УДК 004.056.53

СОЗДАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОБЕСПЕЧЕНИЯ ДОСТАТОЧНОГО УРОВНЯ АНОНИМНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ С СОХРАНЕНИЕМ ЦЕЛОСТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ПЕРЕДАВАЕМЫХ ДАННЫХ

Угрюмов Дмитрий Викторович
аспирант, тел.: +7(918) 377-97-29,
ugryumoff@gmail.com

Хализев Вячеслав Николаевич
к.т.н., профессор
Кубанский Государственный Технологический Университет, г. Краснодар, Россия

В статье представлены результаты аналитического обзора существующих методов обеспечения анонимности, исследование архитектур системы электронного голосования, а также представлена авторская идея по улучшению анонимности клиента в таких системах. В результате сформирована математическая модель обеспечения достаточного уровня анонимности в системах электронного голосования с сохранением целостности и конфиденциальности передаваемых данных

Ключевые слова: АНОНИМНОСТЬ, КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ, КЛЮЧ, ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ

UDC 004.056.53

CREATION A MATHEMATICAL MODEL, THAT PROVIDES A SUFFICIENT LEVEL OF ANONYMITY IN E-VOTING SYSTEM WITH THE INTEGRITY AND PRIVACY OF TRANSMITTED DATA

Ugryumov Dmitriy Victorovich
graduate, phone: +7(918) 377-97-29,
ugryumoff@gmail.com

Khalizev Vyacheslav Nikolaevich
Cand.Tech.Sci., professor
Kuban State Technological University, Krasnodar, Russia

The article presents the results of an analytical review of existing methods to ensure anonymity, the study of the system architecture of the electronic voting, and presented the author’s idea to improve the client's anonymity in such systems. The result is a mathematical model, that provides a sufficient level of anonymity in electronic voting system to preserve the integrity and confidentiality of transmitted data

Keywords: ANONYMITY, CRYPTOGRAPHIC ALGORITHM, KEY, ELECTRONIC VOTING

1. ВВЕДЕНИЕ

В настоящее время обеспечение анонимности клиента в сети Интернет становится всё более обсуждаемой и актуальной темой. Повышенное внимание общества к цензуре и методам борьбы с ней, постоянный рост количества преступлений в информационной сфере, забота государства о частной жизни и персональных данных граждан, – данные тезисы всё чаще появляются в средствах массовой информации и являются предметом постоянных дискуссий в правительстве и обществе.

Проблема обеспечения математически доказуемой абсолютной анонимности субъекта при взаимодействии его с адресатом в информационной системе сейчас не решена и относится к ряду

концептуальных проблем современных информационных технологий.

Одной из научных задач в данной сфере, решению которой посвящено данное исследование, является обеспечение достаточного уровня анонимности отправителя электронных сообщений в распределённой компьютерной системе, реализующей также механизмы электронного голосования. Решение данной задачи открывает перспективу практическим реализациям защищенных программно-аппаратных систем электронного анонимного голосования, средств обеспечения и преодоления цензурирования, а также методологии расследования компьютерных инцидентов, в частности, анонимных атак через Интернет.

Следовательно, актуальность всего исследования в общем и данной статьи в частности не вызывает сомнений.

Объектом исследования является совокупность методов и средств обеспечения анонимности клиента в информационных системах, а также механизмов электронного голосования.

Целью работы является создание математической модели обеспечения достаточного уровня анонимности для отправителя электронных сообщений в распределённой компьютерной системе, реализующей механизмы электронного голосования с сохранением целостности и конфиденциальности передаваемых данных.

Для успешного достижения цели работы необходимо решить следующие поставленные задачи:

− провести аналитический обзор традиционных методов и средств обеспечения анонимности в компьютерных сетях;

− выявить различные уязвимости анонимности клиента, а также угрозы конфиденциальности и целостности передаваемых им сообщений;

− сформировать авторскую идею повышения анонимности в системе электронного голосования;

− разработать общую математическую модель обеспечения

достаточного уровня анонимности клиента в компьютерной системе;

− оценить эффективность предложенной модели, выявить ограничения и сформировать перспективы дальнейшего развития.

2. СОСТОЯНИЕ ИССЛЕДОВАНИЙ В ВЫБРАННОЙ ПРЕДМЕТНОЙ ОБЛАСТИ

На данном этапе следует провести аналитический обзор традиционных методов решения поставленной задачи. В настоящее время существует достаточно много методов обеспечения анонимности клиента, которые можно сгруппировать в несколько направлений: централизованные, гибридные, децентрализованные. Для оценки их эффективности сформируем группу критериев, по которым будет производиться сравнение. Успешный метод решения задачи, поставленной перед исследованием, должен выполнять следующие требования:

− высокий уровень анонимности клиента при отправке данных. Данный критерий оценивает эффективность того, что адресату невозможно было выявить источник сообщения;

− обеспечение конфиденциальности и целостности передаваемых данных. Данный критерий характеризует устойчивость к перехвату и модификации сообщений третьими лицами;

− устойчивость к намеренным атакам и неумышленным воздействиям. Данный критерий определяет устойчивость к вредоносным действиям злоумышленников и негативным событиям окружающей среды;

− удобство применения и кроссплатформенность. Данный критерий оценивает возможность широкого внедрения результатов;

− открытая архитектура необходима для выполнения принципа Керкгоффса [1], согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам криптоалгоритм должен быть открытым. Открытая архитектура позволяет всему мировому экспертному сообществу оценивать защищенность

метода, выявлять уязвимости и оперативно устранять их.

К первому направлению относятся централизованные решения, в архитектуре которых обязательным компонентом являются один или несколько центральных узлов, осуществляющих перенаправление сетевого траффика, скрытие реальных адресов и реквизитов клиента, координация всего множества узлов, сбор статистики и т.д.

Централизованные решения отличаются высокой скоростью работы, однако обладают невысокой надежностью, так как при выходе из строя центральных узлов функционирование всей системы становится невозможным. К таким решениям в частности относятся http-прокси-серверы, SOCKS-прокси-серверы, VPN-сервисы, SSH-туннели. Общая схема работы централизованного средства анонимизации представлена на рисунке 1.

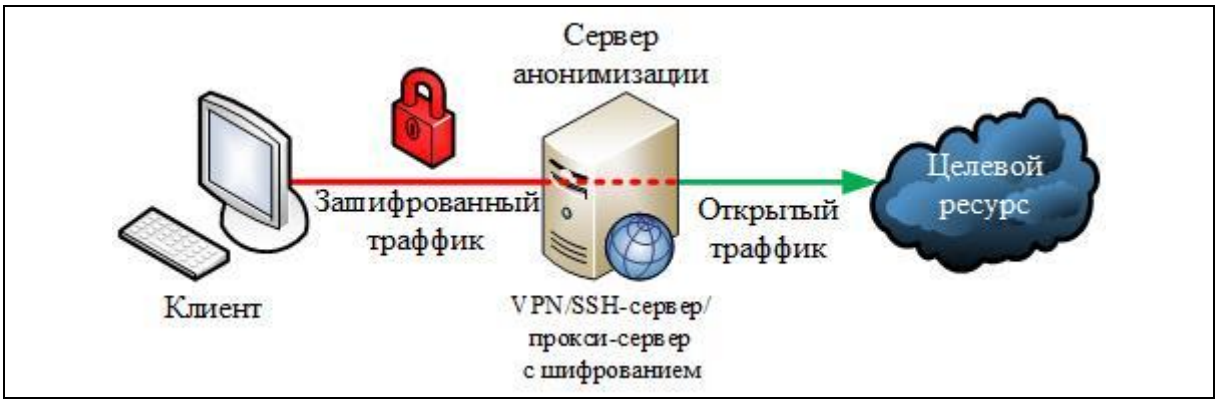

Рисунок 1. Централизованное средство анонимизации

Важной уязвимостью при обеспечении анонимности для данной группы методов является то, что клиент вынужден полностью доверять третьей стороне: анонимизирующему узлу. Также не обеспечивается конфиденциальность и целостность передаваемых данных, сетевой траффик может быть прослушан на сервере-посреднике, а в некоторых случаях – и на канале связи. Централизованные сервисы слабо могут противостоять как целенаправленным атакам, так и неумышленным воздействиям внешней среды, они имеют низкую отказоустойчивость, и при компрометации центральных узлов злоумышленник может нарушить

анонимность пользователя либо вывести всю систему из строя. Следовательно, использовать их как средство анонимизации пользователя в системах анонимного голосования не рекомендуется.

Рассмотрим второе направление методов. К нему относятся гибридные решения, в которых, помимо непосредственных механизмов анонимизации, существуют серверы, используемые для координации работы всей системы, предоставления статистических и иных данных. Гибридные решения, как правило, имеют высокую скорость, достаточную надежность и отказоустойчивость. При выходе из строя одного или нескольких таких узлов, сеть продолжит нормально функционировать. Одним из наиболее популярных, распространенных и безопасных гибридных решений является анонимная сеть Tor.

Основной принцип сети Tor основан на механизмах так называемой «луковой маршрутизации». Она заключается в том, что передаваемые сообщения последовательно шифруются открытыми ключами соответствующих узлов и отсылаются через несколько промежуточных «луковых» маршрутизаторов, в большинстве случаев цепочка состоит из трёх узлов [2]. Каждый маршрутизатор расшифровывает («снимает») слой шифрования, чтобы получить свои инструкции и отослать сообщения на следующий узел, где все повторяется.

Описанная схема гарантирует, что любой из узлов Tor не будет знать конечного адресата сообщения, его отправителя и содержимого одновременно. Общая схема работы гибридного средства анонимизации Tor представлена далее на рисунке 2.

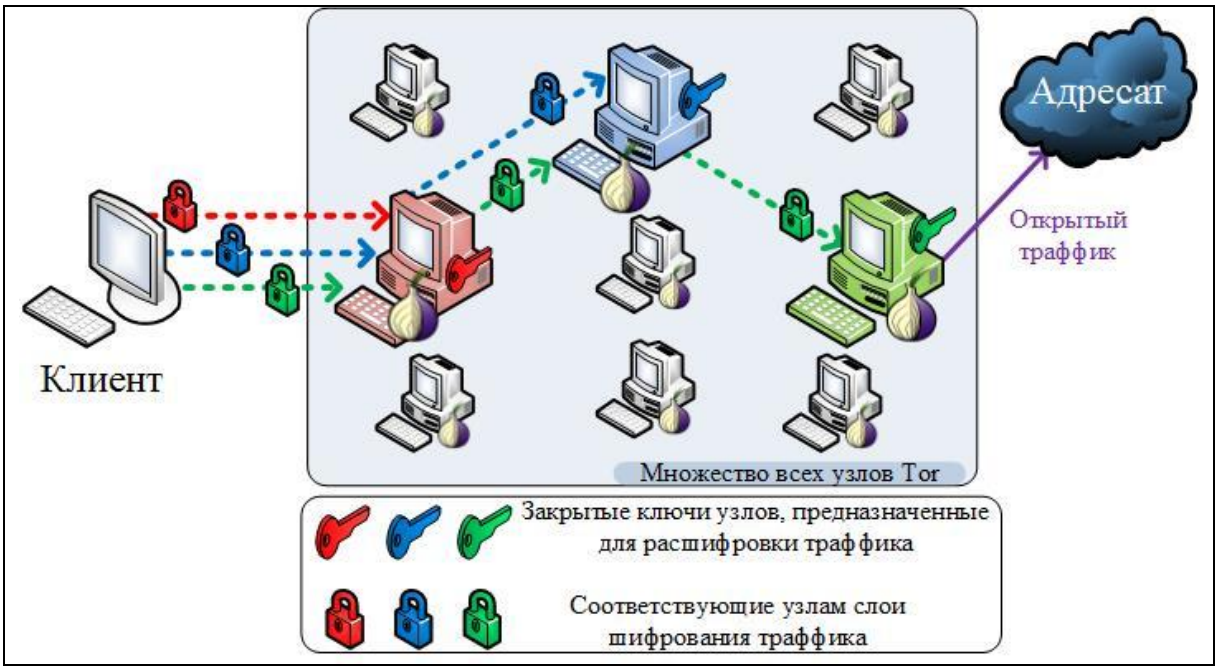

Рисунок 2. Гибридное средство анонимизации Tor

Стоит отметить, что наиболее высокую опасность при работе с Tor представляет тот факт, что злоумышленник может создать свои выходные узлы и прослушивать открытый траффик. В таком случае конфиденциальность и целостность передаваемых между клиентом и адресатом данных может быть обеспечена только при использовании двустороннего сквозного шифрования, например, протокола https. Сеть Tor активно развивается и предоставляет клиенту удобные программные средства для подключения к ней, а также обладает хорошей кроссплатформенностью. В настоящее время не выявлено практических эффективных атак, компрометирующих механизмы самой сети Tor. Следовательно, можно сделать вывод, что метод использования сети Tor для анонимизации передачи сообщений клиентом удовлетворяет критериям, поставленным перед аналитическим обзором, но только с условием обязательного сквозного шифрования траффика.

К третьему направлению методов относятся полностью децентрализованные решения, когда любой узел системы может установить соединение с другим узлом, передавать данные напрямую, выполняя при этом некоторые технические обслуживающие функции.

Следует отметить, что с ростом размера всей системы растёт и её надёжность, так как в системе начинают появляться узлы с одинаковыми функциями, что обеспечивает высокую отказоустойчивость. Наиболее популярным, быстро развивающимся и безопасным представителем таких решений является анонимная сеть I2P.

Сеть I2P (Invisible Internet Project) – это защищённая, полностью децентрализованная, анонимная сеть, работающая поверх обычного Интернета. Основными целями проекта I2P являются анонимное размещение различных ресурсов внутри сети и обеспечение анонимности пользователей при работе с ними. Каждый участник сети, запустивший у себя на компьютере клиент I2P, становится полноценным узлом сети.

Сеть I2P – основной проект, базирующийся на технологии так называемой «чесночной маршрутизации». Данная технология является развитием «луковой» маршрутизации, используемой в сети Tor. Чесночная технология использует многослойное последовательное шифрование. В один «чеснок» в момент его создания перед отправкой закладываются множество «зубчиков», являющихся зашифрованными сообщениями, как исходящего узла, так и чужими, транзитными, проходящими через этот узел. Является ли тот или иной «зубчик» в «чесноке» сообщением конкретного узла или это чужое транзитное сообщение, которое просто проходит через него, знает только тот, кто создал «чеснок» [3]. Сторонний наблюдатель узнать эту информацию не может. Когда сообщение проходит через узлы сети, каждый узел своим закрытым ключом «снимает» соответствующий ему слой шифрования и получает дальнейшие инструкции, что ему делать с данным сообщением: передать дальше или оставить себе.

Важно отметить, что в I2P применяется сквозное шифрование для защиты соединения между двумя клиентом и адресатом. Данная особенность позволяет обеспечить конфиденциальность и целостность

передаваемых данных между клиентом и адресатом.

Сеть I2P обеспечивает высокий уровень анонимности клиентов, серверов-точек назначения, а также конфиденциальность передаваемых между ними данных внутри сети. Также I2P имеет высокий уровень отказоустойчивости, и в настоящий момент не существует эффективных практических атак на механизмы самой сети. Можно сделать вывод, что метод использования сети I2P для анонимизации траффика удовлетворяет критериям, поставленным перед аналитическим обзором.

Важно отметить, что иные, намного менее популярные методы решения поставленной задачи, централизованные, гибридные, децентрализованные, в настоящий момент либо уже имеют критические уязвимости, либо не изучены в достаточной степени мировым экспертным сообществом, а, следовательно, их нельзя считать безопасными.

Также следует отметить, что в настоящее время любая из вышерассмотренных технологий не может предотвратить утечку от используемого клиентом программного обеспечения, так как по своей концепции она не может фильтровать весь пользовательский траффик. Многие приложения и протоколы изначально задумывались и проектировались не столько для обеспечения анонимности, сколько для получения доступа в сеть, обхода межсетевых экранов, прокси-серверов и пр. Некоторые приложения способны посылать сообщения напрямую в открытую сеть, в обход средств анонимизации, вызывая тем самым утечку деанонимизирующих данных. Следовательно, для устранения данных уязвимостей необходимо применение дополнительных средств.

В результате проведенного аналитического обзора выявлено, что для решения поставленной научной задачи, в частности, для обеспечения достаточного уровня анонимности отправителя электронных сообщений в распределённой компьютерной системе, наиболее подходит средство анонимизации I2P с применением некоторых дополнительных механизмов

безопасности, отвечающих за блокировку утечки деанонимизирующих данных пользовательских приложений и протоколов.

3. ПОСТАНОВКА И РЕШЕНИЕ ЗАДАЧИ

Для устранения выявленных уязвимостей и для обеспечения достаточного уровня анонимности отправителя электронных сообщений системе электронного голосования, необходимо модифицировать и дополнить метод использования механизмов анонимизирующей сети I2P. Для этого необходимо разработать схему фильтрации клиентского траффика с целью недопущения утечки деанонимизирующих данных в прикладных протоколах и приложениях. Также необходимо сформировать эффективный алгоритм взаимодействия клиента с системой анонимного голосования. Введём обозначения узлов системы, указанные в таблице 1.

Таблица 1 – ОБОЗНАЧЕНИЯ ОСНОВНЫХ ЭЛЕМЕНТОВ СИСТЕМЫ

Элемент системы	**Обозначение**
Открытый клиент	X
Анонимный клиент	AX
Открытый ключ клиента X	Ex
Закрытый ключ клиента X	Dx
Идентификационные данные клиента X	ПДx
Центр Регистрации	ЦР
Центр Сертификации	ЦС
Центр Анонимизации	ЦА
Сообщение M, подписанное клиентом X	Dx(h(M))
Сообщение M, зашифрованное открытым ключом клиента X	Ex(M)
Сообщение M, расшифрованное закрытым ключом клиента X	Dx(M)

Разработаем алгоритм работы системы анонимного голосования. Весь алгоритм делится на две части: открытую и анонимную. Центр сертификации, центр регистрации и центр анонимизации доверяют друг другу, при этом им всем доверяет открытый клиент.

Полная схема работы алгоритма указана на рисунке 3.

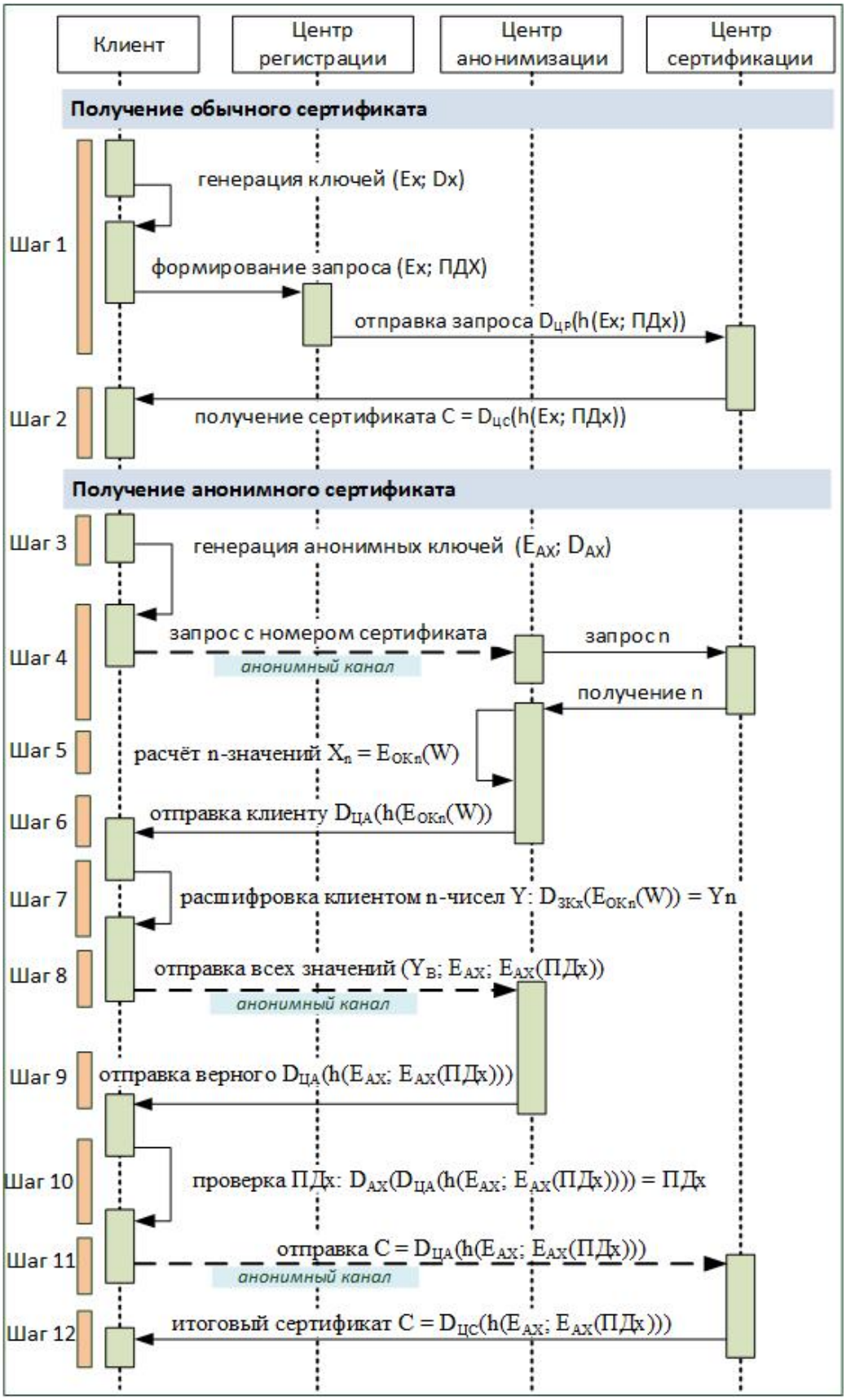

Рисунок 3. Схема работы алгоритма анонимного голосования

Рассмотрим открытую часть алгоритма.

Шаг 1. Сначала клиент X генерирует закрытый, Dx, и открытый, Ex, ключи клиента. Далее в центре регистрации клиент удостоверяет свою личность, там же формируется запрос на сертификат: (Ex; ПДx), включающий открытый ключ клиента и его персональные данные. Центр регистрации подписывает запрос на сертификат: $D_{ЦР}$(h(Ex; ПДx)), своим закрытым ключом и отправляет его в центр сертификации.

Шаг 2. ЦС, получив запрос, проверяет подпись ЦР, подписывает запрос своим ключом, формирует сертификат: C = $D_{ЦС}$(h(Ex; ПДx)), и передает его клиенту. Сертификат подтверждает действительность закрытого ключа клиента и подлинность клиента. Клиент с помощью своего закрытого ключа подписывает сообщение и отправляет его адресату вместе со своим сертификатом. Адресат с помощью сертификата проверяет подпись на документе.

Сертификат и закрытый ключ клиента записываются на защищенный носитель: смарт-карту или USB-ключ, при этом используется первый цикл перезаписи. Данный носитель по своим характеристикам может хранить в себе только две пары ключей и имеет фиксированное число циклов перезаписи, равное 4.

Далее рассмотрим анонимную часть алгоритма.

Шаг 3. Клиент генерирует свои анонимные ключи, вычисляя значение хеш-функции от своего закрытого ключа, получая закрытый анонимный ключ, D_{AX}, далее он вычисляет открытый анонимный ключ, E_{AX}. Анонимные ключи записываются на защищенный накопитель клиента, который на данном шаге оказывается полностью заполненным, при этом проходит второй цикл перезаписи.

Шаг 4. Далее клиент через анонимный канал I2P делает запрос в центр анонимизации, указывая порядковый номер своего открытого сертификата с обнуленными последними цифрами. ЦА запрашивает у ЦС все подходящие сертификаты и получает n-сертификатов.

Шаг 5. ЦА генерирует случайное число W, далее ЦА шифрует число

W n-раз открытыми ключами n-клиентов и получает n-чисел: X_1, X_2, X_n.

Шаг 6. ЦА подписывает все эти числа и отправляет клиенту обратно.

Шаг 7. Клиент проверяет подпись ЦА своим ЗКх, всё расшифровывает и получает n-чисел Y, при этом одно из них, Yв – верное. Клиент не догадывается, какое верное W было сгенерировано ЦА, об этом знает только сам ЦА.

Шаг 8. Клиент через анонимный канал делает запрос в ЦА со всеми получившимися n-значениями. В запрос входят следующие данные:

- число Y_1, Y_2, Y_n, Y_B;
- открытый анонимный ключ клиента (E_{AX});
- зашифрованные ПДн клиента E_{AX}(ПДх).

Шаг 9. ЦА проверяет уникальность открытого анонимного ключа клиента и ищет в сообщении верное значение $W = Y_B$. Если находит, то ЦА подписывает своей подписью это сообщение, $D_{ЦА}(h(E_{AX}; E_{AX}(ПДх)))$, и отправляет его назад клиенту. Само число Y больше не нужно, оно отбрасывается.

Шаг 10. Клиент проверяет подпись ЦА, расшифровывает полученный запрос своим закрытым ключом, проверяет свои ПДх, равные $D_{AX}(D_{ЦА}(h(E_{AX}; E_{AX}(ПДх))))$, и получает анонимный сертификат: $C=D_{ЦА}(h(E_{AX}; E_{AX}(ПДх)))$, подписанный ЦА. Сертификат записывается взамен анонимного открытого ключа на защищенный носитель, тратя еще один, третий, цикл перезаписи.

Шаг 11. Клиент по анонимному каналу отправляет свой анонимный сертификат в ЦС, где проверяется подпись ЦА, далее ЦС ставит свою подпись на данном сертификате и возвращает его клиенту. Итоговый анонимный сертификат, $D_{ЦС}(h(E_{AX}; E_{AX}(ПДх)))$, записывается на защищенный носитель, при этом тратится четвертый, последний, цикл записи. Защищенный носитель заполняется, все циклы перезаписи использованы, далее ключевой носитель не позволяет проводить с собой какие-либо операции перезаписи.

В итоге было введено понятие «анонимного сертификата», подписанного легитимным центром сертификации. При этом данный сертификат обладает всем свойствами классического сертификата открытого ключа, при этом ни центр анонимизации, ни центр сертификации не знают персональных данных клиента. Также достигаются следующие преимущества:

- упрощается протокол анонимного голосования;
- становится возможным использование стандартных схем инфраструктуры открытых ключей;
- схема с «анонимным сертификатом» может быть реализована на сертифицированных криптографических стандартах ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- появляются дополнительные возможности: многократные проверки наличия подписи, переголосование, отзыв голоса и др.

Далее рассмотрим способы решения задачи недопущения утечки деанонимизирующих данных в клиентском траффике для прикладных протоколов и приложений. В качестве основного решения предлагается схема, при которой используется две виртуальные машины, одна из которых является шлюзом, цель которого – отправлять весь траффик только через анонимную сеть. А другая машина является изолированной рабочей станцией клиента, подключающейся только к шлюзу. Таким образом, любые запросы клиентских приложений и протоколов направляются только на шлюз, который физически не может отправить их по какому-либо каналу связи, кроме анонимного, через сеть I2P. Таким образом, реализуется концепция изолирующего прокси-сервера. Так как рабочая станция не знает свой внешний ip-адрес в Интернете, это позволяет нейтрализовать множество уязвимостей, например, даже если

вредоносная программа получит административный доступ к рабочей станции, у него не будет возможности узнать реальный ip-адрес клиента. В результате созданный в ходе исследования программный инструментарий, реализующий математическую модель, позволяет обеспечить анонимность клиента в системе электронного голосования в частности, а также и обеспечить достаточный уровень анонимности отправителя электронных сообщений в распределённой компьютерной системе в целом.

4. ВНЕДРЕНИЕ И ОЦЕНКА ЭФФЕКТИВНОСТИ

Предложенная технология имеет некоторые ограничения на пути использования её в современных условиях. К данным сложностям можно отнести высокую коммуникационную сложность системы, а также некоторые организационные и технические сложности, связанные с тем, что для систем электронного голосования необходимо наладить функционирование инфраструктуры открытых ключей для каждого клиента. В масштабах всего государства, для использования данной технологии в федеральных выборных мероприятиях необходимо внедрить персонализированные ключи электронной подписи, создать необходимую программно-аппаратную базу, провести несколько этапов тестирования с привлечением экспертного сообщества. Результаты данного исследования, помимо решения поставленной задачи, применимы также и для других областей, в частности, разработанная математическая модель имеет перспективы для практической реализации в виде систем автоматического цензурирования и преодоления цензуры, а также методологий расследования инцидентов информационной безопасности.

Предложенная математическая модель эффективно решает поставленную задачу, так как объединяет в себе методы, проверенные мировым сообществом и не имеющие доказанных уязвимостей, ведущих к теоретической компрометации. Оценить экономическую эффективность на данный момент не представляется возможным в виду неподготовленности в Российской Федерации необходимых условий для внедрения

практической системы электронного анонимного голосования. Разработанная технология имеет перспективы дальнейшего развития, связанные с внедрением системы на различных уровнях: муниципальном, региональном, федеральном, а также реализацию её в виде отдельного коммерческого продукта, реализующего систему анонимного электронного голосования.

5. ЗАКЛЮЧЕНИЕ

В результате проведенного исследования были выполнены работы, позволяющие получить решение поставленных перед исследованием задач. В частности, был проведен аналитический обзор традиционных методов и средств обеспечения анонимности в компьютерных сетях. Были сформированы критерии обеспечения эффективного уровня анонимности, по которым было проведено аналитическое исследование и сравнение существующих подходов к решению задачи. Были рассмотрены централизованные, гибридные и децентрализованные решения. В итоге методом, удовлетворяющим всем поставленным критериям, был признан метод использования механизмов анонимизирующей сети I2P.

На следующем этапе исследования были рассмотрены возможные уязвимости анонимности клиента при передаче сообщений в компьютерных сетях, а также угрозы конфиденциальности и целостности передаваемых им сообщений. Было выявлено, что угрозу может представлять утечка деанонимизирующих данных через различные пользовательские приложения и протоколы. Для предотвращения этого была разработана идея, заключающаяся в том, что в системах анонимного электронного голосования необходимо применение эффективных централизованных и клиентских анонимизирующих механизмов, обеспечивающих высокий уровень безопасности клиента. Ранее в протоколах электронных голосований данным механизмам не уделялось достаточного внимания. Было введено понятие: «анонимный сертификат». Введение анонимного сертификата позволяет достичь приватность

персональных данных клиента и при этом обеспечить его аутентификацию. Далее была разработана математическая модель, реализующая алгоритм получения анонимного сертификата для дальнейшего электронного голосования.

Следовательно, подход, предложенный в статье для решения поставленной задачи, является эффективным по всем обоснованным критериям и перспективным с точки зрения дальнейшего развития и внедрения. Значит, главная цель исследования, создание математической модели обеспечения достаточного уровня анонимности для отправителя электронных сообщений в распределённой компьютерной системе, реализующей механизмы электронного голосования с сохранением целостности и конфиденциальности передаваемых данных, была успешно достигнута. Результаты, полученные в ходе исследования, способны оказать значительное влияние как на развитие практических систем обеспечения анонимности и деанонимизации, так и для решения важной научной проблемы – обеспечения математически доказуемой абсолютной анонимности субъекта при взаимодействии его с адресатом.

Литература

1. Шнайер Б. Прикладная криптография (Applied Cryptography). – М.: Триумф, 2002. 816 с.
2. Tor: The Second-Generation Onion Router: https://svn.torproject.org/svn/projects/design-paper/tor-design.html
3. Invisible Internet Project (I2P) Project Overview: http://www.i2p2.de/_static/pdf/i2p_philosophy.pdf.

References

1. Shnajer B. Prikladnaja kriptografija (Applied Cryptography). – M.: Triumf, 2002. 816 s.
2. Tor: The Second-Generation Onion Router: https://svn.torproject.org/svn/projects/design-paper/tor-design.html
3. Invisible Internet Project (I2P) Project Overview: http://www.i2p2.de/_static/pdf/i2p_philosophy.pdf.