ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 5
2015

Г. А. Шевцова, К. А. Градусов (Москва, РГГУ)**. Особенности применения электронной подписи.**

Для защищенных систем передачи информации и автоматизированных систем, контролирующих работу удаленных объектов, в том числе функционирующих полностью в автоматическом режиме, все чаще используется электронная подпись.

Электронная подпись позволяет осуществить аутентификацию источника данных и обеспечить их целостность. При электронном взаимодействии обеспечивается подтверждение авторства.

Ее использование открывает нам новые возможности и различные вариации в электронном документообороте, но на современном технологическом этапе развития общества, данное средство, основанное на криптографической защите, является не до конца устоявшимся и доработанным методом подтверждения оригинальности важнейших электронных документов.

Электронная подпись предполагает наличие двух алгоритмов — вычисления и проверки, обычно называемых в математике схемой цифровой подписи. Алгоритм вычисления электронной подписи должен быть «закрытым» для того, чтобы исключить возможность вычисления правильного значения подписи, т. е. определяться «закрытым ключом» и зависеть от всех подписываемых данных. Алгоритм проверки — открытым, для гарантирования возможности проверки подписи любым из участников электронного взаимодействия без знания какой-либо закрытой информации.

Электронная подпись называется подписью лишь условно, по причине того, что она целиком и полностью не имеет связи с электронным документом. Связь между электронной подписью и электронным документом является особой математической связью, результатом сложного криптографического преобразования информации.

Главной проблемой использования электронной подписи, является невозможность точно определить лицо, которое подписало документ. В отличие от собственноручной подписи, у электронной подписи нельзя осуществить проверку подлинности почерка. Соответственно, нельзя, основываясь только на наличии в документе электронной подписи, установить: действительно ли документ подписывался самим владельцем электронной подписи или же каким-либо иным лицом.

Сложность заключается и в самом ее использовании, т. к. электронная подпись требует дополнительных механизмов, реализующих алгоритмы ее вычисления и проверки, создания доверенной инфраструктуры сертификатов открытых ключей и, что немаловажно, имеет ограничения по сроку действия.

В настоящее время достаточно большое количество коммерческих сделок, а также некоторые деловые операции выполняются через Интернет, причем для их защиты от злоумышленников оказывается вполне достаточным использования таких криптографических функций, как конфиденциальность и аутентификация, реализуемых при помощи криптосистем шифрования, дешифрования и электронной подписи.

Однако, существует множество других взаимодействий между двумя или более пользователями сети Интернет, для которых обеспечение их безопасности не может быть реализовано только перечисленными выше функциями. Примерами подобных действий являются: электронные платежи, лотереи и аукционы, тайное голосование,

анонимная покупка данных, выполнение совместных вычислений с сохранением индивидуальных данных в секрете.

Для обеспечения безопасности выполнения этих или иных действий, выполняемых дистанционно, в условиях присутствия в этих сетях недобросовестных пользователей (в том числе и среди законных участников этих процедур), используются специально для них разработанные криптографические протоколы.

К примеру, одной из уязвимых услуг в современном мире, являются платные ТВ-программы, они могут быть зашифрованы при помощи ключей, которые передаются легальным подписчикам этих программ. Однако существует опасность, что некоторые из таких подписчиков могут продать ключи другим пользователям, не оплатившим эти программы. Криптографический протокол обеспечивает возможность поиска таких «подписчиков» в случае, когда ТВ-декодер пользователей может быть открыт для необходимого контроля.

Таким образом, электронная подпись является очень надежным инструментом, который позволяет, как установить авторство, так и подтвердить целостность любых данных в электронном виде.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ. Об электронной подписи. — Российская газета, 2011, 08 апреля.
2. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
3. *Жданов О. Н.*, *Золотарев В. В.* Методы и средства криптографической защиты информации: Учебное пособие. Красноярск, СибГАУ, 2007, 28 с.