УДК 349:[005.92:004.056.55]

Комлык А. А., Слащев А. Н.

МАТЕМАТИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ ЭЛЕКТРОННОЙ ПОДПИСИ

Анастасия Александровна Комлык
магистрант
nastyakomlyk@mail.ru
ФГБОУ ВО «Кубанский государственный университет», Россия, Краснодар
Артем Николаевич Слащев
магистрант
slashevartem@gmail.com
ФГБОУ ВО «Кубанский государственный университет», Россия, Краснодар

MATHEMATICAL AND LEGAL ASPECTS OF ELECTRONIC SIGNATURE

Anastasia Aleksandrovna Komlyk
Kuban State University, Russia, Krasnodar
Artem Nikolaevich Slashchev
Kuban State University, Russia, Krasnodar

Аннотация*. В статье раскрываются основные подходы при работе в электронной подписью. Раскрыты основные аспекты, позволяющие обезопасить работу с электронной подписью.*

Abstract*. The article reveals the main approaches when working with an electronic signature. The main aspects are disclosed that allow to secure the work with an electronic signature.*

Ключевые слова: *электронная подпись, хэш-код, безопасность, открытый ключ, закрытый ключ.*

Keywords: *electronic signature, hash code, security, public key, private key.*

Электронная подпись — это математическая схема для демонстрации подлинности цифровых сообщений или документов. Она обеспечивает соблюдение правовых норм, а также действительность и подлинность цифрового документа, и личность подписывающего лица. Подпись должна подтверждать тот факт, что данные исходят от подписывающей стороны и они не были подделаны во время передачи.

Регулирование электронной подписи приняло множество разных форм на международных и всероссийских уровнях. Можно выделить три основных подхода к работе с электронной подписью:

- минималистический подход;
- технологический подход;
- двухуровневый подход.

Рассмотрим подробнее эти три подхода.

В некоторых юрисдикциях признают все технологии электронной подписи, следуя политике технологической нейтральности. Такой подход называется минималистическим, потому что он придает минимальный юридический статус всем формам электронной подписи.

Такие электронные подписи принято считать эквивалентными собственноручной подписи при условии, что используемая технология предназначена для выполнения определенно заданных функций и, кроме того, отвечает определенным технологически нейтральным требованиям надежности.

В соответствии со вторым подходом, основанным на конкретных технологиях, нормативные акты обязывают использовать конкретную технологию выполнять юридические требования в отношении действительности электронной подписи. Это имеет место, например, когда закон, направленный на более высокий уровень безопасности требует приложений основанных на инфраструктуре открытых ключей (ИОК). Поскольку этот подход предписывает использование определенных технологий, его также можно назвать «предписывающим» подходом.

Недостатки такого подхода, ориентированного на конкретные технологии, заключаются в том, что, отдавая предпочтение определенным типам электронной подписи, есть риск исключить возможность выхода на рынок других, возможно, более совершенных технологий.

Еще один важный момент, который стоит учитывать заключается в том, что не всем приложениям может потребоваться уровень безопасности, сопоставимый с уровнем безопасности, обеспечиваемым некоторыми указанными методами электронной подписи. Также может возникнуть ситуация, когда скорость и простота связи могут быть для сторон более важными факторами, чем обеспечение целостности электронной информации посредством какого-либо конкретного процесса. Требования к использованию чрезмерно безопасных средств аутентификации может привести к потраченным впустую затратам и усилиям, что может помешать распространению электронной торговли.

При двухуровневом подходе законодательство устанавливает низкий порог требований к методам электронной подписи для получения определенного минимального правового статуса и придает большую юридическую силу определенным методам электронной подписи.

На базовом уровне законодательство, принимающее двухуровневую систему, обычно предоставляет электронным подписям статус функционально эквивалентный собственноручной подписи на основе технологически нейтральных критериев. Подписи более высокого уровня, к которым применяются определенные опровержимые презумпции, необходимы для соответствия конкретным требованиям, которые могут относиться к конкретной технологии.

У цифровой электронной подписи также есть ряд недостатков. В отличии от традиционной подписи, которая не имеет срока действия (кроме смерти физического лица), максимальная продолжительности признания цифровой подписи в соответствии с законом составляет три года с даты ее выдачи. Также

стоит отметить, что нет положения, регулирующего продление цифровых сертификатов. Это означает, что физическому лицу придется повторно подать заявку на новый сертификат в том же порядке.

По поводу безопасности использования электронной подписи нередко возникали споры в связи с тем, что оборудование и программное обеспечение, используемое для создания электронной подписи, могут быть уязвимы для несанкционированного доступа. Закон не запрещает сторонам согласовывать другие типа электронной подписи с использованием других технологий. Но закон, в свою очередь, устанавливает режим использования и признания электронной подписи и содержит несколько положений, касающихся вопросов безопасности, таких как обязательство со стороны сертифицированного органа и физического лица использования надежной системы, проявление осторожности при использовании секретного ключа и предотвращение разглашения его неавторизированным лицам. Но закон не регулирует аспекты взлома (несанкционированный доступ и несанкционированное изменение).

Дополнительными мерами безопасности могут послужить следующие действия.

Все криптосистемы с открытым (закрытым) ключом полностью зависят от сохранения секретного ключа. Закрытый ключ может храниться на компьютере пользователя и быть защищен локальным паролем, но этот способ имеет следующие два недостатка:

- пользователь может подписать документы только на этом конкретном компьютере;
- безопасность закрытого ключа полностью зависит от безопасности компьютера.

Более безопасный способ — хранить закрытый ключ на смарт-карте. Многие смарт-карты защищены от несанкционированного доступа. В стандартной реализации цифровой подписи хэш, вычисленный на основе документа, отправляется на смарт-карту, а электронная подпись, используя сохраненный закрытый ключ пользователя возвращает зашифрованный хэш.

Как правило, пользователь должен активировать свою смарт-карту введя личный идентификационный номер или PIN-код (обеспечивая двухфакторную аутентификацию).

Можно сделать так, чтобы закрытый ключ никогда не покидал смарт-карту, но это не всегда возможно реализовать. Если смарт-карта украдена, похитителю все равно понадобится PIN-код для создания электронной подписи.

Смягчающим фактором является то, что закрытые ключи, если они сгенерированы и хранятся на смарт-картах, обычно считаются трудно копируемыми, и предполагается, что они существуют только в одной копии.

Таким образом, утеря смарт-карты, может быть, обнаружена владельцем и соответствующий сертификат может быть немедленно отозван. Закрытые ключи, защищенные только программным обеспечением, легче скопировать, а такие взломы гораздо труднее обнаружить.

Для ввода PIN-кода для активации смарт-карты обычно требуется цифровая клавиатура. Некоторые устройства чтения карт имеют собственную цифровую клавиатуру. Это безопаснее, чем использование устройства чтения карт, встроенные в ПК, с последующим вводом PIN-кода с клавиатуры этого компьютера. Считыватели с цифровой клавиатурой предназначены для того, чтобы обойти угрозу подслушивания, когда на компьютере может быть запущен регистратор нажатия клавиш, что потенциально может нарушить PIN-код. Специализированные устройства чтения карт также менее уязвимы для несанкционированного доступа к их программному или аппаратному обеспечению и часто имеют сертификат EAL3.

Основным различием между цифровой и письменной подписью является то, что пользователь не «видит» то, что он подписывает. Пользовательское приложение представляет собой хэш-код, который должен быть зашифрован алгоритмом электронной подписи с использованием закрытого ключа. Злоумышленник, получивший контроль над ПК пользователя может заменить пользовательское приложение чужим. Это может позволить вредоносному

приложению обмануть пользователя и заставить его подписать любой документ, отображая исходный текст пользователя на экране, но предоставляя собственные документы для подписи. Для защиты от этого между приложением пользователя и приложением подписи может быть установлена система аутентификации. Общая идея состоит в том, чтобы предоставить как пользовательскому приложению, так и приложению для подписи средства для проверки целостности друг друга, что в разы увеличит безопасность при подписывании документов.

Список литературы

1. *Коваленко, Ю. И.* Правовой режим лицензирования и сертификации в сфере информационной безопасности / Ю. И. Коваленко. Москва: Горячая линия-Телеком, 2012. 140 с. Текст: непосредственный.

2. *Организационно-правовое* обеспечение информационной безопасности / А. А. Стрельцов, В. С. Горбатов, Т. А. Полякова [и др.]; под ред. А. А. Александрова, М. П. Сычева. Москва: Издательство МГТУ им. Н. Э. Баумана, 2018. 291 с. Текст: непосредственный.

3. Об электронной подписи: Федеральный закон № 63-ФЗ: принят Государственной Думой 25 марта 2011 года: одобрен Советом Федерации 30 марта 2011 года. Москва: Рид Групп, 2011.