ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В ОПАСНОСТИ! ЧТО ДЕЛАТЬ?!

Начальник сектора управления защиты информации Оперативно-аналитического центра при Президенте Республики Беларусь
Комисаренко Владимир Владимирович
Заведующий научно-исследовательской лабораторией НИИ ПМИ БГУ
Костевич Андрей Леонидович

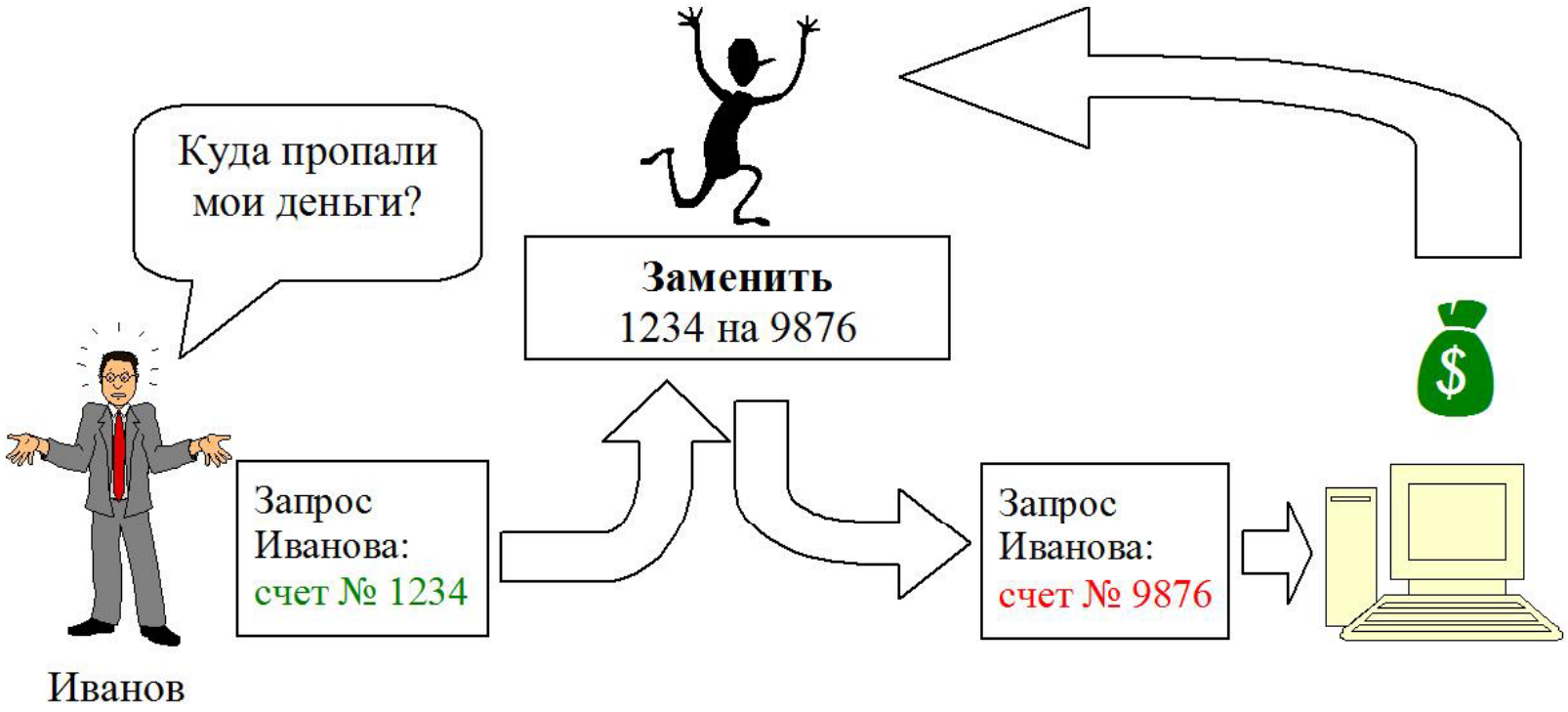
ЭЦП экономит время. А время – деньги!

Угроза подделки сообщения

Аутентификация сообщения — проверка того, что лицо, пославшее сообщение, не выдает себя за другое лицо, что источник сообщения не является поддельным

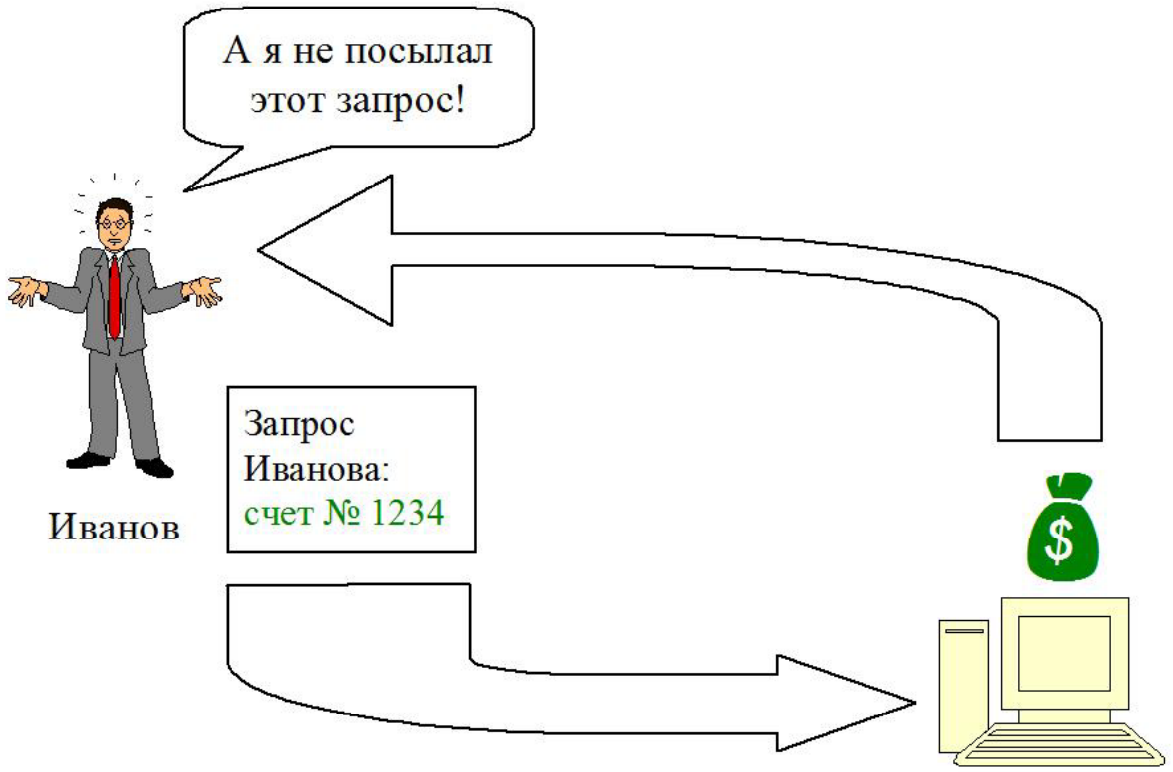
Угроза изменения сообщения

Проверка целостности — проверка того, что сообщение не было изменено; гарантия обнаружения изменения сообщения



Угроза отказа от авторства

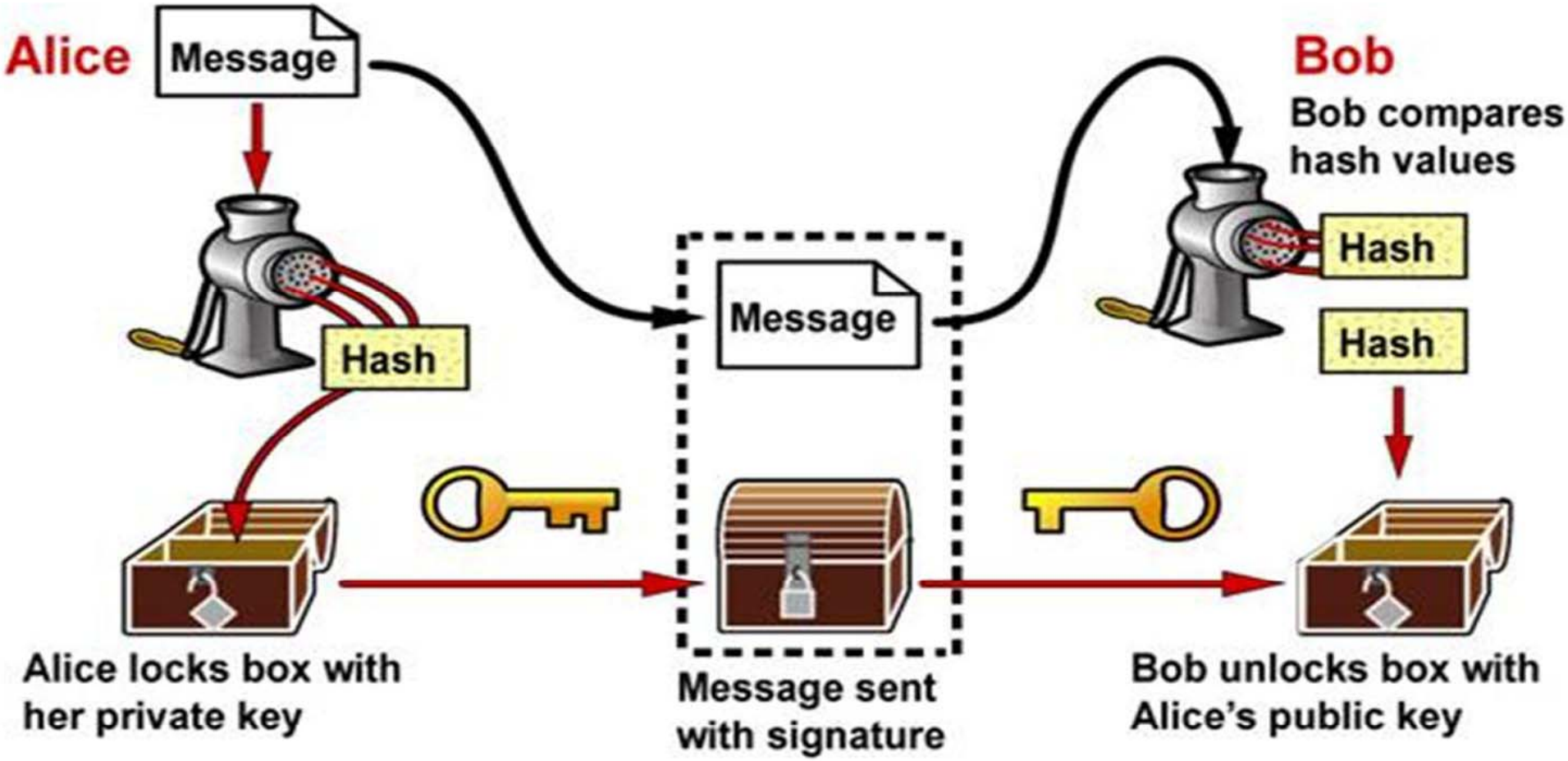
Невозможность отказа от авторства — при отправке сообщения невозможность отправителю сообщения отказаться от факта отправки сообщения



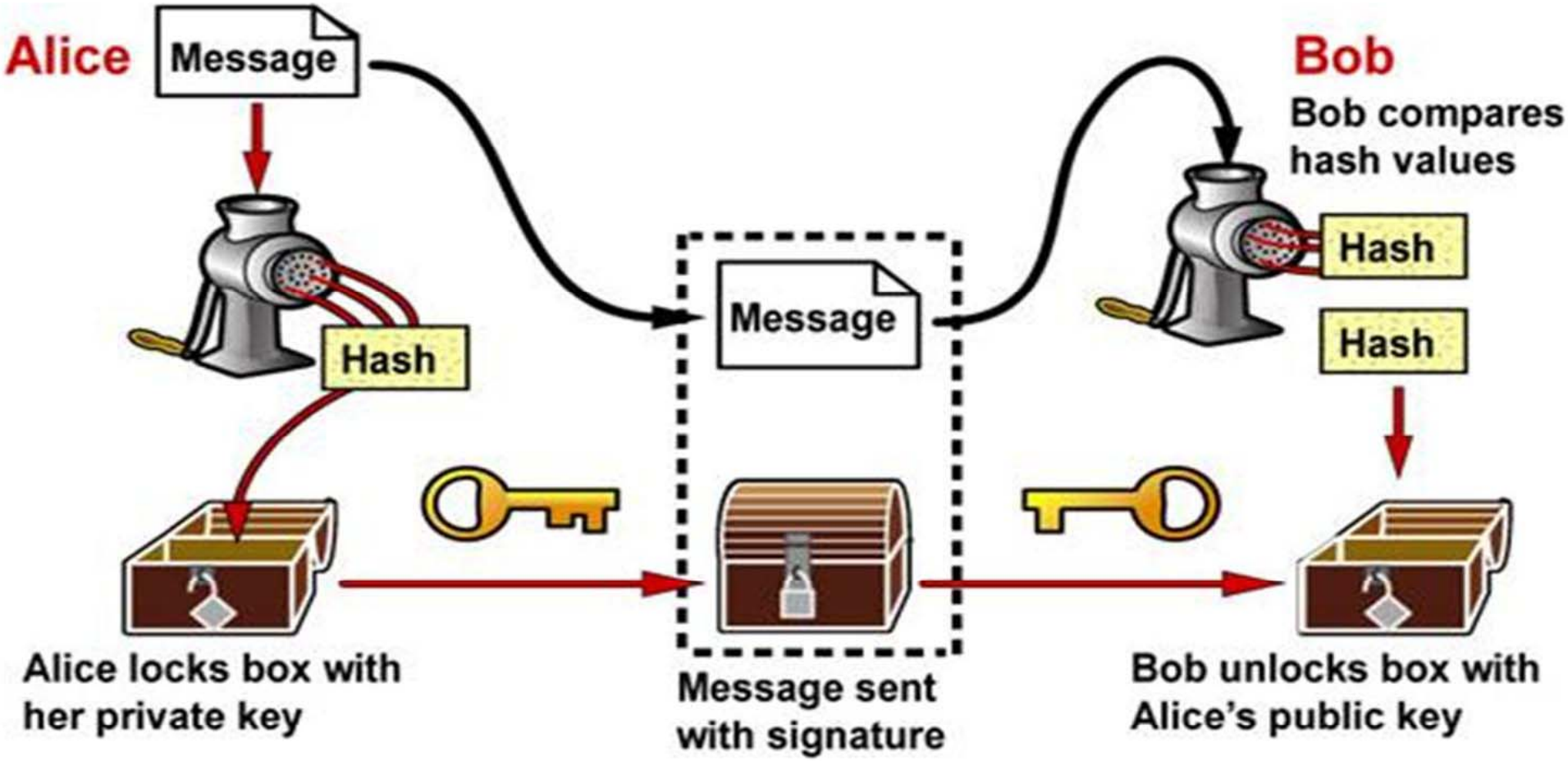
	Критерий сравнения	Подпись человека	Электронная цифровая подпись	Результат сравнения
1.	Зависимость от подписываемого текста	Одинакова для всех подписываемых документов	Зависит от содержания электронного документа	**Преимущество** ЭЦП
2.	Привязка к человеку	Свойственна человеку, не может быть утеряна	Определяется личным ключом (одноразовым секретным параметром)	**Создает опасность**, связанную с возможностью хищения личного ключа
3.	Способ подписания	Человек видит содержание, которое он подписывает	ЭЦП вырабатывает программа	**Порождает опасности**, связанные с качеством программ и безопасности среды ее исполнения
4.	Связь подписи с носителем информации	Неотделима от бумаги, требуются копии	ЭЦП отделима от электронного документа, оригиналы легко тиражируются	**Преимущество** ЭЦП
5.	Наличие инфраструктуры	Применение не требует особой инфраструктуры	Требуются дополнительная инфраструктура	**Дополнительные угрозы** от инфраструктуры
6.	Возможность подделки	Подлинность подписи определяется по результатам криминологической экспертизы	Подделать практически не возможно	Вероятность подделки ЭЦП **существенно меньше**

Широкое применение технологии ЭЦП порождает интерес злоумышленников к проведению различного рода атак, направленных на подделку ЭЦП.

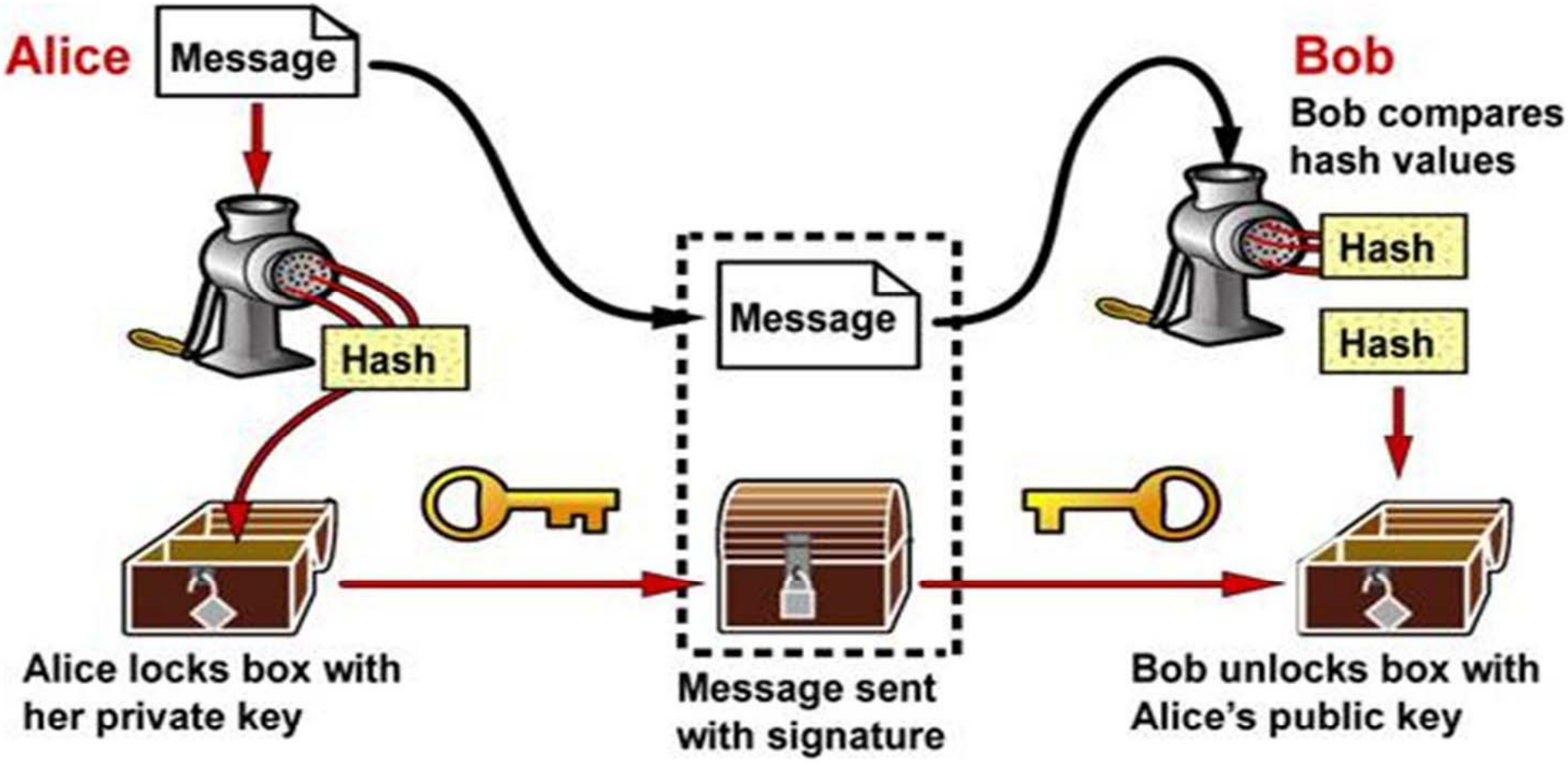
Интернет и СМИ пестрят сообщениями о проблемах, связанных со взломом систем, использующих криптографические методы с открытым ключом.



Центр сертификации GlobalSign признал повреждение своего веб-сервера, но **выдача поддельных сертификатов** и нарушения безопасности пользователей пока ещё не доказаны.



DigiNotar – **сертификационный центр** (Нидерланды), который выдает сертификаты для голландского правительства недавно **обанкротился**. Голландское правительство предупредило пользователей своих сайтов о том, что пока они не могут гарантировать безопасность он-лайн услуг. Было повреждено около 500 сертификатов, это коснулось также пользователей **Facebook, Twitter**, и даже **Microsoft**'s Windows Update. Кроме того, **Моссад**, государственная служба Израиля, **МИ-6** – Великобритании и **ЦРУ** в США также подвергались таким атакам.



✓ Совсем недавно, промежуточный центр сертификации Digicert в Малайзии отменил 22 своих сертификата, так, как использовались слабые ключи шифрования RSA и произошла пропажа некоторых расширенных сертификатов.

✓ Проблемы начались тогда, когда была нанесена атака на важный центр сертификации – американскую компанию Comodo. В заявлении по поводу таких атак, иранской функциональной структурой Comodohaker позже утверждалось, что при выдаче поддельных сертификатов использовался партнерский аккаунт для захвата важных доменов, включая mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org и login.live.com.

✓ Поступило более серьезное обвинение голландской компании Vasco, которая является филиалом DigiNotar. То есть, подозрение упало на ещё одну важную компанию сертификации в введении в обращение сотни поддельных ее сертификатов. Это негативное событие испортило статус компании и она вышла из бизнеса.

✓ Голландский сертификационный центр DigiNotar объявил о взломе сети и выдаче хакерами поддельных сертификатов для нескольких важных доменов, в том числе и для Google и Hotmail. После инцидента, голландское правительство отменило все сертификаты DigiNotar и главный сертификационный центр компании был занесен в черный список браузеров и операционных систем.

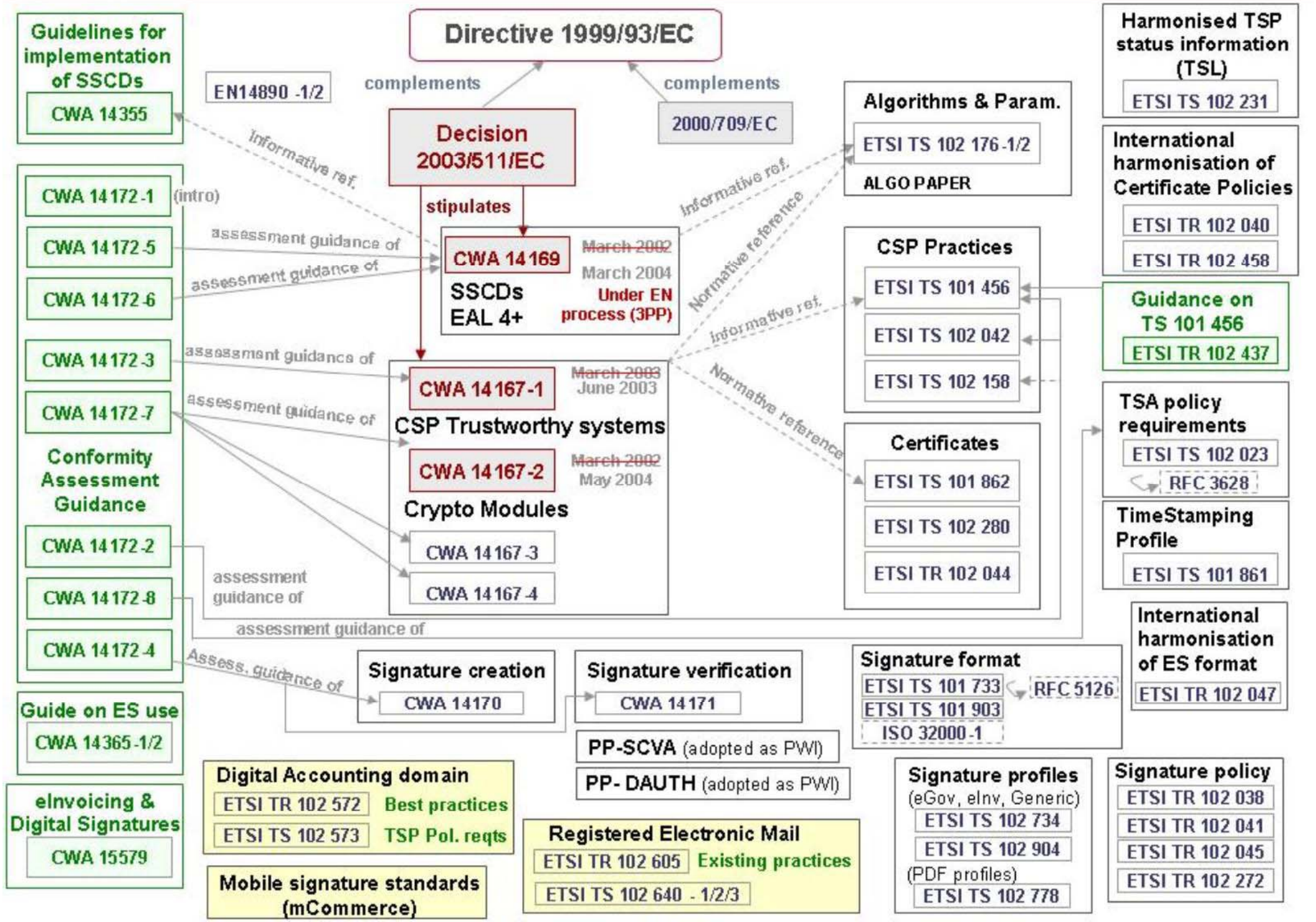
✓ Хакеры атакуют системы дистанционного банковского обслуживания.

✓ Цифровые подписи нескольких недавно обнаруженных троянских программ по причине некорректного отзыва определенного сертификата получали подтверждение подлинности у операционных систем. Троянские программы получили подпись с помощью сертификатов японской компании, о компрометации которых стало известно в июле этого года. После раскрытия факта взлома серверов компании, центр сертификации VeriSign отозвал похищенный сертификат.

✓ Уязвимые версии: RPM Package Manager версии до 4.9.1.2
Описание: Обнаруженные уязвимости позволяют удаленному пользователю выполнить произвольный код на целевой системе.
1. Уязвимость существует из-за ошибки проверки границ данных в функции headerLoad() в файле lib/header.c при обработке смещений регионов. Злоумышленник может обманом заставить пользователя проверить подпись специально сформированного RPM архива, вызвать переполнение буфера и выполнить произвольный код на целевой системе.

✓ В мире около 2 миллиардов браузеров, и все они используют SSL так или иначе для всей электронной коммерции, потому МЫ ДОЛЖНЫ БЫТЬ ОСТОРОЖНЫ.

EU eSignature Standardisation Work overview



Приказ ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи"

Приказ ФСБ РФ от 27 декабря 2011 г. N 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра"

НОРМАТИВНАЯ БАЗА В СФЕРЕ ПРИМЕНЕНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 3 марта 2011 г. № 18 «Об утверждении Положения о порядке применения средств криптографической защиты информации в системах защиты информации»

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 сентября 2011 г. № 68 «О некоторых вопросах применения средств криптографической защиты информации»

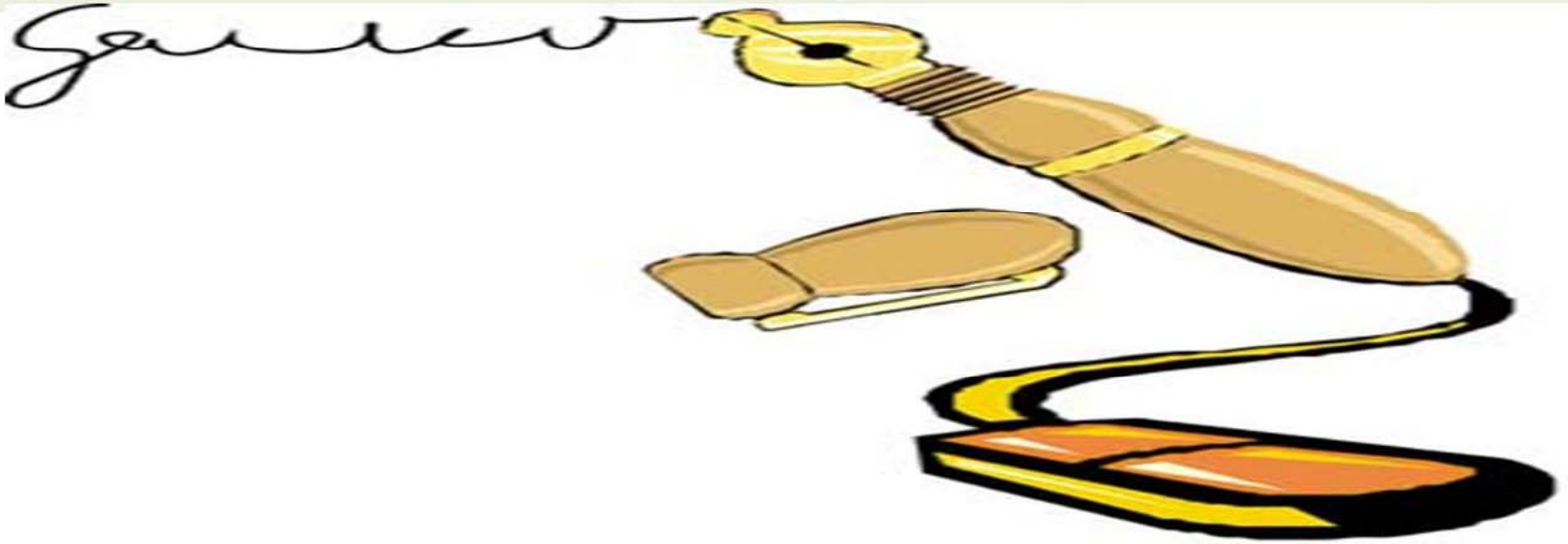
Приложение
к Положению о порядке организации
криптографической защиты информации в системах
защиты информации

ПЕРЕЧЕНЬ

технических нормативных правовых актов и документов, в которых определены требования к средствам криптографической защиты информации и на соответствие которым осуществляется сертификация и государственная экспертиза.

Средства ЭЦП. Криптографические алгоритмы

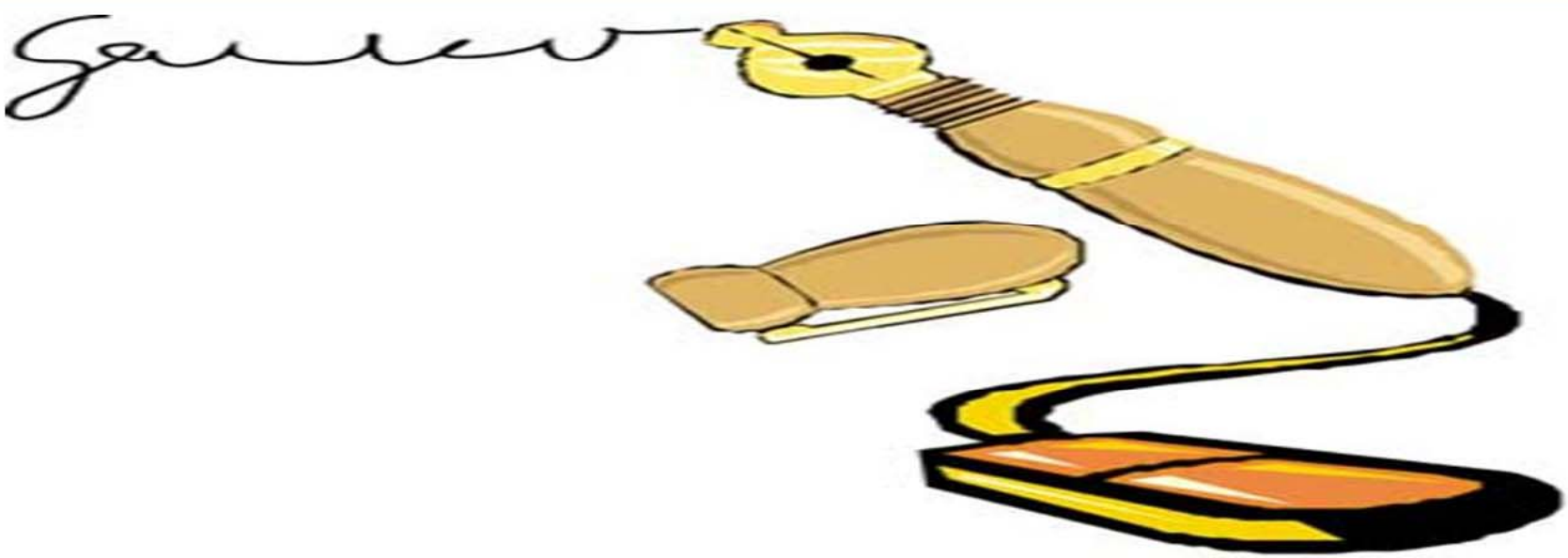
- СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»
- СТБ 1176.1-99 «Информационная технология. Защита информации. Процедура хэширования»
- СТБ П 34.101.45-2011 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых»
- СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»
- СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»



Приложение
к Положению о порядке организации
криптографической защиты информации в системах
защиты информации

ПЕРЕЧЕНЬ
технических нормативных правовых актов и документов, в которых определены требования к средствам криптографической защиты информации и на соответствие которым осуществляется сертификация и государственная экспертиза.
Средства ЭЦП. Защита средств ЭЦП

- СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» или СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации» (задание по безопасности)



СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»

СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации»

1. Общая модель
2. Криптографическая граница
3. Ключевая система
4. Среда безопасности объекта
5. Угрозы (активы, источники и спецификации угроз)
6. Задачи безопасности для объекта и для среды
7. Функциональные требования безопасности
    - Криптографическая поддержка
    - Защита данных пользователя
    - Идентификация и аутентификация
    - Управление безопасностью
8. Защита комплекса средств безопасности
9. Доверенный путь/канал передачи данных
10. Гарантийные требования безопасности
11. Обоснование

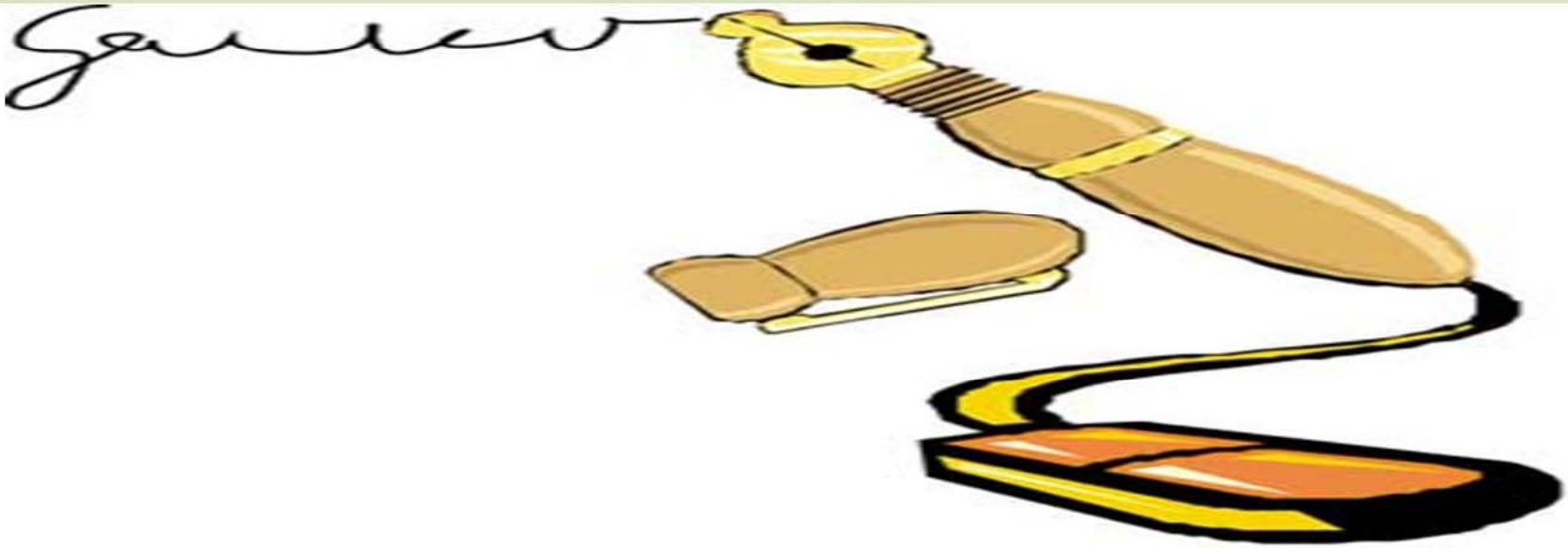
Приложение
к Положению о порядке организации
криптографической защиты информации в системах
защиты информации

ПЕРЕЧЕНЬ

технических нормативных правовых актов и документов, в которых определены требования к средствам криптографической защиты информации и на соответствие которым осуществляется сертификация и государственная экспертиза.

Средства ЭЦП. Безопасность удостоверяющих центров

- СТБ 34.101.48 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров»



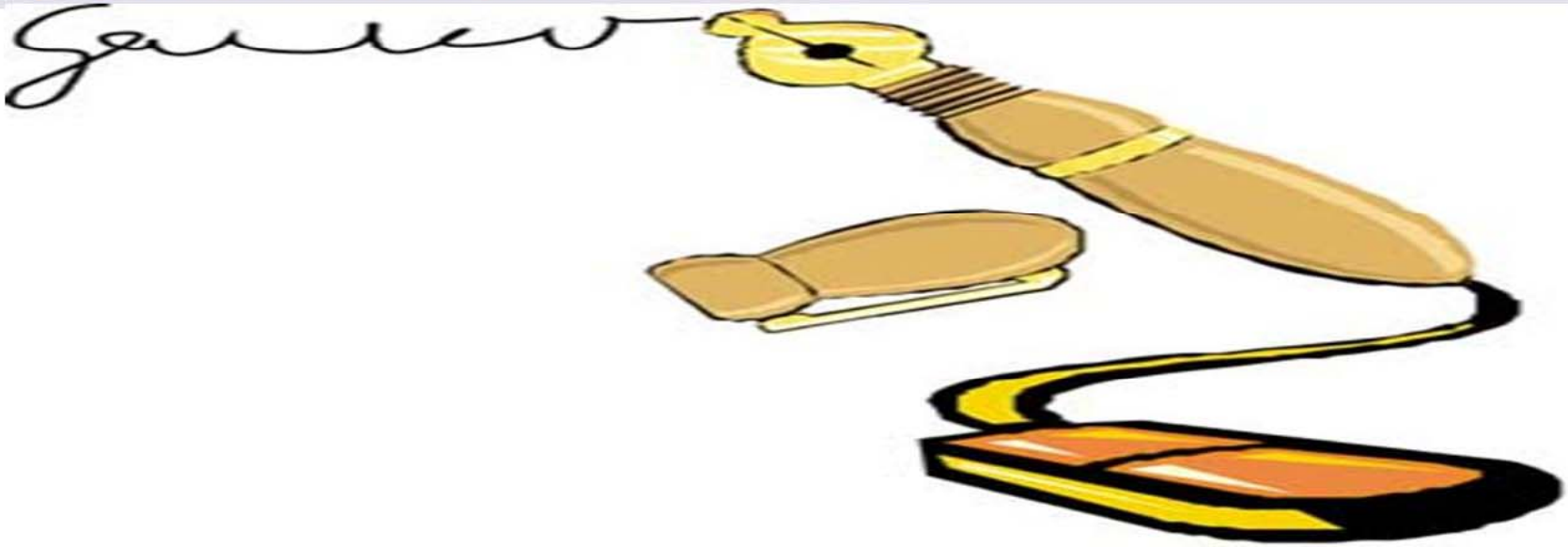
СТБ 34.101.48 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров»

5 Введение в политику применения сертификатов
6 Требования к участникам инфраструктуры открытых ключей к удостоверяющему центру, требования к подписчикам
7 Требования к удостоверяющему центру
7.1 Требования по управлению ключами
7.1.1 Выработка личного ключа подписи удостоверяющего центра
7.1.2 Хранение, резервное копирование и восстановление личного ключа подписи удостоверяющего центра
7.1.3 Распространение открытых ключей удостоверяющего центра
7.1.4 Депонирование личного ключа удостоверяющего центра
7.1.5 Использование личного ключа удостоверяющего центра
7.1.6 Окончание срока действия личного ключа удостоверяющего центра
7.1.7 Управление средством ЭЦП, используемым для издания сертификатов
7.2 Требования по управлению сертификатами
7.2.1 Регистрация субъекта
7.2.2 Возобновление сертификата и обновление данных
7.2.3 Издание сертификата
7.2.4 Распространение нормативных и организационных
7.2.6 Отзыв и приостановка действия сертификата
7.3 Управление и деятельность УЦ
7.3.1 Управление безопасностью
7.3.2 Классификация и управление активами
7.3.3 Безопасность персонала
7.3.4 Физическая безопасность и безопасность окружени
7.3.8 Восстановление при сбоях и обеспечение непрерывности деятельности
7.3.9 Прекращение функционирования УЦ
7.3.11 Сохранение информации, касающейся сертификатов

Приложение
к Положению о порядке организации
криптографической защиты информации в системах
защиты информации

ПЕРЕЧЕНЬ
технических нормативных правовых актов и документов, в которых определены требования к средствам криптографической защиты информации и на соответствие которым осуществляется сертификация и государственная экспертиза.
Средства ЭЦП. Форматы данных

- СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»
- СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией» с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011
- СТБ 34.101.19-2009 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»
- СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»



НОВЫЕ СТАНДАРТЫ РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (стадия утверждения)

- **СТБ 34.101.17 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»**
- **СТБ 34.101.19 «Информационные технологии и безопасность. Формат сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»**
- **СТБ 34.101.23 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»**
- **СТБ 34.101.26 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)»**
- **СТБ 34.101.47 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»**
- **СТБ 34.101.48 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров»**
- **СТБ 34.101.49 «Информационные технологии и безопасность. Формат карточки открытого ключа»**
- **СТБ П 34.101.50 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий»**