4. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. – М.: Акад. Проект, 2008. – 544 с.

Электронная цифровая подпись и её применение

Галко В.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

В мире электронных документов подписание файла с помощью графических символов теряет смысл, так как подделать и скопировать графический символ можно бесконечное количество раз. Электронная цифровая подпись является полным электронным аналогом обычной подписи на бумаге, но реализуется не с помощью графических изображений, а с помощью математических преобразований над содержимым документа.

Электронная цифровая подпись (ЭЦП)– реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Особенности математического алгоритма создания и проверки ЭЦП гарантируют невозможность подделки такой подписи посторонними лицами, чем достигается неопровержимость авторства.

Схема электронной подписи обычно включает в себя:

– алгоритм генерации ключевых пар пользователя;
– функцию вычисления подписи;
– функцию проверки подписи.

Электронная цифровая подпись может иметь следующее назначение:

– Удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т.д.
– Защиту от изменений документа.
– Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.
– Предприятиям и коммерческим организациям сдачу финансовой отчётности в государственные учреждения в электронном виде.

Пользоваться электронной подписью достаточно просто. Никаких специальных знаний, навыков и умений для этого не потребуется. Каждому пользователю ЭЦП, участвующему в обмене электронными документами, генерируются уникальные *открытый* и *закрытый* (*секретный*) криптографические ключи.

Закрытый ключ– это закрытый уникальный набор информации объёмом 256 бит, хранится в недоступном другим лицам месте на дискете, смарт-карте. Работает закрытый ключ только в паре с открытым ключом.

Открытый ключ– используется для проверки ЭЦП получаемых документов/файлов. Технически это набор информации объёмом 1024 бита. Открытый ключ передаётся вместе с письмом, подписанным ЭЦП.

Дубликат открытого ключа направляется в Удостоверяющий Центр, где обеспечивается регистрация и надёжное хранение открытых ключей во избежание попыток подделки или внесения искажений.

В ЭЦП записывается следующая информация:

– имяфайла открытого ключа подписи;
– информация о лице, сформировавшем подпись;
– дата формирования подписи.

Применение ЭЦП имеет следующие преимущества:

– Конфиденциальность: ЭЦП безошибочно указывает на аутентичность и уникальность своего автора;
– Приоритетность сдачи отчётности в электронном виде;
– Прохождение первичного камерального контроля, что исключает наличие арифметических и логических ошибок;
– Возможность оперативного обновления форматов представления документов в электронном виде по каналам связи.

Перечисленные выше свойства электронной цифровой подписи позволяют использовать её в следующих основных целях электронной экономики и электронного документального и денежного обращения:

– Использование в банковских платёжных системах.
– Электронная коммерция(торговля).
– Электронная регистрация сделок по объектам недвижимости.
– Таможенное декларированиетоваров и услуг (таможенные декларации).
– В электронных системах обращения граждан к органам власти, в том числе и по экономическим вопросам.
– Формирование обязательной налоговой, бюджетной, статистической и прочей отчётности перед государственными учреждениями и внебюджетными фондами.
– Управление акционерным капиталом и долевым участием.

– ЭЦП является одним из ключевых компонентов сделок вкриптовалютах.

VPN - Виртульные частные сети

Долгий И.С., Поляков М.О.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

VPN–аббревиатура английских словVirtualPrivateNetwork, что в дословном переводе на русский язык означает Частная Виртуальная Сеть. Представляет собой совокупность технологий/служб туннелирования,аутентификации, управления доступом и контроля, используемых для защиты данных и передачи трафика через Интернет. В настоящее время популярна как среди обычных пользователей интернета, так и у различных компаний.

С помощью аутентификации получатель сообщения, являющийся пользователем виртуальной частной сети, можетотслеживать источник полученных пакетов и обеспечить целостность данных.С помощьюсредств защитыданныхв виртуальных частных сетях гарантируется конфиденциальность исходных пользовательских данных.

Организация виртуальной частной сети позволяет пользователям, её использующих, передавать данные через линии доступа к Интернету, таким образом уменьшая необходимость в некоторых из существующих линий.

При организации виртуальной частной сети снижаются расходы на междугороднюю телефонную связь, поскольку пользователь обычно получает услуги от местного Интернет-провайдера, а не совершает междугородний звонок для установления прямой связи с компанией.

Принцип работы VPN относительно простой. VPN-устройство располагается между внутренней сетью и Интернетом на каждом конце соединения. Когда данные передаются через VPN, они исчезают «с поверхности» в точке отправки и вновь появляются только в точке назначения. Этот процесс принято называть «туннелированием». Это означает создание логического туннеля в сети Интернет, который соединяет две крайние точки. Благодаря туннелированию частная информация становится невидимой для других пользователей Интернета. Прежде чем попасть в интернет-туннель, данные шифруются, что обеспечивает их дополнительную защиту. Протоколы шифрования бывают разные. Все зависит от того, какой протокол туннелирования поддерживается тем или иным VPN-решением. Еще одной важной