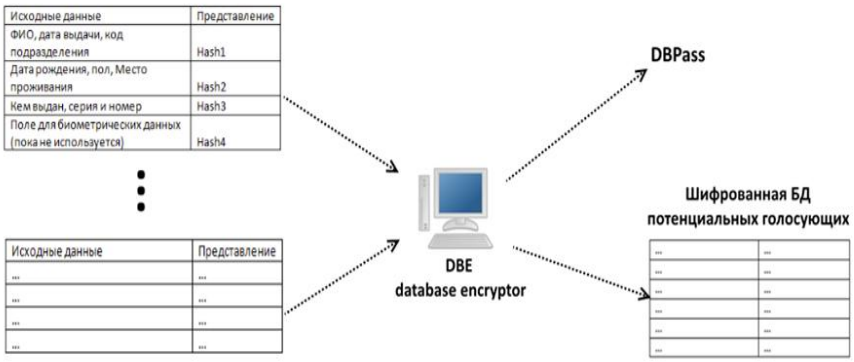

Рис. 3. Подготовка БД

Далее формируется бюллетень, в котором перечислены имена кандидатов и некоторая информация о них. Готовый бюллетень подается в DBE, где он переводится в специфичный формат ballot. После чего бюллетень шифруется на некотором ключе bullotPass с помощью приложения-шифровальщика DBE (рис. 4).

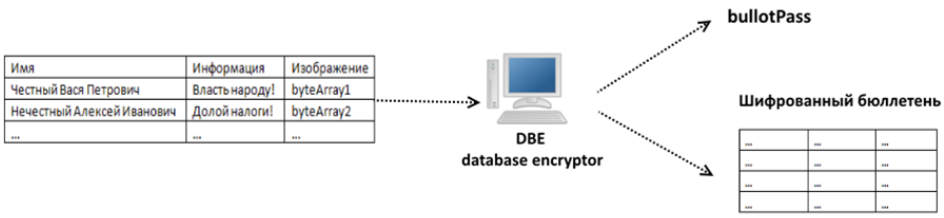

Рис. 4. Подготовка бюллетеня

Специально назначенные должностные лица доставляют шифрованную БД потенциальных голосующих на AS и шифрованный бюллетень на VS.

Этап регистрации и анонимизации. AS, PS включены, VS выключен. Шифрованная база подается в компонент AS, расшифровывается и компонент начинает свою работу. Вместе с этим включается компонент PS. Упрощенная схема этапа регистрации изображена на рис. 5.

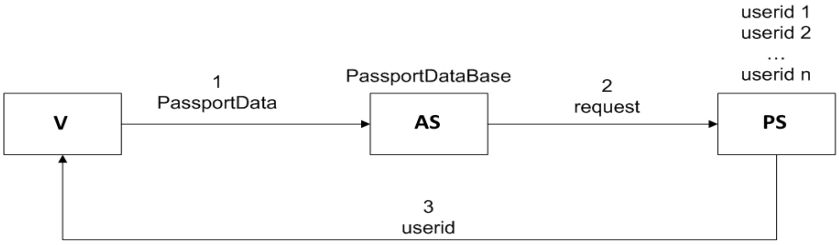

Рис. 5. Упрощенная схема этапа регистрации

Подготовка этапа.

Осуществляется генерация общих секретных ключей V, VAS, VPS с помощью протокола выработки общего сессионного ключа. Стороны-серверы генерируют случайные числа и отправляют своему получателю сообщения (1), (2), (3). Они будут использоваться для аутентификации сторон.

Процесс регистрации и анонимизации.

V генерирует N_v, которое из-за своего расположения в конце сообщения и использования симметричного шифра в режиме сцепления блоков, позволит проверить сообщение на целостность. Далее формирует сообщение (4) с паспортными данными, которые являются набором хешей от набора полей, шифрованными случайными числами на общем секретном ключе VPS, все это шифруется на ключе VAS и отправляется AS. AS в данном случае является слепым посредником. Он проверяет наличие PassportData в БД и в случае успеха перенаправляет другую часть сообщения (5) PS. PS проверяет случайное число и в случае успеха генерирует userid, добавляет его в свою БД и отсылает его V в виде сообщения (6). Голосующий расшифровывает сообщение, проверяет значения случайных чисел и запоминает свой обезличенный уникальный идентификатор userid, с помощью которого пользователь сможет проголосовать.

Подготовка этапа:

ECDHE (V, AS) - vas – общий секретный ключ для обмена

V: генерирует N_{as}

(1)AS -> V: $E_{vas}(N_{as})$

ECDHE (V, PS) – vps – общий секретный ключ для обмена

PS: генерирует N_{ps}

(2)PS -> V: $E_{vps}(N_{ps})$

ECDHE (PS, AS) – psas – общий секретный ключ для обмена

PS: генерирует N_{psas}

(3)PS -> AS: $E_{psas}(N_{psas})$

Процесс регистрации:

V: генерирует N_v.

(4)V -> AS: E_{vas} (N_{as}, PassportData, E_{vps} (N_{ps}, N_v,))

AS -> V: “Success”

(5)AS -> PS: E_{psas} (N_{psas}, $E_{vps}(N_{ps}, N_v)$) сообщает, что это доверенный адрес

PS: генерирует userid

(6)PS -> V: E_{vps} (N_{ps}, userid, N_v)

Этап голосования. AS выключен, PS, VS включены Компонент AS выключается, а VS включается. В компонент VS подается шифрованный бюллетень. Упрощенная схема этапа голосования изображена на рис. 6.

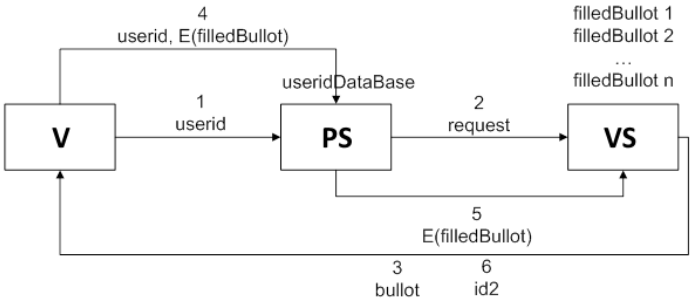

Рис. 6. Упрощенная схема этапа голосования

Подготовка этапа.

Осуществляется генерация общих секретных ключей V, VPS, VVS аналогично с помощью протокола выработки общего сессионного ключа. Стороны-серверы генерируют случайные числа и отправляют своему получателю сообщения (1), (2), (3).

Процесс голосования.

V генерирует N_{v1},. Далее формирует сообщение (4) со своим уникальным идентификатором userid, шифрованными случайными числами на общем секретном ключе VVS, все это шифруется на ключе VPS и отправляется PS. PS в данном случае является слепым посредником. Он проверяет наличие userid в БД и в случае успеха перенаправляет другую часть сообщения (5) VS. VS проверяет случайное число и в случае успеха отсылает V бюллетень в виде сообщения (6). Голосующий расшифровывает сообщение, проверяет значения случайных чисел, генерирует новое число Nv2, заполняет бюллетень, формирует сообщение (7) и отправляет PS. PS Расшифровывает, проверяет userid ещё раз, в случае успеха перенапрявляет оставшуюся часть сообщения (8) VS. VS расшифровывает, проверяет случайное число и принимает голос. Далее генерирует уникальный идентификатор id2, формирует сообщение (9) и отправляет его пользователю. Пользователь расшифровывает, проверяет случайные числа и запоминает свой id2, по которому он может проверить свой голос. Второй идентификатор нужен для усиления анонимности голоса.

Подготовка этапа:

ECDHE (V, PS) – vps – общий секретный ключ для обмена

PS: генерирует N_{ps}

(1)PS -> V: $E_{vps}(N_{ps})$

ECDHE (V, VS) – vvs – общий секретный ключ для обмена

VS: генерирует N_{vs}

(2)VS -> V: $E_{vvs}(N_{vs})$

ECDHE (PS, VS) – psvs – общий секретный ключ для обмена

VS: генерирует N_{psvs}

(3)VS -> PS: $E_{psvs}(N_{psvs})$

Процесс голосования:

V: генерирует N_{v1}

(4)V -> PS: E_{vps} (N_{ps}, userid, $E_{vvs}(N_{vs}, N_{v1})$)

(5)PS -> VS: E_{psvs} (N_{psvs}, $E_{vvs}(N_{vs}, N_{v1})$))

(6)VS -> V: $E_{vvs}(N_{vs}$, ballot, $N_{v1})$)

(7)V -> PS: E_{vps} (N_{ps}, userid, E_{vvs} (N_{vs}, N_{v2}, filledBullot))

(8)PS -> VS: E_{psvs} (N_{psvs}, E_{vvs} (N_{vs}, N_{v2}, filledBullot))

VS: запоминает голос

VS: генерирует id2

(9)VS -> V: $E_{vvs}(N_{vs}$, id2, $N_{v2})$

Этап подсчета и проверки голосов.

AS, PS выключены, VS включен. Публикуется подробный результат, который представляет собой структуру, где рядом с каждым кандидатом будет список id2 проголосовавших за него людей. Любой проголосовавший пользователь может проверить свой голос в этом списке. Пример представления результатов изображен в табл. 1.

Таблица 1

Пример представления результатов

Кандидат	id2 голосующего
Честный Вася Петрович	df8273
Честный Вася Петрович	cc8b2c
Честный Вася Петрович	aa12bc
Честный Вася Петрович	f1ffac
Нечестный Алексей Иванович	a34ccb
Нечестный Алексей Иванович	fcbb12

Пояснения по выбору средств реализации системы и алгоритмов ее функционирования:

- Для шифрования используется симметричный шифр AES с 256 битным ключом и в режиме распространяющегося сцепления блоков.
- Для выработки общего сессионного ключа используется протокол ECDHE – Диффи-Хеллмана на эллиптических кривых с использованием эфемерных ключей.
- В качестве хэш функции используется SHA-512.
- Разрядность случайных чисел и идентификаторов можно задавать. На данный момент их величина следующая: userid (4096 байт), id2 (128 байт), N (512 байт).
- При создании новой сессии с клиентом запоминается текущая отметка времени, и если присланный ответ от клиента пришел позднее некоторого порогового значения, то такое сообщение не принимается, а адрес машины так же записывается в черный список.

Направление дальнейшей работы. Данная система в настоящее время пригодна для проведения электронного голосования в небольших компаниях, однако для использования её в более серьезных целях, следует провести доработку на начальном этапе, поскольку тот, кто будет составлять базу данных голосующих, сможет легально воздействовать на выборы. На данном этапе в любом случае будет присутствовать человеческий фактор, никто на данный момент ещё не решил эту проблему, и единственным выходом в этой ситуации будет максимальное снижение человеческого фактора путем введения организационно технических мер.

Заключение. Разработанный алгоритм защищенного электронного голосования является простым в практической реализации и одновременно с этим обеспечивает безопасность и честность выборов. Реализация предложенного принципа «слепых посредников» обеспечивает анонимность голосующего, сохранность его персональных данных в процессе передачи, исключение «вброса» голосов, возможность проверки своего голоса, снижение человеческого фактора. На основе предложенных алгоритмов была создана система, состоящая из нескольких приложений, реализованных на языке программировании я C# в среде .Net Framework. Проведенные вычислительные эксперименты подтвердили корректную работу основных этапов голосования и приемлемую скорость выполнения алгоритмов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Marcin Kucharczyk*. Blind Signatures in Electronic Voting Systems // International Conference on Computer Networks. – 2010.
2. Overview of e-voting systems, NICK Estonia. – Estonian National Electoral Commission. Tallinn 2005.
3. *Shubhangi S. Shinde, Sonali Shukla, D.K. Chitre*. Secure E-voting Using Homomorphic Technology // International Journal of Emerging Technology and Advanced Engineering. – 2013.
4. *Markus Jakobsson, Ari Juels, Ronald L. Rivest*. Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking // 11th USENIX Security Symposium. – 2002.
5. *Ben Adida.* Mixnets in Electronic Voting. – Cambridge University, 2005.
6. *Лифшиц Ю*. Электронные выборы. – 2005. – http://yury.name/crypto/03cryptonote.pdf.
7. Electronic elections: fear of falsification of the results. – Kazakhstan today, 2004,
8. *Lipen V.Y., Voronetsky M.A.* Lipen DV technology and results of testing electronic voting systems. – United Institute of Informatics Problems NASB, 2002.
9. *Chaum David L.* Untraceable electronic mail, return addresses, and digital pseudonyms // Communications of the ACM. – 1981. – Vol. 24 (2). – P. 84-90.
10. *Ali S. T., Murray J.* An Overview of End-to-End Verifiable Voting Systems // arXiv preprint arXiv: 1605.08554. – 2016.
11. *Smart M., Ritter E.* True trustworthy elections: remote electronic voting using trusted computing // International Conference on Autonomic and Trusted Computing. – Springer Berlin Heidelberg, 2011. – S. 187-202.
12. *Bruck S., Jefferson D., Rivest R.L.* A modular voting architecture ("frog voting") // Toward strustworthy elections. – Springer Berlin Heidelberg, 2010. – S. 97-106.
13. *Jonker H., Mauw S., Pang J.* Privacy and verifiability in voting systems: Methods, developments and trends // Computer Science Review. – 2013. – Vol. 10. – P. 1-30.
14. *Dossogne J., Lafitte F.* Blinded additively homomorphic encryption schemes for self-tallying voting //Journal of Information Security and Applications. – 2015. – Vol. 22. – P. 40-53.
15. *Neumann S., Volkamer M.* Civitas and the real world: problems and solutions from a practical point of view // Availability, Reliability and Security (ARES), 2012 Seventh International Conference on. – IEEE, 2012. – S. 180-185.
16. *Yi X., Okamoto E.* Practical remote end-to-end voting scheme // International Conference on Electronic Government and the Information Systems Perspective. – Springer Berlin Heidelberg, 2011. – S. 386-400.
17. *Hirt M., Sako K.* Efficient receipt-free voting based on homomorphic encryption // International Conference on the Theory and Applications of Cryptographic Techniques. – Springer Berlin Heidelberg, 2000. – P. 539-556.
18. *Rivest L. R. et al.* Lecture notes 15: Voting, homomorphic encryption. – 2002.
19. *Sako K., Kilian J.* Secure voting using partially compatible homomorphisms //Annual International Cryptology Conference. – Springer Berlin Heidelberg, 1994. – P. 411-424.
20. Izabachene M. A Homomorphic LWE Based E-voting Scheme // Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016.
21. *Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine J. Alex Halderman*. Security Analysis of the Estonian Internet Voting System, University of Michigan, Ann Arbor, MI, U.S.A. – 2014.

REFERENCES

1. *Marcin Kucharczyk*. Blind Signatures in Electronic Voting Systems, *International Conference on Computer Networks*, 2010.
2. Overview of e-voting systems, NICK Estonia. Estonian National Electoral Commission. Tallinn 2005.
3. *Shubhangi S. Shinde, Sonali Shukla, D.K. Chitre*. Secure E-voting Using Homomorphic Technology, *International Journal of Emerging Technology and Advanced Engineering,* 2013.
4. *Markus Jakobsson, Ari Juels, Ronald L. Rivest*. Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking, *11th USENIX Security Symposium*, 2002.
5. *Ben Adida.* Mixnets in Electronic Voting. Cambridge University, 2005.

6. *Lifshits Yu.* Elektronnye vybory [Electronic elections], 2005. Available at: http://yury.name/crypto/03cryptonote.pdf.
7. Electronic elections: fear of falsification of the results. Kazakhstan today, 2004.
8. *Lipen V.Y., Voronetsky M.A.* Lipen DV technology and results of testing electronic voting systems. United Institute of Informatics Problems NASB, 2002.
9. *Chaum David L.* Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 1981, Vol. 24 (2), pp. 84-90.
10. *Ali S. T., Murray J.* An Overview of End-to-End Verifiable Voting Systems, *arXiv preprint arXiv: 1605.08554*, 2016.
11. *Smart M., Ritter E.* True trustworthy elections: remote electronic voting using trusted computing, *International Conference on Autonomic and Trusted Computing*. Springer Berlin Heidelberg, 2011, pp. 187-202.
12. *Bruck S., Jefferson D., Rivest R.L.* A modular voting architecture ("frog voting"), *Toward strustworthy elections*. –pringer Berlin Heidelberg, 2010, pp. 97-106.
13. *Jonker H., Mauw S., Pang J.* Privacy and verifiability in voting systems: Methods, developments and trends, *Computer Science Review*, 2013, Vol. 10, pp. 1-30.
14. *Dossogne J., Lafitte F.* Blinded additively homomorphic encryption schemes for self-tallying voting, *Journal of Information Security and Applications*, 2015, Vol. 22, pp. 40-53.
15. *Neumann S., Volkamer M.* Civitas and the real world: problems and solutions from a practical point of view, *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*. IEEE, 2012, pp. 180-185.
16. *Yi X., Okamoto E.* Practical remote end-to-end voting scheme, *International Conference on Electronic Government and the Information Systems Perspective*. Springer Berlin Heidelberg, 2011, pp. 386-400.
17. *Hirt M., Sako K.* Efficient receipt-free voting based on homomorphic encryption, *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer Berlin Heidelberg, 2000, pp. 539-556.
18. *Rivest L. R. et al.* Lecture notes 15: Voting, homomorphic encryption, 2002.
19. *Sako K., Kilian J.* Secure voting using partially compatible homomorphisms,*Annual International Cryptology Conference*. Springer Berlin Heidelberg, 1994, pp. 411-424.
20. Izabachene M. A Homomorphic LWE Based E-voting Scheme, *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016*.
21. *Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine J. Alex Halderman.* Security Analysis of the Estonian Internet Voting System, University of Michigan, Ann Arbor, MI, U.S.A. 2014.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@fib.tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Писарев Илья Александрович – e-mail: ilua.pisar@gmail.com; г. Таганрог, ул. Котлостроительная, 7, кв. 35; тел.: 89885350837; кафедра безопасности информационных технологий; студент.

Макаревич Олег Борисович – e-mail: mak@tsure.ru; г. Таганрог, ул. Пальмиро Тольятти, 24/6, кв. 43; тел.: 89034043583; кафедра безопасности информационных технологий; д.т.н.; профессор.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; Block “I”, 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Pisarev Ilya Aleksandrovich – e-mail: ilua.pisar@gmail.com; 7, Kotlostroitelnaia street, Apt. 35, Taganrog, Russia; phone: +79885350837; the department of information technology security; student.

Makarevich Oleg Borisovich – e-mail: mak@tsure.ru; 24/6, Palmiro Togliatti street, apt. 43, Taganrog, Russia; phone: +79034043583; the department of information technology security; dr. of eng. sc.; professor.