



конференция

РусКрипто'2013



Конференция «РусКрипто'2013»

**Условия применения квалифицированной
электронной подписи: технологические и
организационные аспекты**

**Маслов Юрий,
ООО «КРИПТО-ПРО»
maslov@cryptopro.ru**

© 2000-2013 КРИПТО-ПРО

Усиленная квалифицированная электронная подпись

Не требует превентивного заключения соглашения сторон о порядке применения ЭП, т.е. не требует организационной составляющей (по закону)

Могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

- Квалифицированный СКПЭП изготовленный и выданный аккредитованным УЦ
- Используются сертифицированные ФСБ России средства ЭП, указанные в СКПЭП

Угрозы как следствие наличия неопределённостей

Уменьшение неопределённостей уменьшает вероятность возникновения угрозы

Угрозы

Лицо может не принять к исполнению документ, удостоверенный «действительной» электронной подписью



Определение меры неопределённости

Мера неопределённости - вероятность наступления событий, от которых зависит возникновение угрозы.

Мера неопределённости определим как произведение вероятностей событий:

Перечень событий (независимых и совместных)

Лица, подписавшее электронный документ, определено однозначно:

- ключ подписи и ключ проверки подписи являются уникальными
- существует однозначная связь между ключом подписи и ключом проверки подписи
- существует однозначная связь между ключом проверки подписи и его владельцем

Доказано отсутствие изменения в документе после подписания:

- однозначность механизма контроля целостности подписи документа и подписи

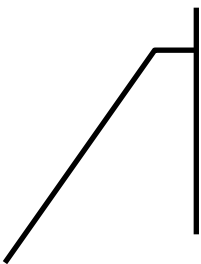
Доказана действительность электронной подписи на любой момент времени:

- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи
- однозначность механизма определения статуса ключа проверки подписи на момент времени (создания и/или проверки ЭП)

Оценим вероятности событий

В связи с невозможностью использования объективных методов определения вероятности исхода в неопределённости (нет статистики), используется субъективный метод оценки (на суждениях и личном опыте) вероятности исхода неопределённости

Неопределённости	Без криптографических средств (для простой ЭП)
Однозначность определения лица, подписавшего электронный документ:	
- уникальность ключа подписи и ключа проверки подписи	0.5
- однозначная связь между ключом подписи и ключом проверки подписи	0.5
- однозначная связь между ключом проверки подписи и его владельцем	0.5
Доказуемость отсутствия изменения в документе после подписания:	
- однозначность механизма контроля целостности подписи документа и подписи	0.5
Доказуемость действительности электронной подписи на любой момент времени	
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи	0.5
- однозначность механизма проверки статуса ключа проверки подписи на момент времени	0.5



Надёжность методов и технологий основывается на экспертной оценке. Вероятность дана с учётом состязательности процесса.



Оценим вероятности событий

Средства ЭП криптографические, но реализованы с использованием не ГОСТ алгоритмов и без удостоверяющего центра

Неопределённости	Криптографически неГОСТ средства ЭП без СКПЭП
Однозначность определения лица, подписавшего электронный документ:	
- уникальность ключа подписи и ключа проверки подписи	0.8
- однозначная связь между ключом подписи и ключом проверки подписи	0.8
- однозначная связь между ключом проверки подписи и его владельцем	0.5
Доказуемость отсутствия изменения в документе после подписания:	
- однозначность механизма контроля целостности подписи документа и подписи	0.8
Доказуемость действительности электронной подписи на любой момент времени	
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи	0.5
- однозначность механизма проверки статуса ключа проверки подписи на момент времени	0.5

Пусть и не ГОСТ, но всё таки экспертам труднее найти дыры в технологии

Так как нет СКПЭП, то механизм связи может быть экспертами рассмотрен и так и так.



Оценим вероятности событий

Средства ЭП криптографические, реализованы с использованием ГОСТ алгоритмов, но не сертифицированы ФСБ России и без удостоверяющего центра

Неопределённости	Криптографически е ГОСТ средства ЭП без СКПЭП
Однозначность определения лица, подписавшего электронный документ:	
- уникальность ключа подписи и ключа проверки подписи	0.9
- однозначная связь между ключом подписи и ключом проверки подписи	1
- однозначная связь между ключом проверки подписи и его владельцем	0.5
Доказуемость отсутствия изменения в документе после подписания:	
- однозначность механизма контроля целостности подписи документа и подписи	1
Доказуемость действительности электронной подписи на любой момент времени	
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи	0.5
- однозначность механизма проверки статуса ключа проверки подписи на момент времени	0.5

Пусть и ГОСТ, но нет экспертно
подтверждённых условий эксплуатации, при
которых невозможен доступ посторонних лиц
к ключу подписи

Так как нет СКПЭП, то механизм связи может
быть экспертами рассмотрен и так и так.

Надёжность методов и технологий
основывается на экспертной оценке.

Оценим вероятности событий

Средства ЭП криптографические, реализованы с использованием не ГОСТ алгоритмов, но не сертифицированы ФСБ России, и есть удостоверяющий центр

Неопределённости	Криптографически неГОСТ средства ЭП с СКПЭП
Однозначность определения лица, подписавшего электронный документ:	
- уникальность ключа подписи и ключа проверки подписи	0.8
- однозначная связь между ключом подписи и ключом проверки подписи	0.8
- однозначная связь между ключом проверки подписи и его владельцем	0.8
Доказуемость отсутствия изменения в документе после подписания:	
- однозначность механизма контроля целостности подписи документа и подписи	0.8
Доказуемость действительности электронной подписи на любой момент времени	
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи	0.8
- однозначность механизма проверки статуса ключа проверки подписи на момент времени	0.8

Пусть и не ГОСТ, но всё таки экспертам труднее найти дыры в технологии и в реализации

Есть СКПЭП, но экспертно не оценена реализация средства УЦ и меры его информационной безопасности

Оценим вероятности событий

Средства ЭП криптографические, реализованы с использованием ГОСТ алгоритмов, но не сертифицированы ФСБ России и есть удостоверяющий центр

Неопределённости	Криптографически е ГОСТ средства ЭП с СКПЭП
Однозначность определения лица, подписавшего электронный документ:	
- уникальность ключа подписи и ключа проверки подписи	0.9
- однозначная связь между ключом подписи и ключом проверки подписи	1
- однозначная связь между ключом проверки подписи и его владельцем	0.9
Доказуемость отсутствия изменения в документе после подписания:	
- однозначность механизма контроля целостности подписи документа и подписи	1
Доказуемость действительности электронной подписи на любой момент времени	
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи	1
- однозначность механизма проверки статуса ключа проверки подписи на момент времени	0.9

Надёжные ГОСТ алгоритмы, но экспертно не
оцененная реализация, которая даёт
свободу состязательности в её оценке

Единица достигается использованием ГОСТ
алгоритмов

Тут предполагается с использованием
механизм CRL, поэтому и нет практической
достоверности

Оценим вероятности событий

Используется квалифицированная ЭП, т.е. средства ЭП сертифицированы ФСБ России и используются квалифицированные СКПЭП

Неопределённости	Сертифицированн ые средства ЭП с квалифицированн ым СКПЭП
Однозначность определения лица, подписавшего электронный документ:	
- уникальность ключа подписи и ключа проверки подписи	1
- однозначная связь между ключом подписи и ключом проверки подписи	1
- однозначная связь между ключом проверки подписи и его владельцем	1 (0.5 если СКПЭП признаётся неквалифицированн ым)
Доказуемость отсутствия изменения в документе после подписания:	
- однозначность механизма контроля целостности подписи документа и подписи	1
Доказуемость действительности электронной подписи на любой момент времени	
- однозначность механизма информирования участников системы о факте аннулирования ключа проверки подписи	1
- однозначность механизма проверки статуса ключа проверки подписи на момент времени	1 (0.9 если нет доказательства момента подписи)

Даём оценку, что события практически достоверные (равна 1) при следующих условиях:

1. СКПЭП признан квалифицированным на момент проверки ЭП
2. Имеются доказательства момента создания электронной подписи



Мера неопределённости зависит от технологии, используемой для применения ЭП



Квалифицированная подпись – как реализовать угрозы

УГРОЗА:

Вариант 1 реализации стратегии злоумышленника: Играем на отсутствии доказательства момента подписи. Смотрим периодичность издания СОС, подписываем документ и отдаём стороне на исполнение. Дожидаемся исполнения и, пока не издан новый СОС, подаём заявление на аннулирование СКПЭП. Далее признаем подпись «недействительной» на основании пункта 2 ст. 11 63-ФЗ. Вариант применим ко всем случаям и типам документов.

Вариант 2 реализации стратегии злоумышленника: Квалифицированный СКПЭП не удовлетворяет требованиям 795 приказа ФСБ России. Направляю документ с подписью контрагенту, дожидаясь его исполнения контрагентом, потом пишу контрагенту письмо, что УПС, произошла ошибка, сертификат только что признан неквалифицированным и подано в УЦ заявление на аннулирование сертификата. Вариант применим лицом в единичном случае (один раз подписать) использования такого сертификата и только для документов, которые по закону должны подписываться исключительно квалифицированной ЭП.

УГРОЗА:

Лицо может не принять к исполнению документ, удостоверенный «действительной» электронной подписью

Вариант 1: Играем на отсутствии доказательства момента подписи. Блокируем ресурсы с СОС, подписываем документ и отдаём стороне на исполнение. Сторона не принимает документ к исполнению. Далее признаем подпись «недействительной» на основании пункта 2 ст. 11 63-ФЗ. Вариант применим ко всем случаям и типам документов.

Квалифицированная подпись – как реализовать угрозы

Факт признания, что не выполнены все организационно-технические условия штатной эксплуатации, предусмотренные документацией на средство ЭП, не влияет на признание ничтожности сделки и на юридическую силу электронного документа

Вариант реализации стратегии злоумышленника как получение заключения о признании средства ЭП не сертифицированным в связи с нарушением условий использования средства ЭП (отсутствует заключение по контролю встраивания (оценки влияния)) или не соблюден комплекс мер защиты для данного класса защиты средства ЭП и т.д.)

Вопросы?

Маслов Юрий,
ООО «КРИПТО-ПРО»
maslov@cryptopro.ru