

**РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ**

---

Банковские технологии  
**СРЕДСТВА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ПРОГРАММНЫЕ**  
Общие требования

Банкаўскія тэхналогіі  
**СРОДКІ ЭЛЕКТРОННАГА ЛІЧБАВАГА ПОДПІСУ ПРАГРАМНЫЯ**  
Агульныя патрабаванні

**Издание официальное**

УДК

**Ключевые слова:** ключ личный подписи, ключ проверки подписи открытый, подпись электронная цифровая, средство электронной цифровой подписи программное

ОКС 35.240.40

---

### **Предисловие**

1 РАЗРАБОТАН Государственным центром безопасности информации, Учреждением Белорусского государственного университета «Национальный научно-исследовательский центр прикладных проблем математики и информатики», ООО «Энигма», 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 03 марта 2003 г. № 75

4 ВВЕДЕН ВПЕРВЫЕ

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

---

Издан на русском языке

**Содержание**

|  |   |
|--|---|
| 1 Область применения .....   | 1 |
| 2 Нормативные ссылки .....   | 1 |
| 3 Определения .....  | 2 |
| 4 Обозначения и сокращения .....   | 2 |
| 5 Состав ПС ЭЦП .....  | 3 |
| 6 Требования к процедурам выработки и проверки ЭЦП .....   | 3 |
| 7 Требования к процедурам генерации параметров $p$ , $q$ , $a$ .....                                     | 3 |
| 8 Требования к параметрам процедур выработки и проверки ЭЦП.....   | 4 |
| 9 Требования к процедурам выработки псевдослучайных данных с<br>использованием секретного параметра..... | 4 |
| 10 Требования к физическому датчику случайных чисел .....  | 4 |
| 11 Требования к процедурам генерации личного ключа подписи и<br>открытого ключа проверки подписи .....   | 4 |
| 12 Активы ПС ЭЦП.....  | 5 |
| 13 Требования по защите ПС ЭЦП от несанкционированного доступа .....                                     | 5 |
| 14 Требования к документации .....   | 6 |

## **РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ**

---

Банковские технологии  
**СРЕДСТВА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ПРОГРАММНЫЕ**  
Общие требования

Банкаўскія тэхналогіі  
**СРОДКІ ЭЛЕКТРОННАГА ЛІЧБАВАГА ПОДПІСУ ПРАГРАМНЫЯ**  
Агульныя патрабаванні

---

Дата введения 2003-04-01

### **1 Область применения**

Настоящий руководящий документ распространяется на программные средства электронной цифровой подписи, предназначенные для подтверждения подлинности и целостности электронных документов и данных.

Настоящий руководящий документ устанавливает общие требования к программным средствам электронной цифровой подписи, реализующим стандарт СТБ 1176.2, включая требования по их безопасному применению.

Настоящий руководящий документ применяется при разработке и сертификации программных средств электронной цифровой подписи.

### **2 Нормативные ссылки**

В настоящем стандарте использованы ссылки на следующие нормативные документы:

СТБ 1176.1-99 Информационная технология. Защита информации. Функция хэширования

СТБ 1176.2-99 Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи

СТБ 34.101.1-2001 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ 19.202-78 Единая система программной документации. Спецификация. Требования к содержанию и оформлению

ГОСТ 19.401-2000 Единая система программной документации. Текст программы. Требования к содержанию, оформлению и контролю качества

ГОСТ 19.402-2000 Единая система программной документации. Описание программы. Требования к содержанию, оформлению и контролю качества

ГОСТ 19.504-79 Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению

ГОСТ 19.505-79 Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению

### 3 Определения

В настоящем руководящем документе применяют следующие термины с соответствующими определениями:

**Активы программного средства электронной цифровой подписи** – данные программного средства электронной цифровой подписи, нарушение конфиденциальности или целостности которых снижает его безопасность.

**Личный ключ подписи** – набор символов, принадлежащий конкретному лицу и используемый при выработке электронной цифровой подписи.

**Открытый ключ проверки подписи** – набор символов, доступный для всех заинтересованных лиц и используемый при проверке электронной цифровой подписи.

**Программные средства электронной цифровой подписи** – программные средства, обеспечивающие выработку и (или) проверку электронной цифровой подписи и имеющие сертификат соответствия или удостоверение о признании сертификата, выданного в Национальной системе сертификации Республики Беларусь.

**Среда эксплуатации программного средства электронной цифровой подписи** – совокупность аппаратного, аппаратно–программного и программного обеспечения, необходимого для функционирования программного средства электронной цифровой подписи.

**Электронный документ** - информация, зафиксированная на машинном носителе и соответствующая требованиям, установленным Законом Республики Беларусь «Об электронном документе».

**Электронная цифровая подпись** - набор символов, вырабатываемый средствами электронной цифровой подписи и являющийся неотъемлемой частью электронного документа.

### 4 Обозначения и сокращения

В настоящем руководящем документе применяют следующие обозначения и сокращения:

ПС ЭЦП – программное средство электронной цифровой подписи;

ЭЦП – электронная цифровая подпись;

*d* – переменная, определенная в пункте 7.3.2 СТБ 1176.2;

$d_0, \dots, d_t$ ;  $r_0, \dots, r_s$  – переменные, определенные в пункте 7.2.3 СТБ 1176.2;  
 $k$  – целое число, определенное в подразделе 5.2 СТБ 1176.2;  
 $L, H$  – параметры, определенные в разделах 3 и 5 СТБ 1176.1;  
 $p, q, a, l, r$  – параметры, определенные в разделах 4 и 7 СТБ 1176.2;  
 $z_1, \dots, z_{31}$  – инициализирующее значение датчика случайных чисел, определенное в пункте 7.2.1 СТБ 1176.2.

## 5 Состав ПС ЭЦП

ПС ЭЦП включает программные модули, реализующие следующие процедуры:

- выработки ЭЦП;
- проверки ЭЦП;
- генерации параметров  $p, q, a$ ;
- взаимодействия с физическим датчиком случайных чисел;
- генерации псевдослучайных данных с использованием секретного параметра;
- генерации личного ключа подписи и соответствующего ему открытого ключа проверки подписи.

В ПС ЭЦП должна быть реализована, по меньшей мере, одна из процедур выработки или проверки ЭЦП. Наличие реализаций других процедур определяется в зависимости от функционального назначения ПС ЭЦП.

В ПС ЭЦП могут быть реализованы дополнительные процедуры и функции, например, функции пользовательского интерфейса, механизмы защиты.

ПС ЭЦП должно быть разработано в виде одного или нескольких загрузочных модулей.

## 6 Требования к процедурам выработки и проверки ЭЦП

Процедуры выработки и проверки ЭЦП, реализованные в ПС ЭЦП, должны соответствовать процедурам, установленным в СТБ 1176.2. Процедура вычисления значения функции хэширования, используемая в ПС ЭЦП для выработки или проверки ЭЦП, должна соответствовать процедуре, установленной в СТБ 1176.1.

## 7 Требования к процедурам генерации параметров $p, q, a$

Процедуры генерации параметров  $p, q, a$ , реализованные в ПС ЭЦП, должны соответствовать процедурам, установленным в СТБ 1176.2. В процедурах генерации параметров должна быть предусмотрена возможность

сохранять значения последовательностей  $z_1, \dots, z_{31}$ ;  $d_0, \dots, d_i$ ;  $r_0, \dots, r_s$  и числа  $d$  для проверки того, что параметры  $p$ ,  $q$ ,  $a$  сгенерированы в соответствии с СТБ 1176.2.

## **8 Требования к параметрам процедур выработки и проверки ЭЦП**

Процедуры выработки и проверки ЭЦП, реализованные в ПС ЭЦП, в качестве параметров используют значения  $p$ ,  $q$ ,  $a$ ,  $l$ ,  $r$ , а также числа  $L$  и  $H$ , являющиеся параметрами используемой в ПС ЭЦП процедуры вычисления значения функции хэширования.

Если параметры  $p$ ,  $q$ ,  $a$ ,  $l$ ,  $r$ ,  $L$  и  $H$  используются в ПС ЭЦП в виде констант, то их значения должны быть приведены в эксплуатационной документации на ПС ЭЦП. Кроме того, в этом случае в эксплуатационной документации на ПС ЭЦП должны быть приведены значения последовательностей  $z_1, \dots, z_{31}$ ;  $d_0, \dots, d_i$ ;  $r_0, \dots, r_s$  и числа  $d$ , которые были использованы для генерации параметров  $p$ ,  $q$ ,  $a$ .

Если параметры  $p$ ,  $q$ ,  $a$ ,  $l$ ,  $r$ ,  $L$  и  $H$  используются в ПС ЭЦП как внешние данные, то в эксплуатационной документации на ПС ЭЦП должен быть описан формат их представления. Кроме того, в этом случае в эксплуатационной документации на ПС ЭЦП должна быть определена возможность получения доступа к значениям последовательностей  $z_1, \dots, z_{31}$ ;  $d_0, \dots, d_i$ ;  $r_0, \dots, r_s$  и числа  $d$ , которые были использованы для генерации параметров  $p$ ,  $q$ ,  $a$ .

## **9 Требования к процедуре выработки псевдослучайных данных с использованием секретного параметра**

Используемая в ПС ЭЦП процедура выработки псевдослучайных данных с использованием секретного параметра должна удовлетворять требованиям нормативных документов, действующих в Республике Беларусь.

## **10 Требования к физическому датчику случайных чисел**

Используемый в ПС ЭЦП физический датчик случайных чисел должен удовлетворять требованиям нормативных документов, действующих в Республике Беларусь.

## **11 Требования к процедуре генерации личного ключа подписи и открытого ключа проверки подписи**

Значение личного ключа подписи должно генерироваться с помощью физического датчика случайных чисел или псевдослучайным методом с использованием секретного параметра в соответствии с СТБ 1176.2.

Открытый ключ проверки подписи вычисляется на основании личного ключа подписи в соответствии с СТБ 1176.2

## 12 Активы ПС ЭЦП

К активам ПС ЭЦП относятся:

- личный ключ подписи;
- открытый ключ проверки подписи;
- параметры  $p, q, a, l, r, L$  и  $H$ ;
- переменная  $k$ ;
- секретный параметр, используемый в процедуре выработки псевдослучайных данных.

Для безопасного применения ПС ЭЦП должна обеспечиваться конфиденциальность следующих активов:

- личного ключа подписи;
- переменной  $k$ ;
- секретного параметра, используемого в процедуре выработки псевдослучайных данных.

Для безопасного применения ПС ЭЦП должна обеспечиваться целостность следующих активов:

- личного ключа подписи;
- открытого ключа проверки подписи;
- параметров  $p, q, a, l, r, L$  и  $H$ .

Если в ПС ЭЦП для обеспечения конфиденциальности и контроля целостности активов используются криптографические алгоритмы, то они должны удовлетворять требованиям нормативных документов, действующих в Республике Беларусь.

## 13 Требования по защите ПС ЭЦП от несанкционированного доступа

ПС ЭЦП и его активы должны быть защищены от несанкционированного доступа.

Защита активов ПС ЭЦП во время его исполнения должна обеспечиваться ПС ЭЦП, средой эксплуатации и (или) организационными мероприятиями.

Защита ПС ЭЦП и его активов при хранении должна обеспечиваться средой эксплуатации и (или) организационными мероприятиями

Если ПС ЭЦП входит в состав системы информационных технологий, то требования по защите ПС ЭЦП от несанкционированного доступа к информации должны быть включены в документ «Задание по обеспечению безопасности» на систему информационных технологий, разрабатываемый в соответствии с СТБ 34.101.1.

## 14 Требования к документации

К ПС ЭЦП должна быть разработана следующая документация:

- программный документ «Спецификация»;
- программный документ «Текст программы»;
- программный документ «Описание программы»;
- эксплуатационные документы «Руководство программиста» или «Руководство оператора».

В программных документах к ПС ЭЦП должны быть описаны механизмы защиты активов, реализованные в ПС ЭЦП.

Эксплуатационные документы к ПС ЭЦП должны содержать информацию достаточную для правильного применения реализованных в ПС ЭЦП механизмов защиты.

Программный документ «Спецификация» должен соответствовать требованиям ГОСТ 19.202.

Программный документ «Текст программы» должен соответствовать требованиям ГОСТ 19.401 и дополнительно должен содержать подробные комментарии, которые определяют соответствие между операторами программы и шагами алгоритмов, приведенных в СТБ 1176.2.

Программный документ «Описание программы» должен соответствовать требованиям ГОСТ 19.402.

Эксплуатационный документ «Руководство программиста» должен соответствовать требованиям ГОСТ 19.504.

Эксплуатационный документ «Руководство оператора» должен соответствовать требованиям ГОСТ 19.502.

Дополнительно к ПС ЭЦП может быть разработана другая документация.