ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.42, 004.056

ОСОБЕННОСТИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ ПРОТОКОЛА ТАЙНОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ФУДЗИОКА – ОКАМОТО – ОХТА

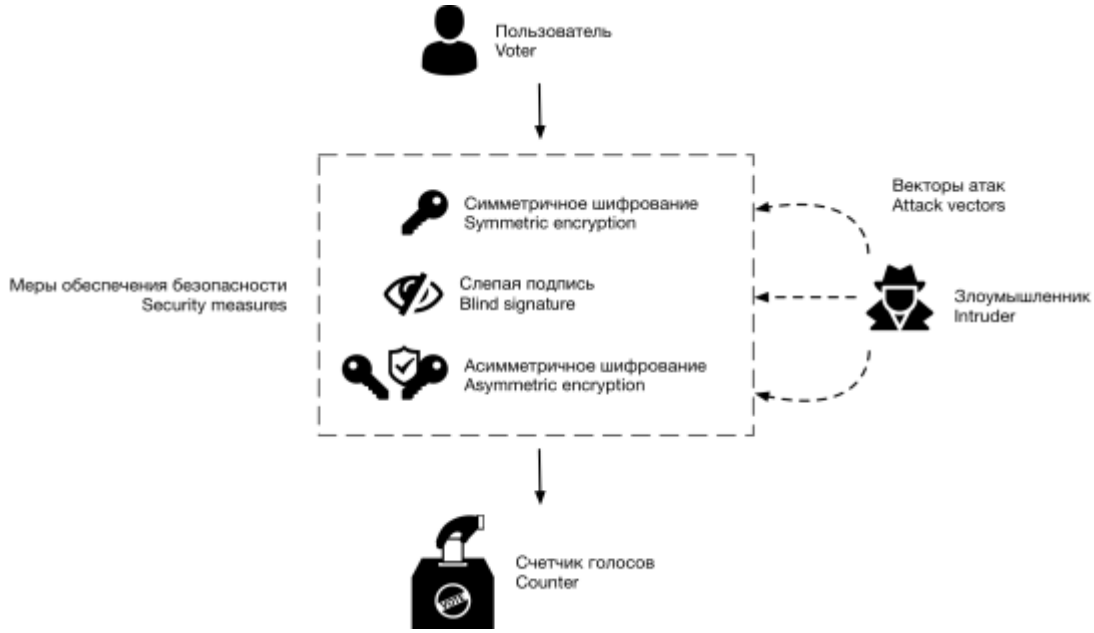
Статья поступила в редакцию 15.05.2019, в окончательном варианте – 28.05.2019.

Чернухин Дмитрий Алексеевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, Татищева, 20а,
магистрант, e-mail: madlabman@mail.ru
Ажмухамедов Искандар Маратович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, Татищева, 20а,
доктор технических наук, профессор, заведующий кафедрой информационной безопасности, e-mail: iskander_agm@mail.ru

Рассмотрен протокол тайного электронного голосования Фудзиока – Окамото – Охта с точки зрения практической реализация. Приведена формализация протокола в виде математической модели и диаграммы последовательностей в нотации UML. Даны рекомендации по выбору отдельных элементов практической реализации информационной системы. Приведены критерии выбора алгоритмов симметричного и асимметричного шифрования в протоколе. Рассмотрены границы практической применимости алгоритма «слепой» подписи на основе криптосистемы RSA. Приведены используемые на практике релевантные информационной системе уникальные идентификаторы пользователей и критерии для их выбора. Предложены варианты выбора структуры бюллетеня и их оценка по критериям удобства и безопасности использования. Дана оценка практической реализации информационной системы с точки зрения информационной безопасности. Рассмотрены отдельные векторы атак, в том числе атаки на бюллетень, «слепую» подпись, хэш-функцию и канал передачи информации.

Ключевые слова: протокол тайного электронного голосования, слепая подпись, практическая реализация, информационная безопасность

Графическая аннотация (Graphical annotation)



SPECIFIC FEATURES OF THE FUJIOKA ET AL. ELECTRONIC VOTING SCHEME REAL-WORLD IMPLEMENTATION

The article was received by the editorial board on 15.05.2019, in the final version – 28.05.2019.

Chernukhin Dmitrii A., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

graduate student, e-mail: madlabman@mail.ru

Azhmukhamedov Iskandar M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

Doct. Sci. (Engineering), Professor, Head of the Department of Information Security, e-mail: iskander_agm@mail.ru

The protocol of Fujioka – Okamoto – Ohta secret electronic voting from the standpoint of practical realisation is considered. Formalisation of the protocol is presented as mathematical model and sequence diagramm in UML notation. Recommendations are given at option of separate elements of practical realisation of information system. The criteria of choice of algorithms of symmetric and asymmetric encryption in the protocol are presented. The boundaries of practicality of algorithm of "blind" signature on the basis of RSA crypto-system are considered. Practically useful and relevant to the information system examples of unique identifiers of the users and criteria for their choice are given. Variants of choice of the structure of bulletin and their evaluation on the criteria of convenience and safety of use are offered. The evaluation of practical realisation of information system from the standpoint of information safety are given. Different attack vectors are examined including attack to bulletin, «blind» signature, hash-function and transmission channel.

Keywords: secure election scheme, blind signature, practical realisation, information security

Введение. Криптографическими методами могут быть обеспечены следующие сервисы информационной безопасности: конфиденциальность – с помощью шифрования, целостность (путём использования хэш-функций), аутентичность и неотказуемость – за счет применения протоколов электронной цифровой подписи [2]. Обычно данные сервисы реализуются таким образом, что не требуется вмешательства пользователя; обеспечивается защищённый доступ к информационным ресурсам. В том числе предоставляется возможность сохранения анонимности в тех случаях, когда она является необходимым условием осуществления взаимодействия с информационной системой (ИС). Ярким примером подобной ИС является система тайного электронного голосования, подразумевающая сокрытие личности участника процесса при возможности удостоверения в легитимности полученного от него голоса. Для реализации подобных информационных систем были разработаны различные протоколы, обладающие следующими, необходимыми для голосования свойствами:

- все голоса должны быть учтены верно;
- недобросовестный участник не способен нарушить ход голосования;
- все голоса должны быть учтены конфиденциально;
- никто не может проголосовать дважды;
- могут голосовать только допущенные к голосованию лица;
- внешние факторы не влияют на процедуру голосования;
- никто не может повлиять на результаты голосования.

Наиболее известным представителем семейства протоколов, отвечающих приведённым требованиям, является протокол на основе слепой подписи Фудзиока – Окамото – Охта. Данный протокол является детально описанным, хорошо изученным с теоретической точки зрения и отличается своей простотой, что делает его особенно привлекательным для практического использования. Тем не менее широкого распространения протокол не получил в силу ограничений, связанных с его практической реализацией. Таким образом, ***целью данной работы*** является предложить меры устранения препятствий практической реализации протокола тайного электронного голосования Фудзиока – Окамото – Охта [4]. Для достижения данной цели необходимо ***решить следующие задачи***:

- построить математическую модель протокола Фудзиока – Окамото – Охта;
- описать практическую реализацию протокола и ее особенности;
- дать оценку практической реализации с точки зрения информационной безопасности.

Математическая модель протокола. Протокол включает в себя трёх акторов: избирателя (И), регистратора (Р), счётчика (С). При этом каждый из акторов выполняет ряд действий на различных шагах выполнения протокола. Графическое представление в виде диаграммы последовательностей приведено на рисунке.

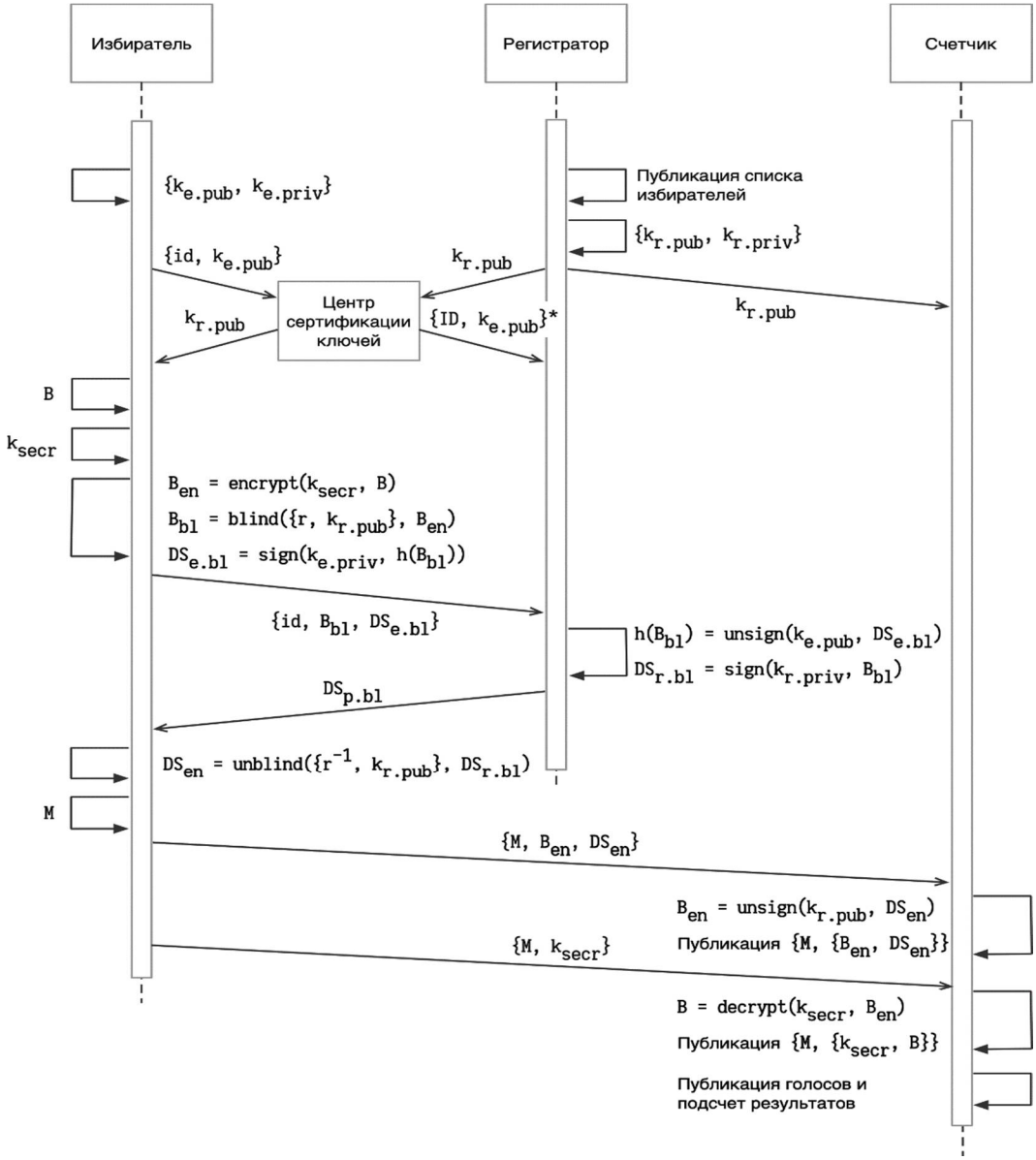


Рисунок – Диаграмма последовательностей протокола Фудзиоко – Окамото – Охта

Формализация действий, приведенных на диаграмме, приведена ниже:

1. Регистратор:

а) публикует список всех правомочных избирателей;

б) создаёт пару ключей для асимметричного шифрования $\{k_{r.pub}, k_{r.priv}\}$;

в) публикует открытый ключ $k_{r.pub}$ в центре сертификации ключей (ЦСК). ЦСК может

г) быть независимой организацией или подчиняться регистратору.

2. Избиратель:

а) создаёт пару ключей для асимметричного шифрования $\{k_{e.pub}, k_{e.priv}\}$ и публикует свой открытый ключ в ЦСК. Публикация ключа подразумевает регистрацию конкретного избирателя с присвоенным ему уникальным идентификатором *id*;

б) создаёт секретный ключ для симметричного шифрования k_{secr};

в) делает свой выбор в бюллетене B;

г) с помощью секретного ключа k_{secr} зашифровывает бюллетень $B_{en} = encrypt(k_{secr}, B)$;

д) с помощью «маскирующего» множителя r и открытого ключа регистратора $k_{r.pub}$ скрывает содержимое зашифрованного бюллетеня $B_{bl} = blind(\{r, k_{r.pub}\}, B_{en})$;

е) с помощью своего закрытого ключа $k_{e.priv}$ подписывает хэш-образ зашифрованного бюллетеня $DS_{e.bl} = sign(k_{e.priv}, h(B_{bl}))$;

ж) посылает регистратору свой идентификатор *id*, скрытый зашифрованный бюллетень B_{bl} и электронно-цифровую подпись (ЭЦП) к нему $DS_{e.bl}$.

3. Регистратор:

а) проверяет ЭЦП с помощью открытого ключа избирателя $h(B_{bl}) = unsingn(k_{e.pub}, DS_{e.bl})$;

б) с помощью своего закрытого ключа подписывает скрытый зашифрованный бюллетень $DS_{r.bl} = sign(k_{r.priv}, B_{bl})$;

в) посылает избирателю «слепую» ЭЦП $DS_{r.bl}$.

4. Избиратель:

а) снимает «маскирующий» множитель *r* со слепой ЭЦП регистратора и получает ЭЦП регистратора $DS_{en} = unblind(\{r^{-1}, k_{r.pub}\})$ к открытому зашифрованному бюллетеню B_{en};

б) генерирует уникальную метку *M*;

в) анонимно посылает счетчику свою метку *M*, зашифрованный бюллетень B_{en} и ЭЦП регистратора DS_{en}.

5. Счетчик:

а) с помощью открытого ключа регистратора проверяет ЭЦП к зашифрованному бюллетеню $B_{en} = unsign(k_{r.pub}, DS_{en})$;

б) по истечении времени, отведенного на голосование, публикует все метки *M* и зашифрованные бюллетени с ЭЦП к ним $\{B_{en}, DS_{en}\}$ в доказательство избирателю, что его голос принят.

6. Избиратель:

1) анонимно посылает счетчику секретный ключ k_{secr} для метки *M*.

7. Счетчик:

а) расшифровывает бюллетень $B = decrypt(k_{secr}, B_{en})$;

б) в дополнение к $\{M,\{B_{en},DS_{en}\}\}$ публикует $\{M,\{k_{secr},B\}\}$ для того, чтобы избиратель убедился в правильности учета его голоса;

в) подводит подсчет голосов и публикует результаты голосования.

Приведенная математическая модель отражает отдельные этапы протокола с точки зрения теории и позволяет перейти к описанию особенностей реализации протокола на практике.

Особенности практической реализации. Особенности, связанные с выбором основных элементов практической реализации информационной системы электронного голосования, приведены ниже.

Идентификатор пользователя. Как отмечено в пункте 2а, пользователь должен передать свой открытый ключ и связанный с ним идентификатор, позволяющий однозначно определить личность представителя ключа. Данный идентификатор необходим для проверки легитимности голоса и контроля за повторным голосованием. Протокол не предлагает определенной процедуры генерации и распределения идентификаторов между пользователями информационной системы. Возможные реализации данного элемента приведены ниже.

Задача идентификации личности пользователя в большинстве случаев является обязательным условием для многопользовательских информационных систем. Наиболее распространенная стратегия решения данного вопроса – передача данной задачи доверенной третьей стороне. На практике превалирующим вариантом является идентификация личности посредством подтверждения факта владения идентификационным модулем абонента в сотовых сетях (SIM-карта). SIM-карта предоставляется пользователю провайдером услуг связи, обязанностью которого является связать персональные данные пользователя с предоставляемым ему уникальным номером, используемым для идентификации абонента в сетях сотовой связи. Данная схема идентификации является двухфакторной, поскольку позволяет подтвердить личность пользователя посредством двух факторов:

- фактора знания уникального идентификатора, связанного с пользователем;
- фактора владения, подтверждаемого предоставлением одноразового пароля, отправляемого пользователю посредством сетей сотовой связи.

Другим примером идентификатора для информационной системы может выступать идентификатор пользователя в какой-либо иной доверенной информационной системе, например, такой как Федеральная миграционная служба, предоставляющая пользователю уникальные значения серии и номера выдаваемого соответствующей организацией документа – пас-

порта гражданина Российской Федерации. В данном случае сторонняя информационная система берет обязанности по идентификации пользователя и передает конечную информацию целевой информационной системе.

При отсутствии возможности использования третьей стороны для решения задачи идентификации пользователя возможным является генерация собственного типа идентификатора и его распределения между всеми легитимными пользователями.

В качестве рекомендуемого варианта реализации идентификатора предлагается к использованию схема с использованием модулей идентификации абонента в сотовых сетях.

Алгоритм симметричного шифрования. На этапе 2г перед пользователем стоит задача зашифровать сформированный бюллетень с помощью алгоритма симметричного шифрования. Наиболее распространенными алгоритмами симметричного шифрования являются алгоритмы на основе SP-сетей (подстановочно-перестановочных сетей). Подобные алгоритмы используют предварительно рассчитанные таблицы замены байтов в совокупности с несколькими раундами соответствующих замен, что позволяет получить важное свойство, заключающееся в изменение всех битов выходной последовательности при изменении одного бита информации, поступающей на вход. Также распространенность данных алгоритмов обусловлена простотой и эффективностью реализаций непосредственно на аппаратном обеспечении, которые значительно превосходят по производительности программные решения. Самым известным среди подобных алгоритмов является Advanced Encryption Standard (AES), также известный как Rijndael – симметричный алгоритм блочного шифрования, работающий с блоками размером по 128 бит и с ключом размером 128, 192 или 256 бит [5]. Альтернативой AES может служить блочный шифр «Кузнечик», разработанный Центром защиты информации и специальной связи ФСБ России. Данный алгоритм также работает с блоками размером 128 бит, но с фиксированной длиной ключа в 256 бит. В случае применения блочных симметричных алгоритмов шифрования в настоящее время, как отмечено в [1], 256 бит является достаточной длиной ключа для сохранения устойчивости шифра. В практических реализациях протокола выбор алгоритма шифрования не является критичным, достаточно соблюдения устойчивости к взлому и оптимальной производительности при работе как на устройстве участника голосования, так и на устройстве счетчика голосов. Тем не менее размер блока, используемый алгоритмом для шифрования, может повлиять на особенности реализации бюллетеня.

Таким образом, в качестве алгоритма симметричного шифрования предлагается использовать AES в силу приведенных выше преимуществ.

Бюллетень. Протокол требует формирования бюллетеня с выбором пользователя. Протокол не предъявляет никаких требований к выбору структуры бюллетеня. Таким образом, на практике стоит вопрос, какая структура данных оптимальна для его представления. Форматы представления данных делятся на две основные группы: человекочитаемые и бинарные [3]. В первом случае бюллетень является битовой последовательностью, которую можно представить в виде символьной информации, воспринимаемой человеком. В случае бинарного формата представления, бюллетень является упорядоченной структурированной последовательностью битов. В практической реализации возможно использование любого из представленных вариантов, при условии соблюдения следующего требования: информационная система должна контролировать структуру бюллетеня и отказывать в учете бюллетеней со структурой, отличной от объявленной. Данной требование позволяет ограничить потенциального злоумышленника в возможности манипулирования данными в бюллетене при проведении атаки на хэш-функцию, значительно сократив возможное число вариантов для прямого перебора. В соответствии с приведенным требованием, также следует обратить внимание на выравнивание размера данных в бюллетене под размер блока, используемого алгоритмом шифрования, что также позволит минимизировать количество информации, доступной в бюллетене для модификации.

Уникальная метка пользователя. При генерации метки возникает проблема проверки уникальности данного идентификатора без центра координации, который может стать потенциальным источником компрометации или дать злоумышленнику дополнительную информацию, указав на существование сгенерированной ранее метки до ее фактической публикации. Для генерации уникальных идентификаторов для распределенных систем существует стандарт идентификации UUID (universally unique identifier – «универсальный уникальный идентификатор»). Данный стандарт позволяет пользователю сгенерировать идентификатор с приемлемой для конкретной информационной системы вероятностью коллизии. Стандарт предоставляет несколько версий реализации, наиболее подходящим для системы электронного голосования

является UUID 3 или 5, действующих аналогичным образом, получая идентификатор из двух входных значений: идентификатора пространства имен («namespace»), также представляющий собой UUID, и некоего строкового значения. Отличие версии 3 от 5 заключается в используемой функции хеширования – MD5 для 3 версии и SHA-1 для 5. Таким образом, на вход функции генерации UUID 3/5 в практической реализации возможно подать сгенерированное UUID 4 значение, которое формируется на основе генератора псевдослучайных чисел, и некоего уникального идентификатора пользователя. Данная схема является безопасной с точки зрения возможности восстановления входных значений в силу использования хэш-функции при генерации значения и рекомендуется для практической реализации протокола.

Алгоритм шифрования с открытым ключом. На шаге 2а избиратель генерирует ключи для асимметричного шифрования [9]. Выбор алгоритма шифрования распространяется на всю информационную систему. Наиболее распространенные криптографические алгоритмы с открытым ключом основываются на вычислительной сложности задачи факторизации произведения больших простых целых чисел. Криптографические системы с открытым ключом используют так называемые односторонние функции, которые обладают следующими свойствами:

- если известно x, то вычислить $f(x)$ относительно просто;
- если известно $y = f(x)$, то для вычисления x нет простого (эффективного) пути.

Под односторонностью понимается практическая невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени. Наибольшее распространение на практике получил алгоритм RSA [10], находящий применение в электронной цифровой подписи, шифровании данных пользователя, установке защищенного соединения и аутентификации пользователя. Также стоит отметить, что данный алгоритм является возможным для применения схемы слепой подписи, необходимой для реализуемого протокола.

Слепая подпись. Дэвидом Чаумом было введено понятие слепой подписи [6] и предложен широко известный алгоритм на основе криптосистемы RSA:

- Боб выступает в качестве нотариуса и предоставляет свой открытый ключ (p, e), где p – модуль открытого ключа, e – публичная экспонента;
- Алиса выбирает случайный маскирующий множитель r, взаимно простой с p, и вычисляет $m' \equiv m \times r^e \bmod p$;
- Алиса отправляет Бобу m';
- Боб вычисляет $s' \equiv (m')^d \bmod p$, где d – приватная экспонента;
- Боб отправляет подписанное сообщение Алисе;
- Алиса снимает маскирующий множитель и получает исходное сообщение m, подписанное Бобом: $s \equiv s' \times r^{-1} \bmod p \equiv m^d \bmod p$.

Стоит отметить, что данная схема применима исключительно при условии коммутативности операций подписи и маскировки сообщения. Приведенная схема RSA на практике не допускается к использованию по причине того, что она не является *практически надежной*, так как функция подписи в данном случае является детерминированной, то есть при одних и тех же входных значениях приводит к одинаковому результату. Для практических реализаций принято использовать схемы «дополнения», так что исходное сообщение M расширяется и приводится к подобному виду [10]:

0x00	0x02	PS	0x00	M,

где первые два октета являются контрольными; PS – псевдослучайная последовательность битов. Математически упрощенно операцию расширения можно представить в следующем виде:

$$M' = l + M;\ l > 2^{log_2 M}.$$

Очевидно, что расширенное сообщение становится непригодным для применения в схеме слепой подписи из-за нарушения свойства коммутативности, в результате чего процедура снятия маскирующего множителя приведет к невозможности проверить цифровую подпись. Таким образом, в практической реализации требуется игнорировать стандарт PKCS, что приводит к необходимости дать оценку данного решения с точки зрения информационной безопасности.

Оценка практической реализации с точки зрения информационной безопасности. При использовании приведенных ранее практических реализаций отдельных элементов протокола возможны следующие атаки на информационную систему.

Атака на канал передачи информации. Очевидно, что передача информации между компонентами информационной системы требует отдельного рассмотрения. В протоколе не приводится требований к каналу передачи информации, тем не менее отмечается, что канал должен быть *защищенным*. Данное требование является очевидным для большинства информационных систем, и в особенности для системы тайного электронного голосования. При атаке на систему голосования злоумышленник может преследовать одну или несколько из приведенных целей:

- раскрыть личность голосующего и связать его с конкретным бюллетенем;
- проголосовать от имени другого пользователя;
- раскрыть бюллетень пользователя до принятия голоса с целью повлиять на итоговый результат голосования.

Данные векторы атак в случае их реализации нарушают приведенные ранее требования к информационной системе электронного голосования. Общепринятой реализацией безопасного канала передачи информации является канал на основе протокола HTTPS. Тем не менее данный протокол не защищен от атак, связанных с перехватом информации при условии предварительной подготовки злоумышленником сетевой инфраструктуры, которую используют участники голосования для доступа к информационной системе. Таким образом, при оценке защищенности информационной системы следует предполагать, что злоумышленнику могут быть доступны все данные, передаваемые по сети между участником голосования и частями информационной системы.

Атака на зашифрованный бюллетень. Использование современных блочных шифров с длиной ключа в 256 бит позволяют надежно сокрыть информацию в большинстве случаев. Атака методом перебора на ключ указанной длины является неэффективной и по различным оценкам на настоящий момент может занять до $3{,}31 \times 10^{56}$ лет, что однозначно превышает сроки актуальности сокрытой информации. Тем не менее разрабатываются атаки на алгоритмы шифрования, связанные с архитектурными недостатками данных алгоритмов или особенностей их применения в программном или аппаратном обеспечении. Так, для алгоритма шифрования AES может быть использована уязвимость, позволяющая получить ключ шифрования путем анализа тактов центрального процессора вычислительной машины, используемой для шифрования данных. Тем не менее данный способ требует не только удаленного или физического привилегированного доступа к аппаратной системе, но и предварительно подготовленной программной закладки, что позволяет судить о крайне низкой вероятности реализации данного вектора атаки.

Атака на слепую подпись. Так как в основе алгоритма слепой подписи лежит один из алгоритмов асимметричного шифрования, уязвимости выбранного алгоритма непосредственно отразятся на применимости алгоритма слепой подписи. Как было отмечено ранее, RSA не используется на практике без схем «дополнения» из-за свойства детерминированности наивной реализации, позволяющей злоумышленнику изменять расшифрованные данные на основе известного шифротекста предсказуемым образом. Например, имея шифротекст c, который получен из сообщения m, злоумышленник может вычислить: $c' = c \times 2^e \bmod n$, при расшифровании которого пользователь получит значение $2m$. Тем не менее в алгоритме слепой подписи алгоритм симметричного шифрования применяется для проверки электронной цифровой подписи, осуществляя шифрование данных не открытым ключом пользователя, а секретным, при том, что открытый текст не является секретной информацией и, напротив, используется для контроля за целостностью и источником предоставляемой информации. Таким образом, применение простой схемы RSA или подобного ему алгоритма без использования схем «дополнения» являются допустимым, так как не приводит к раскрытию шифротекста.

Заключение. Таким образом, рассмотрение математической модели, вариантов реализации элементов протокола и его оценка с точки зрения информационной безопасности позволяет перейти непосредственно к практической реализации протокола в виде программного обеспечения для электронно-вычислительных машин.

Библиографический список

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – Москва : Триумф, 2002. – 815 с.

2. Мао В. Современная криптография. Теория и практика / В. Мао. – Москва : Вильямс, 2005. – 763 с.

3. Шаньгин В. Ф. Защита в компьютерных системах и сетях / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2012. – 592 с.

4. Fujioka A. A practical secret voting scheme for large scale election / A. Fujioka, T. Okamoto and K. Ohta // Advances in Cryptology-Auscrypt'92, LNCS 718. – Springer-Verlag, 1992. – P. 244–260.

5. Announcing the Advanced Encryption Standard (AES). – Federal Information Processing Standards Publication 197, 2001.

6. Chaum D. Blind signatures for untraceable payments / D. Chaum // Proceedings of Crypto 82. – New York : Plenum Press, 1983. – P. 199–203.

7. Nurmi H. Secret ballot elections in computer networks / H. Nurmi, A. Salomaa, L. Santean // Computers and Security. – 1991. – Vol. 36, № 10. – P. 553–560.

8. RFC 2818 HTTP over TLS. – 2000.

9. Rivest R. L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems / R. L. Rivest, A. Shamir, L. M. Adleman Communications of the ACM. – 1978. – Vol. 21, № 2. – P. 120–126.

10. RSA Laboratories. PKCS #1 v2.2: RSA Cryptography Standard. – 2012.

11. Shamir A. Comm. of the ACM / A. Shamir. – 1979. – Vol. 22. – P. 612.

References

1. Shnayer. B. *Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si* [Applied Cryptography. Protocols, algorithms, sources in C++]. Moscow, Triumf Publ., 2002. 815 p.

2. Mao V. *Sovremennaya kriptografiya. Teoriya i praktika* [Modern cryptography. Theory and practice]. Moscow, Vilyams Publ., 2005. 763 p.

3. Shangin V. F. *Zashchita v kompyuternykh sistemakh i setyakh* [Security in computer systems and networks]. Moscow, DMK Press Publ., 2012. 592 p.

4. Fujioka A., Okamoto T. and Ohta K. A practical secret voting scheme for large scale election. *Advances in Cryptology-Auscrypt'92, LNCS 718*. Springer-Verlag, 1992, pp. 244–260.

5. *Announcing the Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197, 2001.

6. Chaum D. Blind signatures for untraceable payments. *Proceedings of Crypto 82*. New York, Plenum Press, 1983, pp. 199–203.

7. Nurmi H., Salomaa A., Santean L. Secret ballot elections in computer networks. *Computers and Security*, vol. 36, no. 10, 1991, pp. 553–560.

8. RFC 2818 HTTP over TLS, 2000.

9. Rivest R. L., Shamir A., Adleman L. M. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120–126.

10. *RSA Laboratories, PKCS #1 v2.2: RSA Cryptography Standard*, 2012.

11. Shamir A. *Comm. of the ACM*, 1979, vol. 22, p. 612.

УДК 004.056
DOI 10.21672/2074-1707.2019.47.3.102-121

АНАЛИЗ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП ГАЗОДОБЫВАЮЩИХ ПРЕДПРИЯТИЙ

Статья поступила в редакцию 10.06.2019, в окончательном варианте – 26.08.2019.

Римша Андрей Сергеевич, Тюменский государственный университет, 625003, Российская Федерация, г. Тюмень, ул. Перекопская, 15А,

аспирант, e-mail: RimshaAndrew@gmail.com

Римша Константин Сергеевич, Тюменский государственный университет, 625003, Российская Федерация, г. Тюмень, ул. Перекопская, 15А,

студент, e-mail: RimshaKonstantin@ya.ru

Цели исследования, описанного в данной статье: анализ актуальных классов решений для обеспечения информационной безопасности АСУ ТП газодобывающего предприятия; выбор наиболее подходящего решения и сравнение его с используемыми на рынке решениями соответствующего класса; формирование нового подхода к моделированию угроз; разработка программной реализации для предложенного раннее метода оценки угроз. Для достижения поставленных целей решен ряд научных задач. Проведено исследование нескольких средств информационной безопасности с учетом опыта их применения в автоматизированных системах; установлены критерии для сравнения рассматриваемых решений; в результате было определено средство, по своим характеристикам в наибольшей степени удовлетворяющее критериям сравнения. Рассмотрены популярные решения, относящиеся к данному классу, их достоинства и недостатки. Учитывая специфические особенности обеспечения информационной безопасности АСУ ТП, были сформулированы определенные требования, причем ни одно из рассмотренных решений в полной