

РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ

**Банковские технологии
ТЕХНОЛОГИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ
Термины и определения**

**Банкаўскія тэхналогіі
ТЭХНАЛОГІЯ ЭЛЕКТРОННАГА ЛІЧБАВАГА ПОДПІСУ
Тэрміны і азначэнні**

**Национальный банк Республики Беларусь
Минск**

УДК [681.3.067:003]:006.354(476)

Ключевые слова: ключ личный подписи, ключ проверки подписи открытый, подпись электронная цифровая, средства электронной цифровой подписи, карточка открытого ключа, сертификат открытого ключа

МКС 01.040.03

Предисловие

1 РАЗРАБОТАН Государственным центром безопасности информации при Президенте Республики Беларусь, ЗАО «Авест»

2 ВНЕСЕН Управлением безопасности и защиты информации Национального банка Республики Беларусь

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Совета директоров Национального банка Республики Беларусь от «___» 2004 г. №

4 ВВЕДЕН ВПЕРВЫЕ

Настоящий руководящий документ не может быть тиражирован и распространен без разрешения Национального банка Республики Беларусь

Издан на русском языке

Содержание

Введение.....	IV
1 Область применения	1
2 Нормативные ссылки	1
3 Обозначения и сокращения	1
4 Основные понятия.....	1
5 Генерация и управление ключами ЭЦП	3
6 Применение технологии ЭЦП для обеспечения подлинности электронных документов	5
Алфавитный указатель терминов	7
Приложение А	8

Введение

Установленные в руководящем документе термины расположены в систематизированном порядке, отражающем систему понятий в данной области знаний. Для каждого понятия установлен один стандартизованный термин.

В алфавитном указателе данные термины приведены отдельно с указанием номера статьи.

РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ

**Банковские технологии
ТЕХНОЛОГИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ
Термины и определения****Банкаўскія тэхналогіі
ТЭХНАЛОГІЯ ЭЛЕКТРОННАГА ЛІЧБАВАГА ПОДПІСУ
Тэрміны і азначэнні**

Дата введения 2004–07–01

1 Область применения

Настоящий руководящий документ устанавливает термины и определения основных понятий в областях, связанных с применением технологии электронной цифровой подписи.

Термины, установленные настоящим руководящим документом, обязательны для применения во всех видах документов, относящихся к банковским технологиям, связанным с применением технологии электронной цифровой подписи.

2 Нормативные ссылки

В настоящем руководящем документе использована ссылка на руководящий документ:

РД РБ 07040.1201-2003 Банковские технологии. Средства электронной цифровой подписи программные. Общие требования

3 Обозначения и сокращения

В настоящем руководящем документе применяют следующие обозначения и сокращения:

ЭЦП – электронная цифровая подпись

4 Основные понятия**4.1****алгоритм ЭЦП**

Совокупность алгоритмов вычисления открытого ключа проверки подписи, выработки ЭЦП и проверки ЭЦП, установленных в государственных стандартах Республики Беларусь и обладающих таким свойством, что при фиксированных значениях параметров алгоритма ЭЦП для произвольно выбранного открытого ключа проверки подписи без знания соответствующего ему личного ключа подписи в течение срока криптографической стойкости алгоритма ЭЦП практически невозможно найти данные и их ЭЦП, использование которых в алгоритме проверки ЭЦП дает положительный результат

4.2

личный ключ подписи

Набор символов, принадлежащий конкретному лицу и используемый при выработке ЭЦП и соответствующего ему открытого ключа проверки подписи

[1]

4.3

открытый ключ проверки подписи

Набор символов, доступный для всех заинтересованных лиц и используемый при проверке ЭЦП

[1]

4.4

карточка открытого ключа проверки подписи

Документ на бумажном носителе, содержащий значение открытого ключа проверки подписи и подтверждающий его принадлежность какому-либо физическому или юридическому лицу

[1]

4.5

срок криптографической стойкости алгоритма ЭЦП

Срок, в течение которого при фиксированных значениях параметров алгоритма ЭЦП для произвольно выбранного открытого ключа проверки подписи без знания соответствующего ему личного ключа подписи практически невозможно найти данные и их ЭЦП, использование которых в алгоритме проверки ЭЦП дает положительный результат

4.6

средства ЭЦП

Программные и (или) технические средства, реализующие все или некоторые алгоритмы из совокупности алгоритма ЭЦП и имеющие сертификат соответствия или удостоверение о признании сертификата, выданного в Национальной системе сертификации Республики Беларусь

[1]

4.7

ЭЦП

Набор символов, вырабатываемый средствами ЭЦП и являющийся неотъемлемой частью электронного документа

[1]

4.8

процедура выработки ЭЦП

Процедура, определяющая исходные данные, параметры, переменные, алгоритм и результат выработки ЭЦП

4.9

процедура проверки ЭЦП

Процедура, определяющая исходные данные, параметры, переменные, алгоритм и результат проверки ЭЦП

4.10

технология ЭЦП

Совокупность процедур, методов, программных и технических средств, нормативных и правовых документов, относящихся к применению алгоритмов ЭЦП на практике

5 Генерация и управление ключами ЭЦП

5.1

личный ключ подписи, соответствующий данному открытому ключу проверки подписи

Личный ключ подписи, который был использован при вычислении значения данного открытого ключа проверки подписи в соответствии с алгоритмом ЭЦП

5.2

владелец личного ключа подписи

Конкретное физическое или юридическое лицо, осуществившее выработку этого ключа и соответствующего ему открытого ключа проверки подписи путем применения средств ЭЦП, а также осуществляющее его хранение и использование.

Примечание – Владелец личного ключа подписи в своих интересах должен хранить его в тайне и обеспечивать его защиту от случайного уничтожения или модификации

[1]

5.3

срок использования личного ключа подписи

Промежуток времени, в течение которого владелец личного ключа подписи предполагает использовать этот ключ для выработки ЭЦП

5.4

владелец открытого ключа проверки подписи

Физическое или юридическое лицо, являющееся владельцем личного ключа подписи, соответствующего данному открытому ключу проверки подписи

5.5

пользователь открытого ключа проверки подписи

Лицо, которому владельцем личного ключа подписи, уполномоченным им лицом или удостоверяющим центром предоставлена карточка или сертификат открытого ключа проверки подписи для проверки ЭЦП.

Примечание - Пользователь открытого ключа проверки подписи обязан обеспечивать идентичность используемого им открытого ключа проверки подписи тому ключу, который зафиксирован в карточке или сертификате открытого ключа проверки подписи

5.6

срок действия открытого ключа проверки подписи

Промежуток времени, в течение которого предполагается использовать этот ключ для проверки ЭЦП.

Примечание - Срок действия открытого ключа проверки подписи не должен превышать срок криптографической стойкости алгоритма ЭЦП

5.7

время прекращения действия открытого ключа проверки подписи

Момент времени, начиная с которого применение данного открытого ключа для проверки ЭЦП не позволяет сделать вывод о целостности и подлинности проверяемых данных только на основании этой проверки.

Примечание – Время прекращения действия открытого ключа проверки подписи наступает либо при истечении срока его действия, либо с момента отзыва этого ключа

5.8

отзыв открытого ключа проверки подписи

Процедура, направленная на оповещение пользователей открытого ключа проверки подписи о времени прекращения его действия, наступившем до окончания срока действия этого открытого ключа проверки подписи

5.9

ключи ЭЦП

Личный ключ подписи и открытый ключ проверки подписи

5.10

процедура генерации ключей ЭЦП

Процедура, реализующая алгоритм генерации личного ключа подписи и вычисление соответствующего ему открытого ключа проверки подписи

5.11

процедуры управления ключами ЭЦП

Совокупность процедур, обеспечивающих выполнение функций управления ключами ЭЦП

5.12

компрометация личного ключа подписи

Событие, состоящее в том, что информация о значении личного ключа подписи стала известна какому-либо лицу, кроме его владельца.

Примечание – Личный ключ подписи может считаться скомпрометированным в случае, когда владелец этого личного ключа подписи имеет подозрения в связи с возможностью его компрометации

5.13

уничтожение личного ключа подписи

Уничтожение значения личного ключа подписи, позволяющее гарантировать невозможность восстановления полной или частичной информации о его значении

5.14

регистрационный центр

Организация, выполняющая функции, связанные с достоверным подтверждением принадлежности открытого ключа проверки подписи конкретному физическому или

юридическому лицу

5.15

сертификат открытого ключа

Электронный документ, созданный удостоверяющим центром и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа конкретному физическому или юридическому лицу

5.16

список отозванных сертификатов

Электронный документ, содержащий информацию о сертификатах открытых ключей, действие которых прекращено или приостановлено до истечения срока действия открытых ключей, указанных в сертификатах

5.17

отзыв сертификата открытого ключа

Процедура, направленная на включение удостоверяющим центром сертификата открытого ключа в список отозванных сертификатов и предоставление доступа к этому списку пользователям открытых ключей

5.18

удостоверяющий центр

Организация, выполняющая функции создания, распространения и хранения сертификатов открытых ключей и списков отозванных сертификатов

5.19

срок действия сертификата открытого ключа

Промежуток времени, в течение которого удостоверяющий центр гарантирует подлинность сертификата и актуальность его состояния

6 Применение технологии ЭЦП для обеспечения подлинности электронных документов

6.1

электронный документ

Информация, зафиксированная на машинном носителе и соответствующая требованиям, установленным Законом Республики Беларусь «Об электронном документе»

РД РБ 07040.1201

6.2

подтверждение подлинности электронного документа

Процедура проверки ЭЦП этого документа, путем применения средств ЭЦП с использованием действующих открытых ключей проверки подписей лиц, подписавших электронный документ

6.3

подлинный электронный документ

Электронный документ, подтверждение подлинности которого дает положительный результат

6.4

создание бумажной копии электронного документа

Создание документа на бумажном носителе по содержанию идентичного подлинному электронному документу

6.5

среда эксплуатации программного средства ЭЦП

Совокупность аппаратного, аппаратно–программного и программного обеспечения, необходимого для функционирования программного средства электронной цифровой подписи

РД РБ 07040.1201

6.6

активы программного средства ЭЦП

Данные программного средства ЭЦП, нарушение конфиденциальности или целостности которых снижает его безопасность

РД РБ 07040.1201

Алфавитный указатель терминов

Активы программного средства ЭЦП.....	6.6
Алгоритм ЭЦП.....	4.1
Владелец личного ключа подписи.....	5.2
Владелец открытого ключа проверки подписи.....	5.4
Время прекращения действия открытого ключа проверки подписи.....	5.7
Карточка открытого ключа проверки подписи.....	4.4
Ключи ЭЦП.....	5.9
Компрометация личного ключа подписи.....	5.12
Личный ключ подписи.....	4.2
Отзыв открытого ключа проверки подписи.....	5.8
Отзыв сертификата открытого ключа.....	5.17
Открытый ключ проверки подписи.....	4.3
Подлинный электронный документ.....	6.3
Подтверждение подлинности электронного документа.....	6.2
Пользователь открытого ключа проверки подписи.....	5.3
Процедура выработки ЭЦП.....	4.8
Процедура генерации ключей ЭЦП.....	5.10
Процедура проверки ЭЦП	4.9
Процедуры управления ключами ЭЦП.....	5.11
Регистрационный центр.....	5.14
Сертификат открытого ключа.....	5.15
Создание бумажной копии электронного документа.....	6.4
Список отозванных сертификатов.....	5.16
Среда эксплуатации программного средства ЭЦП.....	6.5
Средства ЭЦП.....	4.6
Срок действия открытого ключа проверки подписи.....	5.6
Срок действия сертификата открытого ключа.....	5.19
Срок использования личного ключа подписи.....	5.3
Срок криптографической стойкости алгоритма ЭЦП.....	4.5
Технология ЭЦП.....	4.10
Удостоверяющий центр.....	5.18
Уничтожение личного ключа подписи.....	5.13
Электронный документ.....	6.1
ЭЦП.....	4.7

Приложение А
(информационное)

Библиография

[1] Закон Республики Беларусь «Об электронном документе» – Национальный реестр правовых актов Республики Беларусь, №4-99