Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Тульский государственный университет»

Интернет-институт ТулГУ

Кафедра ИБ

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ

по дисциплине

«**Методы и средства защиты компьютерной информации**»

на тему

«ГОСТ Р 34.10-2001 Обзор, назначение, область применения, особенности»

Вариант № 5

Выполнил:

студент группы ИБ262521-ф
Артемов Александр Евгеньевич

Проверил:

канд. техн. наук, доц.
Сафронова Марина Алексеевна

Тула, 2025

Содержание

Задание на работу

1. Изучить материал по вопросу "Электронная цифровая подпись".
2. Написать реферат на тему, соответствующую Вашему индивидуальному варианту. Номер варианта соответствует последней цифре номера Вашей зачетной книжки. В реферате обязательно должен быть список использованной литературы и ссылки на нее в материале реферата.
3. Сдать работу преподавателю.

Введение

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но при этом возникает проблема аутентификации автора документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном документе. В обычной (бумажной) информатике эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- активный перехват – нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- маскарад – абонент С посылает документ абоненту В от имени абонента А;
- ренегатство – абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал;
- подмена – абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А;
- повтор – абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Принципиально новым решением является электронная цифровая подпись.

Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;

– гарантирует целостность подписанного текста.

Цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

Система электронной цифровой подписи включает две процедуры:

1. процедуру постановки подписи;
2. процедуру проверки подписи.

В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

При формировании электронной цифровой подписи отправитель прежде всего вычисляет хэш-функцию h(M) подписываемого текста M. Вычисленное значение хэш-функции h(M) представляет собой один короткий блок информации m, характеризующий весь текст M в целом. Затем число m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой электронную цифровую подпись для данного текста M.

При проверке электронной цифровой подписи получатель сообщения снова вычисляет хэш-функцию m = h(M) принятого по каналу текста M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

Принципиальным моментом в системе электронной цифровой подписи является невозможность подделки электронной цифровой подписи пользователя без знания его секретного ключа подписывания.

В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из не подписанного путем добавления в него одной или более электронных подписей.

Каждая подпись содержит следующую информацию:

– дату подписи;
– срок окончания действия ключа данной подписи;
– информацию о лице, подписавшем файл (ФИО, должность, краткое наименование фирмы);
– идентификатор подписавшего (имя открытого ключа);
– собственно цифровую подпись.

В данной работе рассмотрен стандарт ГОСТ Р 34.10-2001. Стандарт описывает процессы формирования и проверки электронной цифровой подписи, реализуемой с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем.

Стандарт разработан взамен ГОСТ Р 34.10-94. Необходимость разработки стандарта ГОСТ Р 34.10-2001 вызвана потребностью в повышении стойкости электронной цифровой подписи к несанкционированным изменениям. Стойкость электронной цифровой подписи основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11.

Данный стандарт терминологически и концептуально увязан с международными стандартами ИСО 2382-2 [1] ИСО/МЭК 9796 [2], серии ИСО/МЭК 14888 [3] - [5] и серии ИСО/МЭК 10118 [6]-[9].

Назначение стандарта ГОСТ Р 34.10-2001

Электронная цифровая подпись — это технология, которая позволяет обеспечить целостность, подлинность и юридическую значимость электронных документов. Основное назначение ГОСТ Р 34.10-2001 — обеспечение целостности и подлинности электронных документов с использованием электронной цифровой подписи. Электронная цифровая подпись позволяет подтвердить авторство документа и гарантировать, что он не был изменен после подписания. Стандарт определяет математические основы для создания и проверки подписей, что делает его важным инструментом в сфере информационной безопасности.

Общепризнанная схема (модель) цифровой подписи охватывает три процесса:

- генерация ключей (подписи и проверки);
- формирование подписи;
- проверка подписи.

В настоящем стандарте процесс генерации ключей (подписи и проверки) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию.

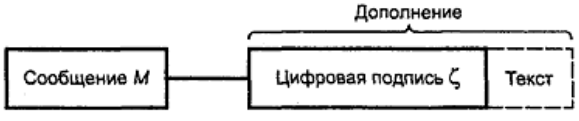
Механизм цифровой подписи определяется посредством реализации двух основных процессов :

- формирование подписи;
- проверка подписи.

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществить контроль целостности передаваемого подписанного сообщения;
- доказательно подтвердить авторство лица, подписавшего сообщение;
- защитить сообщение от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке:



Поле «текст», показанное на данном рисунке и дополняющее поле «цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и (или) метку времени.

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем, а также хэш-функции.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритм вычисления хэш-функции установлен в ГОСТ Р 34.11.

Стандарт не определяет процесс генерации параметров схемы цифровой подписи. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы цифровой подписи исходя из требований к аппаратно-программным средствам, реализующим электронный документооборот.

В хозяйственной деятельности назначение электронной цифровой подписи включает:

– обеспечение целостности данных. Электронная цифровая подпись гарантирует, что документ или данные не были изменены после их подписания. При формировании подписи создается уникальная хэш-сумма (криптографический отпечаток) документа. Любое изменение документа приведет к изменению этой суммы, что будет обнаружено при проверке подписи.

– подтверждение авторства. Электронная цифровая подпись позволяет установить личность лица, подписавшего документ. Подпись создается с использованием закрытого ключа, который известен только владельцу. Проверка подписи осуществляется с помощью открытого ключа, который связан с закрытым. Это подтверждает, что подпись была создана именно владельцем ключа.

– юридическая значимость. Электронная цифровая подпись придает электронным документам юридическую силу, равную собственноручной подписи на бумажных документах. В соответствии с законодательством многих стран (включая Россию), документ, подписанный ЭЦП, признается действительным в суде и других официальных инстанциях.

– защита от подделки. Электронная цифровая подпись предотвращает возможность подделки документа или подписи.

Криптографические алгоритмы, используемые для создания подписи, делают ее практически невозможной для подделки без доступа к закрытому ключу.

– упрощение документооборота. Электронная цифровая подпись позволяет перевести документооборот в электронную форму, что ускоряет процессы согласования, подписания и передачи документов. Электронные документы с электронной цифровой подписью могут быть быстро отправлены и проверены без необходимости физического присутствия сторон.

– обеспечение конфиденциальности. В сочетании с шифрованием ЭЦП может использоваться для защиты конфиденциальности данных. Документ может быть зашифрован, а подпись подтверждает его подлинность после расшифровки.

– использование в различных сферах. Электронная цифровая подпись применяется в государственных, коммерческих и частных системах для обеспечения безопасности и доверия. Например, торги и госзакупки, сдача налоговой и бухгалтерской отчетности, банковские операции и электронные платежи, электронный документооборот между организациями.

Формирование и проверка электронной цифровой подписи предназначены для обеспечения безопасности, доверия и юридической значимости электронных документов и данных. Электронная цифровая подпись является ключевым инструментом в современных информационных системах, позволяя эффективно защищать информацию и упрощать процессы взаимодействия между участниками электронного обмена данными.

Область применения

Электронная цифровая подпись широко используется в различных сферах деятельности, где требуется обеспечение безопасности, целостности и юридической значимости электронных документов и данных. Ниже приведены основные области применения электронной цифровой подписи.

Государственные услуги и взаимодействие с органами власти:

- электронная отчетность: сдача налоговой, бухгалтерской и статистической отчетности в государственные органы (например, ФНС, ПФР, Росстат);
- госзакупки: участие в электронных торгах на платформах, таких как Единая информационная система (ЕИС) в рамках 44-ФЗ и 223-ФЗ;
- регистрация юридических лиц: подача документов для регистрации индивидуальных предпринимателей, ООО или внесения изменений в ЕГРЮЛ через порталы (например, ФНС или Госуслуги);
- лицензирование и аккредитация: получение лицензий, аккредитаций и других разрешительных документов в электронном виде.

Финансовая и банковская сфера:

- электронные платежи: пдписание платежных поручений и других финансовых документов в системах интернет-банкинга;
- кредитование: оформление кредитных договоров и других документов без посещения банка;
- управление счетами: подписание договоров на открытие счетов, управление вкладами и другими банковскими продуктами.

Корпоративный документооборот:

- внутренний документооборот: подписание приказов, договоров, актов и других внутренних документов в электронном виде.
- внешний документооборот: обмен юридически значимыми документами с контрагентами (договоры, счета, акты выполненных работ).
- кадровые документы: оформление трудовых договоров, приказов о приеме на работу, увольнении и других кадровых документов.

Электронная коммерция

- заключение договоров: подписание договоров купли-продажи, оказания услуг и других соглашений.
- электронные торги: участие в коммерческих тендерах и аукционах.
- онлайн-платежи: подтверждение транзакций и подписание финансовых документов.

Юридическая сфера:

- электронное правосудие: подача исковых заявлений, жалоб и других документов в арбитражные суды и суды общей юрисдикции через электронные системы (например, "Мой арбитр").
- нотариальные услуги: удостоверение документов и сделок с использованием ЭЦП.

Медицина и здравоохранение:

- электронные медицинские карты: подписание медицинских документов, рецептов и заключений.
- лицензирование медицинской деятельности: подача документов для получения лицензий и аккредитаций.

Образование:

- электронные дипломы и сертификаты: выдача документов об образовании с использованием ЭЦП.
- дистанционное обучение: подписание договоров на оказание образовательных услуг и других документов.

Логистика и транспорт:

- электронные транспортные накладные (ЭТРН): оформление и подписание транспортных документов.
- таможенное оформление: подача деклараций и других документов в электронном виде.

Энергетика и жилищно-коммунальное хозяйство:

- электронные счета: подписание счетов за коммунальные услуги.
- договоры с поставщиками: оформление договоров на поставку энергоресурсов.

Международная торговля:

- электронные документы: подписание контрактов, инвойсов и других документов для международных сделок.

Информационные технологии:

- защита программного обеспечения: подписание программных продуктов и обновлений для подтверждения их подлинности.
- управление доступом: использование электронной цифровой подписи для авторизации в информационных системах.

Электронная цифровая подпись является универсальным инструментом, который находит применение в самых разных сферах — от государственных услуг и финансов до корпоративного документооборота и международной торговли. Ее использование позволяет ускорить процессы, снизить затраты на бумажный документооборот и обеспечить высокий уровень безопасности и доверия при работе с электронными документами.

Особенности стандарта ГОСТ Р 34.10-2001

ГОСТ Р 34.10-2001 — это российский стандарт, который определяет алгоритмы формирования и проверки электронной цифровой подписи. Он имеет ряд особенностей, которые отличают его от других стандартов, таких как RSA, ECDSA (стандарт на основе эллиптических кривых, используемый в зарубежных странах) и более современных версий ГОСТ (например, ГОСТ Р 34.10-2012).

Ключевые особенности стандарта ГОСТ Р 34.10-2001:

1. Использование эллиптических кривых (ECC). Стандарт основан на математике эллиптических кривых (Elliptic Curve Cryptography, ECC). Эллиптические кривые обеспечивают высокий уровень криптографической стойкости при меньшей длине ключей по сравнению с другими алгоритмами (например, RSA). Это делает электронную цифровую подпись более эффективной с точки зрения вычислительных ресурсов и объема данных.

2. Длина ключей. Стандарт предусматривает использование ключей длиной 256, 512 и 1024 бита. Даже при меньшей длине ключей (например, 256 бит) обеспечивается высокая стойкость к взлому, что делает ГОСТ Р 34.10-2001 конкурентоспособным по сравнению с RSA, где требуются ключи длиной 2048 бит и более.

3. Соответствие российскому законодательству. Стандарт соответствует требованиям российского законодательства в области защиты информации, включая Федеральный закон № 63-ФЗ "Об электронной подписи". Использование этого стандарта позволяет организациям и физическим лицам работать в правовом поле России, обеспечивая юридическую значимость электронных документов.

4. Криптографическая стойкость. Алгоритмы ГОСТ Р 34.10-2001 обеспечивают высокий уровень защиты от взлома и подделки подписи. Стандарт устойчив к современным криптографическим атакам, включая атаки на основе квантовых вычислений (в сравнении с RSA).

5. Использование отечественных криптографических алгоритмов. ГОСТ Р 34.10-2001 является частью семейства российских криптографических стандартов, которые разработаны с учетом национальных требований к безопасности. Это позволяет использовать стандарт в государственных и коммерческих системах, где требуется соблюдение российских норм.

6. Процедуры формирования и проверки подписи. Стандарт определяет четкие процедуры для формирования и проверки подписи, включая использование хэш-функции ГОСТ Р 34.11-94. Это обеспечивает

совместимость и надежность при работе с различными системами, поддерживающими ГОСТ.

7. Ограниченное международное признание. ГОСТ Р 34.10-2001 в основном используется в России и странах СНГ. В международных системах чаще применяются стандарты, такие как ECDSA или RSA, что может создавать сложности при взаимодействии с зарубежными партнерами.

8. Устаревание стандарта. ГОСТ Р 34.10-2001 был заменен на более современный стандарт ГОСТ Р 34.10-2012, который использует более сложные криптографические алгоритмы. В новых системах рекомендуется использовать ГОСТ Р 34.10-2012, так как он обеспечивает более высокий уровень безопасности.

9. Совместимость с инфраструктурой открытых ключей (PKI). Стандарт поддерживает работу с инфраструктурой открытых ключей (PKI), что позволяет использовать сертификаты для проверки подписей. Это упрощает интеграцию с системами электронного документооборота и другими приложениями, требующими аутентификации.

10. Применение в государственных системах. Стандарт широко используется в государственных информационных системах, таких как ЕГАИС, МЭДО (межведомственный электронный документооборот) и других. Это делает стандарт обязательным для организаций, работающих с государственными структурами.

Стандарт ГОСТ Р 34.10-2001 имеет уникальные особенности, такие как использование эллиптических кривых, соответствие российскому законодательству и высокая криптографическая стойкость. Однако его применение ограничено в основном Россией и странами СНГ, а также он уступает более современным стандартам, таким как ГОСТ Р 34.10-2012. Тем не менее, он остается важным инструментом в системах, где требуется соблюдение российских норм и стандартов.

Список литературы

1. ГОСТ Р 34.10-2001 https://kaf401.rloc.ru/Criptfiles/GOST_R_34.10-2001.pdf
2. Федеральный закон № 63-ФЗ "Об электронной подписи" https://www.consultant.ru/document/cons_doc_LAW_112701/
3. Тема 18. Электронная цифровая подпись. https://tulsu.ru/sdoii/pluginfile.php/277389/mod_resource/content/2/lex/lex_18/lex_18_1.html
4. Elliptic-curve cryptography https://en.wikipedia.org/wiki/Elliptic-curve_cryptography