Министерство образования Республики Беларусь
Белорусский государственный университет
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ПРИКЛАДНЫХ ПРОБЛЕМ МАТЕМАТИКИ И ИНФОРМАТИКИ

УТВЕРЖДАЮ
Директор НИИ прикладных проблем
математики и информатики

Ю.С.Харин
«___» _____ 2022 г.

МЕТОДИКА ИСПЫТАНИЙ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СТБ 1176.2-99

МИ.11762.10.01

Листов 44

Минск 2022

Предисловие

Настоящая методика испытаний предназначена для использования в испытательных лабораториях при проведении сертификационных испытаний средств криптографической защиты информации на соответствие требованиям СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»

Содержание

1 Нормативные ссылки

В настоящем документе использованы ссылки на следующие стандарты:

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».

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 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности».

СТБ 34.101.77-2020 «Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции».

2 Термины, обозначения и сокращения

В настоящем документе применяются термины и обозначения СТБ 1176.2, а также следующие обозначения и сокращения:

Σ^n	множество всех слов длины n в алфавите Σ;
Σ^*	множество всех слов конечной длины в алфавите Σ (включая пустое слово длины 0);
Σ^{n*}	множество всех слов из Σ^*, длина которых кратна n;
$\ldots\mathtt{43210}_{\overleftarrow{16}}$	представление $u \in \{0,1\}^{4*}$ шестнадцатеричным словом, октеты которого записаны справа налево (т.е. в порядке big-endian) и у которого последовательным четырем символам u соответствует один шестнадцатеричный символ (например, $10100010 = \mathtt{A2}_{\overleftarrow{16}}$);
$a \leftarrow u$	присвоение переменной a значения u;
ЕСПД	единая система программной документации;
СКЗИ	средство криптографической защиты информации;
ЭЦП	электронная цифровая подпись.

3 Объект и цель испытаний

На испытания представляется средство криптографической защиты информации (СКЗИ), реализующее криптографические алгоритмы СТБ 1176.2, и документация на СКЗИ.

Целью испытаний является проверка соответствия объекта испытаний требованиям СТБ 1176.2.

4 Требования к объекту испытаний

К программе объекта испытаний предъявляются следующие требования, подлежащие проверке во время проведения испытаний:

– в программе должны быть точно и полно реализовываны криптографические алгоритмы СТБ 1176.2, поддерживаемые объектом испытаний;

– программа, реализующая криптографические алгоритмы и требования СТБ 1176.2, не должна содержать недокументированные возможности.

Документация на объект испытаний должна включать документы «Спецификация», «Текст программы» и может включать документы «Описание программы», «Руководство программиста» и другие документы. Документация может быть разработана в соответствии с требованиями единой системы программной документации (ЕСПД).

5 Средства и порядок испытаний

5.1 Общие сведения

Испытания программы состоят из трех этапов:

1 Анализ документации.

2 Тестирование программы.

3 Анализ исходных текстов программы.

Выполнение этапа 1 осуществляется экспертами по анализу документации, выполнение этапа 2 — экспертами по тестированию, а выполнение этапа 3 — экспертами по анализу исходных текстов. К проведению испытаний должно быть привлечено не менее двух экспертов по анализу исходных текстов и один или более эксперт по тестированию. К анализу документации должен быть привлечен, по крайней мере, один эксперт по анализу исходных текстов программ.

По результатам выполнения этапа испытаний эксперт оформляет протокол результатов проверок: протокол анализа документации, протокол тестирования, протокол анализа исходных текстов. В протоколе эксперт делает вывод о соответствии (не соответствии) программы требованиям СТБ 1176.2. Если программа не поддерживает некоторые алгоритмы, определенные в СТБ 1176.2, то в протоколе делается соответствующее примечание. Примеры оформления протоколов приводятся в приложениях А, Б, В. Допускается оформления протоколов в иной форме, но с обязательным указанием результатов по каждой проводимой проверке и вывода о соответствии (не соответствии).

Если в испытуемой программе используются реализации алгоритмов СТБ 1176.2, которые в составе других программ имеют действующие сертификаты соответствия требованиям СТБ 1176.2, то проверки по тестированию и анализу исходных текстов для данных реализаций могут не проводиться. При этом для подтверждения соответствия объекта испытаний требованиям СТБ 1176.2 экспертом оформляется протокол проверки совпадения контрольных характеристик (хэш-значений) файлов реализации испытуемой программы с контрольными характеристиками соответствующих файлов, указанными в сертификатах соответствия.

На основании протоколов результатов проверок оформляется протокол испытаний, обобщающий результаты испытаний программы. В протоколе испытаний вывод о соот-

ветствии программы требованиям СТБ 1176.2 делается тогда и только тогда, когда вывод о соответствии содержится во всех протоколах результатов проверок. Оформление протокола испытаний проводится в соответствии с требованиями технических нормативно-правовых актов в области сертификации продукции, а также документации, применяемой в испытательной лаборатории.

5.2 Анализ документации

Эксперт проводит анализ документации путем проверки соответствия документации программе объекта испытаний. Такой анализ состоит в получении экспертных заключений, касающихся проверки следующих документов:

- спецификация (см. п. 6.1.1);
- текст программы (см. п. 6.1.2);
- описание программы (см. п. 6.1.3);
- руководство программиста (см. п. 6.1.4).

Анализ документов «Описание программы» и «Руководство программиста» производится в случае их наличия.

5.3 Тестирование

Эксперт проводит тестирование путем выполнения испытуемой программы для некоторого набора проверочных входных значений и сравнения полученных результатов с истинными. Истинные результаты, используемые при тестировании, формируются с помощью эталонной реализации.

Эталонной считается реализация, которая ранее успешно прошла сертификационные испытания на соответствие СТБ 1176.2 или которая удовлетворяет следующим условиям:

1 Проведен анализ исходных текстов программ эталонной реализации. К анализу привлекались, по меньшей мере, два независимых эксперта. Использовалась методика анализа исходных текстов, определенная в п. 6.3.

2 Проведено тестирование эталонной реализации. При тестировании использовались две другие независимые реализации. Использовались тесты, определенные в п. 6.2.

Тестированию подлежат криптографические алгоритмы, реализованные в программе и определенные в СТБ 1176.2, включая:

- алгоритм выработки ЭЦП (см. п. 6.2.1);
- алгоритм проверки ЭЦП (см. п. 6.2.1);
- алгоритм генерации параметров p и q (см. п. 6.2.2);
- алгоритм генерации параметра a (см. п. 6.2.3).

Если программа не реализует некоторые из алгоритмов, определенных в СТБ 1176.2, то тесты для них не выполняются.

Для организации тестирования в исходные тексты программы допускается вносить изменения и дополнения, касающиеся:

- способа чтения входных данных;
- способа записи выходных данных.

При внесении модификаций в исходные тексты должен быть проведен анализ корректности внесенных изменений.

При успешном выполнении тест возвращает признак `УСПЕХ`, иначе — `ОШИБКА`. Если при тестировании программы для некоторых входных значений получены результаты отличные от истинных значений, то эксперт по тестированию должен указать эти входные

значения программы и результат ее работы, а также, по требованию, результаты промежуточных вычислений экспертам по анализу исходных текстов.

5.4 Анализ исходных текстов

Эксперт проводит анализ исходных текстов путем проверки корректности реализации в испытуемой программе криптографических алгоритмов СТБ 1176.2. Такой анализ состоит в получении экспертных заключений, касающихся:

- корректности использования локальных переменных (см. п. 6.3.1);
- корректности использования глобальных переменных (см. п. 6.3.2);
- корректности использования констант (см. п. 6.3.3);
- корректности программной логики функций программы (см. п. 6.3.4);
- корректности вызова стандартных функций (см. п. 6.3.5);
- корректности вызова функций программы (см. п. 6.3.6);
- корректности обработки исключительных ситуаций (см. п. 6.3.7);
- корректности реализации криптографических примитивов (см. п. 6.3.8);
- корректности реализации криптографических алгоритмов (см. п. 6.3.9);
- корректности управления секретными данными (см. п. 6.3.10);
- отсутствия недокументированных возможностей (см. п. 6.3.11).

6 Методы испытаний

6.1 Анализ документации

6.1.1 Документ «Спецификация»

При анализе документа «Спецификация» эксперт проверяет, что в нем указаны компоненты и документация, представляемые на испытания.

Если документ «Спецификация» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.202.

6.1.2 Документ «Текст программы»

При анализе документа «Текст программы» эксперт проверяет, что исходные тексты программы, реализующие определенные в СТБ 1176.2 криптографические алгоритмы, представлены полностью и в виде, который использовался при сборке программы.

Если документ «Текст программы» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.401.

6.1.3 Документ «Описание программы»

При анализе документа «Описание программы» эксперт проверяет выполнение следующих требований:

– в документе должна быть указана информация, однозначно идентифицирующая вызываемые стандартные функции (версия компилятора, используемые стандартные библиотеки и т.п.);

– документ должен определять программные модули, реализующие определенные в СТБ 1176.2 криптографические алгоритмы;

– описание программы в терминах программных модулей должно соответствовать исходным текстам программы.

Если документ «Описание программы» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.402.

6.1.4 Документ «Руководство программиста»

При анализе документа «Руководство программиста» эксперт проверяет выполнение следующих требований:

– документ должен содержать описание всех доступных для вызова функций, реализующих определенные в СТБ 1176.2 криптографические алгоритмы;

– описание функций, реализующих определенные в СТБ 1176.2 криптографические алгоритмы, и условия их использования должны соответствовать исходным текстам программы.

При описании в документации функций должны выполняться следующие условия:

– каждая функция должна иметь описание назначения;

– каждый параметр функции должен иметь описание назначения, типа и, при необходимости, диапазона допустимых значений;

– каждая функция должна иметь описание возвращаемого результата с указанием типа;

– каждая функция должна иметь описание условий, при выполнении которых в ходе работы функции могут возникать ошибочные ситуации, требующие специальной обработки;

– в случае если при реализации криптографического алгоритма используется более одной доступной для вызова функции, должны быть указаны порядок и условия вызова данных функций.

Если документ «Руководство программиста» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.504.

6.2 Тестирование

6.2.1 Алгоритмы выработки и проверки электронной цифровой подписи

Для алгоритмов выработки и проверки электронной цифровой подписи (ЭЦП) выполняются тесты SIGN.L01.1 – SIGN.L01.4, SIGN.L02.1 – SIGN.L02.4, ..., SIGN.L10.1 – SIGN.L10.4.

Входными данными тестов являются параметры l, r, p, q, a, личный ключ x, открытый ключ y, одноразовый личный ключ k.

В тестах для хранения результата выработки подписи используются слова $S, S' \in \{0,1\}^{2r}$.

В тестах используется функция хэширования со стартовым значением H, состоящим из 32 октетов $\mathtt{00}_{16}$. Для l, r, p, q, a, x и y используются фиксированные значения, выбор которых зависит от уровня стойкости. Значение k, в зависимости от теста, задается фиксированным или генерируется псевдослучайным методом, при генерации соблюдается условие: $1 < k < q$.

1-й уровень стойкости. В тестах SIGN.L01.1 – SIGN.L01.4 используются параметры и ключи из таблицы 1.

Таблица 1 — Параметры и ключи (1-й уровень стойкости)

l	638
r	143
p	2E612BDF 2FBFCEAE 6B24F873 8BDD18CE 26852CAB D958AC7C 5D086558 B8D554D6 43AF75BD 74C9E622 1F25F41D 3AA2ADB9 6AC35AEA 77F9B09C B52C58F7 9D869267 BE13AFF4 6E46ACC5 ED930532 B7B27ED7$_{\overleftarrow{16}}$
q	71C5 C8FF8AE6 4E9D0415 37034E3F 5B1933A9$_{\overleftarrow{16}}$
a	023BDC86 201567E9 F79653F7 0C64B42C 3AF40D4B B65F83E4 C6A322F2 B880EDEC B6530743 5C1D7297 237318BE 4EAFDEFA 3DDABACC DAC58EA1 F90C0754 CF54DD0F 03F8D6A5 DD05491B ECA3716B 245CAFBC$_{\overleftarrow{16}}$
x	0E3A 37007519 B162FBEA C8FCB1C0 A4E6CC57$_{\overleftarrow{16}}$
y	0418F964 0E1BC6FD 5CE83276 9EC5FA5F E32292AF 88EB5AFD 35BE307D 5248A386 7129787A 86D5D64C CAFB07F2 45FB1356 3FC8CD2A DC146BBA 4C6D2D91 B65816C2 1B59050A 88AB5F7D 2D6DA902 65067456$_{\overleftarrow{16}}$

Тест SIGN.L01.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 1.

2 Задать сообщение длины 32 октета:

$$M \leftarrow \texttt{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{511E 517C8DB8 DF222BB9 45DD9D8B 292C8A0A}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

5 Если

$$S = \texttt{097D93B0 50CD7D36 16B9AF46 8085AE72 57A41190 DFC802EE B0BB152E A9E74CA0 FAD4C341}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L01.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 1.

2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{511E 517C8DB8 DF222BB9 45DD9D8B 292C8A0A}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

5 Если

$$S = \texttt{0AA4EEB8 97CB0367 98B2FF1A A8AA208B 93CDB195 98AF2995}$$
$$\texttt{35D8A54A 4B2728E0 E912815A}_{\overleftarrow{16}},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест SIGN.L01.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 1.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить ОШИБКА.
3 Возвратить УСПЕХ.

Тест SIGN.L01.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 1.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить ОШИБКА.
3 Возвратить УСПЕХ.

2-й уровень стойкости. В тестах SIGN.L02.1 – SIGN.L02.4 используются параметры и ключи из таблицы 2.

Тест SIGN.L02.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 2.
2 Задать сообщение длины 32 октета:

$$M \leftarrow \texttt{29312074 73657428 20656761 7373656D 20657479 62206F77}$$
$$\texttt{74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{295A7A 95E31924 2CC39A68 46C63C0B D4B53847}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{07192A AC7EF968 3FE7F458 ACCE70BD C5097F13 691BBFAD B136B523}$$
$$\texttt{925BCE5C 79AD9E59 8531F791}_{\overleftarrow{16}},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Таблица 2 — Параметры и ключи (2-й уровень стойкости)

l	766
r	154
p	234580A2 9115011C 77FEE8F3 F3FCFA27 E2558889 37FDC5B9 F570CCE3 546D8D29 77C12517 CEEF4360 830D2476 A315AAFC BF9368A6 2434FDE0 C3DB8965 6B3AD98C 47EC1697 820C4382 CD4C63A6 E1790E76 6CACEA5B D7A4D0AE D473C19A 42F3157F$_{\overleftarrow{16}}$
q	023984C7 48285225 8766ECD9 3FF0EB71 6D746823$_{\overleftarrow{16}}$
a	09535F81 1DD2D58B EEBD6918 8035FF97 FE20EA5B CE10F6AC 5947A601 7DBA57ED B8115313 5D39320D 6ABE6B19 39157EDD 9E2CEF81 7616D8C4 C584FE34 19912E3B 74117169 A37D9FF1 C45CCF81 A6DC0F90 67E49EB7 82F764E4 910F7F07 AE5F681E$_{\overleftarrow{16}}$
x	01C67B38 B7D7ADDA 78991326 C00F148E 928B97DD$_{\overleftarrow{16}}$
y	00D76E36 DB687CC1 B9BBE854 DEB98875 30C0DDA8 B4A36E95 A8351CA2 420F2392 0C27C3E9 089ECADB 0BCF5217 6624A8FA 65DA7D5C D6B44BBF F928B0C2 A212C2DD F1AB7766 77532EAE AC479E4F 68B180D4 D36A12F0 BD6AB6AA 3CC38AAC ADD89FEC$_{\overleftarrow{16}}$

Тест SIGN.L02.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 2.

2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{295A7A 95E31924 2CC39A68 46C63C0B D4B53847}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

5 Если

$$S = \texttt{061FE2 DEF1C801 6F7E1E35 B5B0B33A 8303907F 78E651B8 9899ABA7 FE488384 AD556276 593C990B}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L02.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 2.

2 Для $i = 1, 2, \ldots, 10000$ выполнить:

1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;

5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить ОШИБКА.
3 Возвратить УСПЕХ.

Тест SIGN.L02.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 2.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить ОШИБКА.
3 Возвратить УСПЕХ.

3-й уровень стойкости. В тестах SIGN.L03.1 – SIGN.L03.4 используются параметры и ключи из таблицы 3.

Таблица 3 — Параметры и ключи (3-й уровень стойкости)

l	1022
r	175
p	2846B979 F51D4156 B881C96F 3C61A5F3 B5A8F4B4 7B604657 8B92205C A7ADCB9A 77CF7780 023B7217 1BB3BED1 569ECA57 2C5E423B 885C70F5 D2CD3C17 0E31CE50 7DE12C9E 535D71DA 16530C9B E6D078C4 67CE4D24 E7C63181 7FB4BE8F 16EB1B4D E7152DB1 8B23E9B8 99CDAAAB CF7BEC42 CBA90DE4 747EA228 BC267048 0EB191E5$_{\overleftarrow{16}}$
q	7A3D 48C80B17 84985341 4EE450CC 636C93F5 1D63F3C5$_{\overleftarrow{16}}$
a	0CA7F481 B9D2ABE2 E1CBC58F AB8B1FC9 D05234B0 B72AA69B 9A522E1C 18EB73FC CF86CBED 32BD11D0 41AE0434 0D9F732E 7D6A88D0 52BC2CEE 1F8F64CB 0893D92F 365D162E 67B04EEA D6F8FE7F 51B74CF6 1C90C9F4 53F35E56 8E2225F4 5C62BDF0 1E96E131 67CE3338 33B93F65 96332013 2112AADB E4D93404 7AFFBB35 7D931983$_{\overleftarrow{16}}$
x	05C2 B737F4E8 7B67ACBE B11BAF33 9C936C0A E29C0C3B$_{\overleftarrow{16}}$
y	03E66732 5E03412A 6C776C69 31D13CC4 1DF777BA 120E5777 617200DA DEEF6FD9 9A2145BC A6B12824 A15863C9 45145E50 38E50B8A 1E10DB42 290E87D1 94473E14 44E0A945 50147427 5E456D69 D2749C07 8882FD6E 670C0F75 F85732AF 04EF04EF BA91CCE3 A6A0A23F A871412F F91797A7 D59C9C5A 3ACCF56D 7D27756A B577D9AF$_{\overleftarrow{16}}$

Тест SIGN.L03.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 3.
2 Задать сообщение длины 32 октета:

$$M \leftarrow \text{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{67F4 0FC55F70 7EA4DAA8 1A49F648 3CA44BD3 0D1D0F60}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{01B7F04E 0F8B1C15 17344275 29AC1B90 344A7D64 76B30501 B3D2D774 2F61FF59 727DCB01 05C24314 D2ABEDA7}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L03.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 3.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{67F4 0FC55F70 7EA4DAA8 1A49F648 3CA44BD3 0D1D0F60}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{04A18503 EF5CF70C 4D07059A 6D0D9CD1 E00D1AA4 93C0148E 28A277C0 64234C69 49FA4120 AC01F994 1E0939CF}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L03.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 3.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Тест SIGN.L03.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 3.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;

3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.

3 Возвратить `УСПЕХ`.

4-й уровень стойкости. В тестах SIGN.L04.1 – SIGN.L04.4 используются параметры и ключи из таблицы 4.

Таблица 4 — Параметры и ключи (4-й уровень стойкости)

l	1118
r	182
p	3B39C1FA B3D002F4 7928162F 13DFBAE2 1E4B1646 322B9C1A 2846B979 F51D4156 B881C96F 3C61A5F3 B5A8F4B4 7B605629 64C819C3 D1515967 D891BD1F 2B71EB0E 9EB7B7A5 CAFA2A66 38228A44 AB6FD520 AA4484C2 2A7115F2 2034FA2D BF33C4BA 486E9DA7 6F1EBBF9 5B06C9BF 3F617877 2601B34D 01E8057B F187BB1E E2FB1484 97BF4F8E 1E914C73 80033203$_{\overleftarrow{16}}$
q	338BDD 18CE2685 2CABD8F8 5709B00D A683960E 80FA7EB1$_{\overleftarrow{16}}$
a	1AE885C1 7B949DF9 6B3C83DC 780CA9CB A9BE3503 41A6DDBA F7D23456 51952837 AA6A16A3 83A9C2D3 141E4F31 C9479212 23C09504 DF220918 64B04D90 433FA217 2A364144 61ED45C8 B8BC9F48 4ED4A231 C68D7A91 D579D42F 92CD9F86 CFFEB179 E3CAE6D7 6E7EA61E 4156BD2D E3A6F3D4 E3CB9FD0 74D78ACF 5DFD75CE 9A1A9A40 D44420C9 497565EA F5900604$_{\overleftarrow{16}}$
x	0C7422 E731D97A D3542707 A8F64FF2 597C69F1 7F05814F$_{\overleftarrow{16}}$
y	216AC4E2 7F349643 BD2FBC22 01E44506 24B5F7A8 E01DE7B9 D6647E13 F33F69DC 86C1038B A5807B95 FE01C57B 0C95F9CE 49A852EF 00F2B60A ABF5CBB4 0C8B361E 10ACCA1C 29E3C444 D54895E8 F6883DAD F399943B 047803A9 A7AD5AE0 9B453223 A6FD9649 6DA7597A 2462E61D 7DAA5AA6 9B84D8EA 6C5B386A A01174AE 82EAFD42 A385B456 2D87C7FF 84575402$_{\overleftarrow{16}}$

Тест SIGN.L04.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 4.
2 Задать сообщение длины 32 октета:

$$M \leftarrow \text{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \text{149949 D87EC0CF 36CDC707 DEE6EC3A 48B1FDFD A454FF39}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \text{023C 75001F8C 39D973F5 3A48C14F ABD1DB09 0912531A 191D028C 4C80A8C7 06C4116F 2AED4AA1 B8F4671D F4F9F27C}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L04.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 4.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{149949 D87EC0CF 36CDC707 DEE6EC3A 48B1FDFD A454FF39}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{0369 17A0FBE6 BAE8E679 06E73F98 41FD648B C48FDB77 66CBBCDC 3824123E 157CB7D6 868A5469 18A5F5EC EE701C40}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L04.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 4.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Тест SIGN.L04.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 4.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

5-й уровень стойкости. В тестах SIGN.L05.1 – SIGN.L05.4 используются параметры и ключи из таблицы 5.

Таблица 5 — Параметры и ключи (5-й уровень стойкости)

l	1310
r	195
p	2F07C4C3 CED5466C 41A5829D 099FA444 91B0ACCF 99031E4B 6B6E4893 5A6D486D 5006A038 46542CC9 E02CFE85 4BD8CCD8 084713A8 A0BB39C2 20FE0036 AD1C3285 F2A38ACE BB246592 E5C7B6C3 0C36C23B 825ED3A5 DBA6F8A3 7F0C1D78 37BFE6AC 5E0758B2 B810A8FC 50A8B482 698D2639 76818557 5FAB6F08 CF69BB65 9F7A843B E3A52728 4D7765B1 7CB94687 3CDA33F1 DE89C470 D0880E66 4B5659B0 60B31B75 8507F4A1$_{\overleftarrow{16}}$
q	05 888937FD C5B9F570 CCE164AF 8365AEBD 14FF46C2 3B71D4D9$_{\overleftarrow{16}}$
a	22888630 44C540C3 9570F227 00454C1C A44B7DA0 17810175 661DBA0C F65C3222 66504CFA 3B7EF30A 2528BE22 FAA434EC 8A3296E4 4F51F6D3 F5DA0425 671AA13D C23BCEE4 7F95CFB6 550A48E2 47C8BBCB F8B0ECCB C2BA3669 7D32331E 3B648633 3B470B95 33313FE6 158F1543 1011A8CF 88DC3C20 661DC08C AA575F7B 402B88CC 55A37BFE 754F54CD 482BACBB 793E925C 991079F6 150594D9 6C5C4608 53E8E168 3D2A2227$_{\overleftarrow{16}}$
x	02 7776C802 3A460A8F 331E9B50 7C9A5142 EB00B93D C48E2B27$_{\overleftarrow{16}}$
y	216518D5 DF79DFDD 422B1D84 0F068BB2 E1D2A75D 41F2D754 CBE15C86 BC6B64E1 D924D3FE E89D1F7E 2D925A2B 9CA3B5DE 1341C856 6A926D54 B48FC458 0CC4EEBB A362162B E899C4EE AF61EFF7 4161E6FB CD58DA67 72F7BA06 729F3455 44D2496F 63047F82 7837C2D7 B2A3A4A1 4F1845F8 607F5B97 416D95E0 0CE438D3 D2F5750B 8C907E18 CA743ED2 CC160BDA 7E7FD022 0F8C9227 C368A058 790CF8B7 3F77ECD4 9B0FB460$_{\overleftarrow{16}}$

Тест SIGN.L05.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 5.

2 Задать сообщение длины 32 октета:

$$M \leftarrow \texttt{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{04 E8A07947 913BB4CF 8E73BE19 5388F1FE D9CB6A2F 7F3567E7}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

5 Если

$$S = \texttt{16 34AD8CEE 0115CBF5 78B92569 03DCF4A5 B90F9683 2226F11B E2C6BAA3 B4429F3A 6F22684D 5A9CCF89 35744400 B9526A12}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L05.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 5.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{04 E8A07947 913BB4CF 8E73BE19 5388F1FE D9CB6A2F 7F3567E7}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{19 7E392A09 9709B959 FEC89E1F A182C836 84E81049 7A66EFCA 2E280E60 E6745E02 63BC41D6 5745D9DD A5544811 E7D6331C}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L05.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 5.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Тест SIGN.L05.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 5.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

6-й уровень стойкости. В тестах SIGN.L06.1 – SIGN.L06.4 используются параметры и ключи из таблицы 6.

Таблица 6 — Параметры и ключи (6-й уровень стойкости)

l	1534
r	208
p	2E4BC383 5A5B41E3 5D9DC735 157891FC 868064AD 80086810 CB68F580 3DD79608 20A2BAAF 7588969A B9BF5187 3B1E393D 6DABA057 C219EDC6 8183B7EF 07C4C3CE D5466C41 A598A28B D0812BB7 F8AB721D CA6D6D09 AFB97604 4CE6D36C 5F4C1C58 6179EB2F B8F77415 70E8B492 44FD8E02 4398EBED 9B3DD66C 591FD864 83B9FA62 D66F3AFF 7F98ED22 61B15F45 5DEAB8D4 DDC3855D 6EBA0C8A 706F48AC A209ACE2 87AF3A81 CD0AF711 F82A1C65 3C5E5AAA 6BC05AA9 2591AC22 5BEBC6E5 5E953453$_{\overleftarrow{16}}$
q	B7B5 417D8085 27DED8EA EC7CFCB9 742C871B DF45DA71 5F6A453D$_{\overleftarrow{16}}$
a	017CA54B C1BD338D 2F760ACF 08D1124A 57FF866C 24F3DC85 19E03C44 210F4E08 D9950280 C0CC9FBD BA3916D4 18CF1999 B91E413C 402BC00D B8B6BA76 8C45257F 25E9F4D7 1CC78ED3 EF1201D0 12E6B9CE 24913F2F 57E38606 C84D8E18 1A420D54 F1B1E2A1 987BED42 2079E48E 88A03E73 0C36055B 9C9A15D4 2BA8DCCB F810E193 A7653A9C 175A8185 FD73BB1C 17139B31 160B42CA EDF01F01 F799A0B6 1AF8FF8B DE3E2AC1 7145A727 FD7AE027 1BF97092 BF730F08 16C8F376 450A350E B7C78044$_{\overleftarrow{16}}$
x	484A BE827F7A D8212715 13830346 8BD378E4 20BA258E A095BAC3$_{\overleftarrow{16}}$
y	237EA9BC 0703E75B 2EDE1E4D 2E1E46C2 707A64AB 7E45934C 2FEAA889 C7686747 2E00515C 0BB0BF01 8CB6CCC8 221C1274 2F11D3A1 45DA1BD3 73A8E854 A296589C 6ABED310 F6087465 E91DA17B C20BD74C C5556839 9263B510 F9EA9E6D 59557919 CEFD46AB 04343A0C 1AA86EC2 CD03D700 B2FCD6B9 E93BC426 FE9A3683 AAEA6F27 9F47A8AB 10FDFA40 803994CC 9C29FBF4 D9BA3733 EF1AD3F8 5A639BA9 A6E605B1 1764E2DD 68436FDE 23E44139 3B73B834 5B3E2D88 032D1AB4 79906DB0 890D650A$_{\overleftarrow{16}}$

Тест SIGN.L06.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 6.

2 Задать сообщение длины 32 октета:

$$M \leftarrow \text{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \text{501C 1F9EF23F AAD329B1 98478587 4F3D7DEF 05A8119C C6420DF7}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

5 Если

$$S = \text{08D7869E 72DF587B 360F30D4 207D3B10 38179BEB EA4F6D25 48E684D4 C078A766 95D5E25B ED8AEC41 0966358B F244EA89 42D84C26}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L06.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 6.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{501C 1F9EF23F AAD329B1 98478587 4F3D7DEF 05A8119C C6420DF7}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{57764834 253F4779 119A78D0 0587B66E DF1D662F C8F01E1E 7F182225 A4D24432 D6D66609 AC4BD6E4 03044E5C 16CA2F1B A5FF797F}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L06.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 6.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Тест SIGN.L06.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 6.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

7-й уровень стойкости. В тестах SIGN.L07.1 – SIGN.L07.4 используются параметры и ключи из таблицы 7.

Таблица 7 — Параметры и ключи (7-й уровень стойкости)

l	1790
r	222
p	3D57719D 77271E57 C3689909 FD6FC8E9 C889CA56 4922CD95 68537A69 96769040 760E1F5C A505C7B3 5201F256 6A046C9A EB303588 3DC46523 3A2827F7 1B204025 24E2CE4B C3835A5B 41E35D9D C7351578 91FC8707 EB79001A 0A1C5726 6A8BF7E1 0DBCD2B4 E869BC6A D9EF7154 92B73B43 3A3D38E2 3CC115D3 E1A47A5E 7BAE15B5 3062130B B9874AA4 A5C06324 41B5E17A 8B14A054 1219DC80 9494B51A D59B23A9 BC961885 FE5C4E3F 9933C22E 8045BF1D AC4031D2 F92C53FF D35C0B64 246D9CAF 6816E802 F6D3F1A3 C8441374 E9D5A7F3 40F646FF 60F06E72 9B114360 6A204B47$_{\overleftarrow{16}}$
q	26578B92 205CA7AD CB9A77CF 779CC50F EF060012 BCEA0844 D9492A65$_{\overleftarrow{16}}$
a	21018F69 1A8B6B5E 6C494CBE FC010A25 2573A4DD C36CAC7A AFB066B9 51CD7D6B F0FA3895 75A29493 9F431CB5 4E7D8832 3B938085 2D3D5114 16AF23E0 BF5B2176 CAACE54F 3D990308 357735A1 EC6A8F39 2E19406D 2F83B674 41AEA1BB 1EB26B14 AC8D52BE 43281FD6 B86B1502 8A286302 BDC230B1 920F5048 77C5CD89 3BE59BAB A1BDBF78 3BF232DF 42A93626 7AAEC8CB DE0766A4 871D3D6F D8134ADC A2AD7EF1 298E7BA5 86039040 B8BB599F A5033776 B3FD1750 116AFAD2 CD3AE983 8E6776B8 E99B84CF 0912B001 35E0D218 A91642B8 3EA0A2E1 C089E821 3124E60A 593E9481$_{\overleftarrow{16}}$
x	19A8746D DFA35852 34658830 88633AF0 10F9FFED 4315F7BB 26B6D59B$_{\overleftarrow{16}}$
y	2461589A 7CF82D57 BAB2DCF9 482A4536 4088988F DE1D302A A989B582 10781780 39E77623 9C65B78D 609C9711 5258E347 92DAF95A 48E63690 9A430A5A 57C1B682 27B4D6D8 68D1991D 0180B0FC 76CCD167 F5F9D59F 637F1F60 1F926C5A BEC7CEE5 EC08A767 262F5E7E 4CB027D8 10CA98C0 2F1D9AED 53AF934D 4AE5C169 611CF062 986A9256 C6CC69A7 78BCB490 1254E5EB DB85B004 A6D89300 7F26DA62 916DD91A 8E946C62 6D4F671A 4F86AD52 8217B8DA E4A4DA73 10A34568 A0BC1C5B CFE34182 9C61C9F7 C716AB27 1FC90131 1344694E 0894615E 4B1584E6 660ECDF4 69A12ECA$_{\overleftarrow{16}}$

Тест SIGN.L07.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 7.

2 Задать сообщение длины 32 октета:

$$M \leftarrow \texttt{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{19F2BA93 3DD411ED 3A613123 325361A0 65DBFF8F 9283CE62 E84901A2}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

5 Если

$$S = \texttt{073B4A63 AFDF4183 8432DE21 7C3175DF 6DE864CF 862621C5 1B7B0F40 0F55623A 46982BF6 2E722354 10D594D2 422827D5 05D6DDF3 EAA21910}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L07.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 7.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{19F2BA93 3DD411ED 3A613123 325361A0 65DBFF8F 9283CE62 E84901A2}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{0498C52C D075160D 92F8E068 7AAB4612 82FABC44 16C9F96B C7D635EC 437E1E23 8A5E1A00 A0F5D900 C28C009D B8C785BE 631C6F62 4007077B}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L07.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 7.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Тест SIGN.L07.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 7.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

8-й уровень стойкости. В тестах SIGN.L08.1 – SIGN.L08.4 используются параметры и ключи из таблицы 8.

Таблица 8 — Параметры и ключи (8-й уровень стойкости)

l	2046
r	235
p	26D11020 24A7D2CF 7F5560D0 596A51E9 A84884D4 2A5502CE 324DEB04 38FA5314 026657EC 850E0553 582267C3 B74E19FC 8FAB80FD 2CF9E6D8 2B98982F 76AB1BA5 8D572EB1 6917DD57 719D7727 1E57C368 9909FD6F C8E9C889 CA564922 CD956853 7A6E00C9 5EA18264 5BD5DDC9 B10ADC28 606BAC6D 3C5EBD9D D4D59B99 FAB8F4C7 3F2EF833 22734F1B B0CC2AC7 827973E6 D8DB9B82 135ACE17 2FA30DF0 119DF359 54650F1B 451FF12B DF325558 8D981ADA 7CC14F7C C6C9BC5F 578245CB F93793BC C59E718C 4E989E87 F3D34D22 1104DCB7 4AE12544 739C3F49 DD150DD5 3582AFEA 689F91EF 5B8C0FD4 C81A374F B3CE33CA A4BB503D 704EB0D2 6B121A4C 49EE4925$_{\overleftarrow{16}}$
q	0528 162F13DF BAE21E4B 1646322B E7459E57 6BA96381 CFA2A3EE 6CC63E1B$_{\overleftarrow{16}}$
a	21F60E1A 8B43D483 753CBBC8 74F4EF72 014998DE 68EFFB7D 195C7320 937FDC04 65B8E5BC 90AE73A2 D73C36A0 9CDC446F FC37CAF4 6E47F94F 2AEB31E2 3DB2A48E 167482DB 5698928C 97982DE4 DD435B56 2D39E467 FD9E51FC BB431C97 D674484C A1DA0729 56C3EEDD 98486870 FF6E315C A8D1995B 94771827 E7E73133 13CE8DA3 881DD127 07FB53AC D964D34E BCA26EB6 86BD25C2 4882B5A1 4709F924 9A75DE2E FF4A9024 40CCF4F6 559ED678 6FA7B329 F7F14690 AFE97D40 0C826940 0FD693BD 25E4F74B 6E25AFF2 93DA4D30 8E2743EC 626F74AD 36F31749 9C56C654 E034E880 C3E58DC4 FF49E766 69C105C5 F44C713E 60D80718 DE02ABDF FDEDED86 E73C9572$_{\overleftarrow{16}}$
x	02D7 E9D0EC20 451DE1B4 E9B9CDD4 18BA61A8 94569C7E 305D5C11 9339C1E5$_{\overleftarrow{16}}$
y	10D1981F 55E783D1 EE51F424 F5327DF6 C6AF4A23 1E865A41 70F80B8B 0D7237A3 36682A46 CABDBA15 C64E8C51 BBB3D28B FF96880C 17D48C60 BA9C9835 29670261 5722F4C3 C04A11F0 51F2B215 84150747 4B1FC2D8 3244533C 05AF5450 D98377E9 897B4509 860E5365 58376335 A0A82D27 EECB17F3 0F5801E5 72E75031 9869D33E 061E8BD3 ECBC9136 97D9D3DB 9E8E92B5 5E25BE5C 032EE149 5D064D84 B6273D88 7F648417 1BFEB4E6 F7D74239 08F2C9B4 9127733B 876A4C1D FE2E4084 8C2ED0E3 DE7980A3 E026E991 583B3EAD CBC03691 13ACCC69 E7C4BBAD 758D6735 A1357618 0FD7C779 2F0F2DB1 BD87E8B3 5E580A71 8D322000 25B4EB17 C7383432 65196BE4$_{\overleftarrow{16}}$

Тест SIGN.L08.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 8.

2 Задать сообщение длины 32 октета:

$$M \leftarrow \text{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{02A4 F41788F0 9C5B0402 3CEB9DE5 2AF936D1 DA3E1939 4C1DB109 37F4AE41}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{06E65C 3AC07688 A6D46F05 EA4F46FA 869D5DF9 311C3127 0450CE50 11A0C26E 3B19FB21 2F5B361B 7FCC23A9 3878D96D B07DB5D1 D9D36D2B FC40619E}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L08.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 8.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{02A4 F41788F0 9C5B0402 3CEB9DE5 2AF936D1 DA3E1939 4C1DB109 37F4AE41}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{0BD32A E4481B3A 5ADCAF0E BC72F74F D998AC25 0A445056 0509B842 45EBD17B E2EC8AD2 22D726BF 1AA97BF4 C2ABEFFA E376E170 78FBA80E 23F8A738}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L08.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 8.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Тест SIGN.L08.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 8.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

9-й уровень стойкости. В тестах SIGN.L09.1 – SIGN.L09.4 используются параметры и ключи из таблицы 9.

Тест SIGN.L09.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 9.
2 Задать сообщение длины 32 октета:

$$M \leftarrow \texttt{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{0151898B 2003A3FE 5B6498DF 1978D8B9 347465B2 BC5FBDAB 93E39836 8F3EEB5A}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{01B6A1 957F354D 637D966E 5A6A5AC6 B0E66947 0BA39E2B F47022A9 8F635C0A 2C34A5BB 015BE464 3331983C 4471554B 35BEF657 9E38C038 F7DFA314 CA8B2C2C}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L09.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 9.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{0151898B 2003A3FE 5B6498DF 1978D8B9 347465B2 BC5FBDAB 93E39836 8F3EEB5A}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

5 Если

$$S = \begin{array}{l}\texttt{01BBE9 A43D17B9 8C74686D 0BF4C9AE B93E7E08 E6DB29AE}\\ \texttt{33764B58 B0B8871B AA9E8001 E715C269 E491AB2D 1B34F97E}\\ \texttt{728F1D27 D1DB1DF3 CEA3CACB DCE724C2}_{\overleftarrow{16}},\end{array}$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L09.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 9.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Тест SIGN.L09.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 9.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
3 Возвратить `УСПЕХ`.

Таблица 9 — Параметры и ключи (9-й уровень стойкости)

l	2334
r	249
p	218E2DF4 EFD3E1D1 05E034A4 97CFC0FA 4C0239E7 55C13965 D096452B 055A5314 C80FC7F6 3C81014E EE3FA9C6 FDFE9A88 A2E8D113 7ABE01E6 DD806D0A 64A405B3 F30D909C 84B6008F 9D06D110 2024A7D2 CF7F5560 D0596A51 E9A84884 D42A5502 CE324DEB 0438FA53 14026657 EC850E05 536B929D 64B3517B 6A32D5F5 DB43E45C 89975FD6 367DB378 309BDAE3 6E3353C9 DFC821C6 DA572AC9 BEAC4BE1 5AA9CB5D 989D71CD 32B62C67 499D02F2 F21A88D0 62DC0524 7CE355BA 72B5EE43 4A72624A 24950490 67AB2A40 8B712772 E0A7A24C 6818DEFD 8C50D3E9 8F8BFF31 C8E7A6BD B948BB21 45045B21 AB05E992 679DE674 ABFF2BFE FB2FA3AA DD965505 97CC155D D1294C54 22BD197B 6D92B0F5 4BD34DDB A8079951 CB3EA032 34D5925F 533F00F3 56EEB2BD$_{\overleftarrow{16}}$
q	016E4893 5A6D486D 5006A038 46542CCE 0F86897E FEF11481 E9989BE8 AEA7EA8B$_{\overleftarrow{16}}$
a	1E19E2B7 133A089B 0B770791 0D5A0D3B 3C7C5710 A20F72F6 CABD7C6D 69B886FE B0DF34D1 C1F7CF3E 39D3E8E2 7A1A69A2 8724D38A 6C71E39E E44C2958 40B7ADC6 29B4C7A7 D3C4DB41 F9F990A3 0974DBFB 00B397A6 040AAC1E A8067C53 11AEF62D 3437F1EA 8A36B2C9 CDA93E95 5B1F7E6C A230D6A8 0E622982 2A548AF6 A63BC15C CE95CA45 E95BB9E1 45B8AD01 93E11BCF B60547AD 686236D3 9C431BA6 54FDE781 B24C847C 767B81B5 132D85E0 4E6575D3 0E9F603A 7DC2E3D9 8A17C261 B2053129 703CACFF 1C582BF0 992C3EFA 64A67827 64EDD6D9 9F4F11A5 ED0E7420 7D1B9674 DC7CDE96 AFB143C6 4F276E03 5FFB79FE C664E63C A5901E29 DD516F98 CA094AF6 0EBEE299 1675E0DA DD4A59B2 B9812875 5B0AD3C1 8321F6A6 1FB06981 FB0ED824 B50D9C79$_{\overleftarrow{16}}$
x	0091B76C A592B792 AFF95FC7 B9ABD331 F0797681 010EEB7E 16676417 51581575$_{\overleftarrow{16}}$
y	03C776D7 D9A07498 1D60BCDF 22BBFD78 C2CF27A7 46307092 0FD7CEFE F6118620 E61602F7 85392462 8451D326 ADC834CE 39785E85 91C5D7A9 1F729F0A 4A475670 B595A3D6 5A7BD4CB E85F326F 5D69B42D 02085FA6 8A5D0EAC 9B185132 E75EC6CF 74631D6A 6BC28002 EABF693A A8F26A8E F426CD98 1490C9A2 03F4BCFA 51D430E8 C7CE90BA 94559E12 7A074961 0304D6F2 56DF1785 F30EDBF0 2B6CFD1D 4AB7A78F 137E3216 96FE356A 41E4C779 2C48FC01 89907FC5 FC8D0270 75F89FCF 927678A7 3C71A2FF B60C6C29 2DD884B2 2526C3A4 27F5EC74 01617363 83F99F31 68E76F95 2B5A04F0 7475A0A0 1F4ECD2B D423EA3F 7D6878AC 67653DC1 02B222D1 F80B54B8 BABA41C5 BD02D274 ADA8143A 8F6AEF79 A1197F7F 0089476B 5018B606 F32EDF79 A8718958$_{\overleftarrow{16}}$

10-й уровень стойкости. В тестах SIGN.L10.1 – SIGN.L10.4 используются параметры и ключи из таблицы 10.

Таблица 10 — Параметры и ключи (10-й уровень стойкости)

l	2462
r	257
p	2F01EACA 0363BB43 DA7CF0A2 14D2FC03 3A592B2F 2E3FB58D 61D7E42B AA17455B 38167684 BF8F418E 2DF4EFD3 E1D105E0 34A497CF C0FA4C02 39E755C1 3965D096 452B055A 5314C80F C7F63C81 014EEE3F A9C6FDFE 9A88A2E8 D1137ABE 01E6DD80 6D0A64A4 05B3F30D 909C84B6 008F9D06 D1102024 A7D2CF7F 5C041887 3BD222EF 2BE1BFAF 66CB3BBD 7E34AEDF 10C5A70E 1CAC0566 DBC96E05 8B5D0B9D 6875951B 0ADF8D09 BCE5CE60 FC1CBEC0 C49DE8A4 94568263 9E9CF549 93A62251 372DD0EE B3007644 5EFD9B15 5194FA32 54CF3DA6 D0EE8B0C 0F515DF1 949E8F8B 67E7DC1A 14433033 9BA0AEA1 E93C551A 3117CE98 AFD69473 2667E4CE 226779E3 4726E78E 13E916D8 916D2918 BDF5DD77 8C9938E2 F52E3425 714CA7C9 122330D9 2A2DF086 1516CCE3 51E6D76D 7537432A F1F2285F 6F9B1D95$_{\overleftarrow{16}}$
q	01 C3CED546 6C41A582 9D099FA4 4491B119 3D1AB138 A1781046 73D152C1 4F804EEB$_{\overleftarrow{16}}$
a	1E921804 B4E9624E 38CE41C7 79846D4D BB98D53D F634ED69 85FA42BF 079A7BD0 5AAC508F BFC47892 8F9EE2B2 2C2F1B97 D98F6147 7EDC2AAB 4AA32499 552FF72F F1B3AEF2 7F5231DA 1880A153 F1B283E2 2A386554 3B642C35 EFE211C5 046AAE39 6C2811B8 1DBED9C4 AFB1F39E D2F36799 1CC77980 51B99F0B 7FEE1AB4 E85CDBBD 853BCB1B A1902175 9E588CC7 0AF9888A 5C4EC7FF F330749C EA1890BC F722BAE9 37D2B366 3805DC67 F55A591B 6E288962 9D11CD03 C1555AC8 63827B88 A0451A47 26597359 E5902CAD 1EEAF794 EB600530 9988F333 95F42041 4BB0B218 75305E12 CCF177BE 765DF18E DDB7E9AA 37631867 94D3C446 38E1B11A B87C6957 F5C14787 D540959D 3ACB53D3 1BBB2482 3F5AC505 FAF5D86E 0EBA65AE CB14B4B0 0601CC24 26CC476D 8837CC6C 4FCE7B07 0E19ABEB 6DC34FEE$_{\overleftarrow{16}}$
x	3C312AB9 93BE5A7D 62F6605B BB6E4EE6 C2E54EC7 5E87EFB9 8C2EAD3E B07FB115$_{\overleftarrow{16}}$
y	18F2DD0B 45B40B39 AE0785EC 813DF4DE 78486D0F 0470FDB4 C7AD668C E8FD65C4 547BDD7E ED951408 3FF1F760 09197529 B3541755 B8CA008 E7766BF2 CDF4C9C2 DA78A6DE 16E5DA64 4780B264 B2EB4492 ED27D76E D1DDC5C7 350A0154 FA54A83D 69F6C6F6 1874FA78 8DBC6695 3B078296 0F31432D 0F4E2986 EA16E424 878F71EA A1BFE08B 622B2E6C BE72A0CB 64E76E9E C5819C17 6D6B6251 C8277846 783336B3 6E5F24DB BA2AF2DB A221D97A 542FE1D7 C5B0B092 42823DE7 04943D28 1209EB02 30538B98 E4C05155 1C0F746D 325C554E E7F39182 52A5EC55 0E0785FF 912010C9 B08074ED 6143532D D37AC419 7E0B0588 F89D248E 427F6DC2 85248E87 4A2BEBEC E99BCEE7 17FBD086 E8D46991 9E873AC6 E23513F9 D7845246 8621B960 EACA3A7C 1B6ED55E 5E419187 92E8CBA8 1D78BDB1 7CE38C87$_{\overleftarrow{16}}$

Тест SIGN.L10.1

1 Задать параметры l, r, p, q, a и ключ x из таблицы 10.

2 Задать сообщение длины 32 октета:

$$M \leftarrow \texttt{29312074 73657428 20656761 7373656D 20657479 62206F77 74207974 72696854}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{5ECC4CB7 93432FFE C26C0A00 DF820DE6 1478F921 6AB9ED6A 9DEF17BB DE988CE8}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{01 5D0274D9 B3F48C09 DCB825FA A7E12FC3 60C44D74 4B7A328B DF6F6998 123CA96A 1FC6A144 14E755B3 4561E69D 334CEF67 02438659 9806B4CA 77857618 D49F5327}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L10.2

1 Задать параметры l, r, p, q, a и ключ x из таблицы 10.
2 Задать сообщение длины 54 октета:

$$M \leftarrow \texttt{6567 61737365 6D207469 62206F77 74207974 72696874 20646572 646E7568 2072756F 6620726F 20657479 62207275 6F662079 74666946}_{\overleftarrow{16}}.$$

3 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{5ECC4CB7 93432FFE C26C0A00 DF820DE6 1478F921 6AB9ED6A 9DEF17BB DE988CE8}_{\overleftarrow{16}}.$$

4 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
5 Если

$$S = \texttt{00 93845403 1236A236 CE4A20BB F761407E 2C381473 DDFA18DD 38EA6FEB C2A97411 7387F5C6 50032972 40627E8D 4817DB3B 1A9414D1 9C59BE23 C3317019 0FE96E88}_{\overleftarrow{16}},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест SIGN.L10.3

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 10.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;

5) если процедура проверки ЭЦП возвращает признак, что подпись недействительная, то возвратить ОШИБКА.

3 Возвратить УСПЕХ.

Тест SIGN.L10.4

1 Задать параметры l, r, p, q, a и ключи x, y из таблицы 10.

2 Для $i = 1, 2, \ldots, 10000$ выполнить:

1) псевдослучайным методом сгенерировать сообщение M длины 2048 октета;

2) псевдослучайным методом сгенерировать одноразовый личный ключ k;

3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;

4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';

5) если $S \neq S'$, то возвратить ОШИБКА.

3 Возвратить УСПЕХ.

6.2.2 Алгоритм генерации параметров p и q

Для алгоритма генерации параметров p и q выполняются тесты GPQ.L01 – GPQ.L10.

Входными данными тестов являются параметры l, r, $d_0, \ldots, d_t$ и $r_0, \ldots, r_s$.

Дополнительно во всех тестах используются числа $z_i = i$, где $i = 1, 2, \ldots, 31$.

В тестах для хранения результата генерации параметров используются слова $p \in \{0,1\}^l$ и $q \in \{0,1\}^r$.

Тест GPQ.L01

1 Задать параметры l, r из таблицы 1.

2 Задать параметры $d_0, \ldots, d_4$ равными соответственно 320, 161, 81, 41, 21.

3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 143, 72, 37, 19.

4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.

5 Если значения p и q совпадают со значениями, приведенными в таблице 1, то возвратить УСПЕХ, иначе — ОШИБКА.

Тест GPQ.L02

1 Задать параметры l, r из таблицы 2.

2 Задать параметры $d_0, \ldots, d_4$ равными соответственно 384, 193, 97, 49, 25.

3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 154, 78, 40, 21.

4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.

5 Если значения p и q совпадают со значениями, приведенными в таблице 2, то возвратить УСПЕХ, иначе — ОШИБКА.

Тест GPQ.L03

1 Задать параметры l, r из таблицы 3.

2 Задать параметры $d_0, \ldots, d_5$ равными соответственно 512, 257, 129, 65, 33, 17.

3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 175, 88, 45, 23.

4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 3, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GPQ.L04

1 Задать параметры l, r из таблицы 4.
2 Задать параметры $d_0, \ldots, d_5$ равными соответственно 560, 281, 141, 71, 36, 19.
3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 182, 92, 47, 24.
4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 4, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GPQ.L05

1 Задать параметры l, r из таблицы 5.
2 Задать параметры $d_0, \ldots, d_5$ равными соответственно 656, 329, 165, 83, 42, 22.
3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 195, 98, 50, 26.
4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 5, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GPQ.L06

1 Задать параметры l, r из таблицы 6.
2 Задать параметры $d_0, \ldots, d_5$ равными соответственно 768, 385, 193, 97, 49, 25.
3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 208, 105, 53, 27.
4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 6, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GPQ.L07

1 Задать параметры l, r из таблицы 7.
2 Задать параметры $d_0, \ldots, d_5$ равными соответственно 896, 449, 225, 113, 57, 29.
3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 222, 112, 57, 29.
4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 7, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GPQ.L08

1 Задать параметры l, r из таблицы 8.
2 Задать параметры $d_0, \ldots, d_6$ равными соответственно 1024, 513, 257, 129, 65, 33, 17.
3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 235, 118, 60, 31.
4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 8, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GPQ.L09

1 Задать параметры l, r из таблицы 9.
2 Задать параметры $d_0, \ldots, d_6$ равными соответственно 1168, 585, 293, 147, 74, 38, 20.
3 Задать параметры $r_0, \ldots, r_3$ равными соответственно 249, 125, 63, 32.
4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 9, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GPQ.L10

1 Задать параметры l, r из таблицы 10.
2 Задать параметры $d_0, \ldots, d_6$ равными соответственно 1232,617,309,155,78, 40, 21.
3 Задать параметры $r_0, \ldots, r_4$ равными соответственно 257, 129, 65, 33, 17.
4 Испытуемой реализацией сгенерировать параметры и сохранить результат в p и q.
5 Если значения p и q совпадают со значениями, приведенными в таблице 10, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

6.2.3 Алгоритм генерации параметра a

Для алгоритма генерации параметра a выполняются тесты GA.L01 – GA.L10.
Входными данными тестов являются параметры l, r, p, q и случайное число d.
В тестах для хранения результата генерации параметра используется слово $a \in \{0,1\}^l$.

Тест GA.L01

1 Задать параметры l, r, p, q из таблицы 1.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 1, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L02

1 Задать параметры l, r, p, q из таблицы 2.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 2, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L03

1 Задать параметры l, r, p, q из таблицы 3.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 3, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L04

1 Задать параметры l, r, p, q из таблицы 4.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 4, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L05

1 Задать параметры l, r, p, q из таблицы 5.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 5, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L06

1 Задать параметры l, r, p, q из таблицы 6.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 6, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L07

1 Задать параметры l, r, p, q из таблицы 7.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 7, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L08

1 Задать параметры l, r, p, q из таблицы 8.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 8, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L09

1 Задать параметры l, r, p, q из таблицы 9.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 9, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест GA.L10

1 Задать параметры l, r, p, q из таблицы 10.
2 Задать случайное число: $d \leftarrow 5$.
3 Испытуемой реализацией сгенерировать параметр и сохранить результат в a.
4 Если значение a совпадает со значением, приведенным в таблице 10, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

6.3 Анализ исходных текстов

6.3.1 Корректность использования локальных переменных

Анализ корректности использования локальных переменных проводится для всех функций программы.

Под функцией понимается часть программы, которая выполняет специфические действия и описывается типом возвращаемого значения, именем функции, формальными параметрами. Выполнение функции осуществляется посредством вызова из программы или другой функции. Данному термину в языках программирования соответствуют такие понятия как «функция», «процедура», «метод» и т.п.

Для каждой локальной переменной v функции f эксперт определяет языковые конструкции f, в которых v встречается, и выполняет следующие проверки:

1 При использовании v в левой части оператора присваивания тип присваиваемого значения должен совпадать с типом v, в противном случае эксперт проверяет корректность результата, учитывая стандартные правила преобразования типов, определенные в используемом языке программирования.

2 Перед использованием значения переменной v должна быть выполнена ее инициализация.

3 Обращение на чтение/запись к переменной v должно происходить в пределах установленных для нее границ, в частности, если v является переменной составного типа, то обращение к элементам v должно происходить в пределах заданных размерностей.

4 Если v является переменной вещественного типа, то ее использование в операциях сравнения запрещено.

5 Если память для v выделяется в динамической области, то перед каждым выходом из f динамическая память должна быть освобождена. После освобождения памяти не должно быть языковых конструкций, ссылающихся на нее.

Примечание — В языках программирования, снабженных средствами «сборки мусора», освобождение динамической памяти, выделяемой для локальной переменной, может быть неявным.

6.3.2 Корректность использования глобальных переменных

Для каждой глобальной переменной v эксперт определяет языковые конструкции программы, в которых v встречается. Далее выполняются проверки 1 – 4 из п. 6.3.1 и следующие проверки:

1 Если память для v выделяется в динамической области, то перед каждым выходом из программы динамическая память должна быть освобождена. После освобождения памяти не должно быть языковых конструкций, ссылающихся на нее.

2 Если v может использоваться в многопоточном режиме работы программы, то должны быть реализованы механизмы, обеспечивающие разграничение доступа к v (механизмы синхронизации доступа к глобальной переменной), при этом данные механизмы не должны блокировать доступ к v на неограниченное время.

Примечание – В языках программирования, снабженных средствами «сборки мусора», освобождение динамической памяти, выделяемой для глобальной переменной, может быть неявным.

6.3.3 Корректность использования констант

Эксперт определяет языковые конструкции программы, в которых встречаются следующие константы:

– значений l и r в соответствии с заданным порядком криптографической стойкости (таблица 7.1 СТБ 1176.2);

– значений p, q и a (в случае, если используются параметры, не заданные в ТНПА, то эксперт должен проверить, что используемые параметры сгенерированы в соответствии с алгоритмами, определенными в п. 7 СТБ 1176.2).

Для каждой языковой конструкции эксперт проверяет, что константы заданы правильно.

6.3.4 Корректность программной логики функций программы

Для каждой функции программы эксперт выполняет следующие проверки:

1 Проверка допустимости переданных параметров и используемых глобальных переменных выполняется до их использования. Проверка может не выполняться, если в документации или в комментариях к функции оговорены ограничения на входные данные, при которых функция работает правильно, и эти ограничения соблюдаются для входных данных во всех вызовах функции.

2 Все заданные варианты условных переходов возможны.

3 Все адреса безусловных переходов доступны.

4 Каждый цикл завершается за конечное число шагов, т.е. завершение цикла гарантировано.

5 После выполнения операторов функции завершение функции гарантировано: достигается одна из точек выхода из функции.

6 Отсутствуют недостижимые участки кода.

7 Цепочки последовательных действий (например, открытие файла, чтение из файла, закрытие файла) корректны. Проверка выполняется, если в функции требуется выполнить некоторое действие, требующее определенной последовательности операций.

6.3.5 Корректность вызова стандартных функций

Эксперт проверяет, что в документации, комментариях исходных текстов программ или конфигурационных файлах указана информация, однозначно идентифицирующая вызываемые стандартные функции (версии компилятора, используемых стандартных библиотек и т.п.).

Для каждого вызова стандартной функции в программе эксперт проверяет:

1 Типы и значения параметров, фактически переданных в функцию, соответствуют типам и допустимым значениям параметров функции, указанным в документации на функцию (с учетом стандартных правил преобразования типов языка программирования).

2 Если в документации на функцию указано, что функция возвращает значение, то проводится анализ корректности использования возвращаемого значения, например, корректность использования в операторе присваивания, допустимость игнорирования возвращаемого значения и т.п.

3 Если в документации на функцию указано, что вызов функции может привести к возникновению исключительной ситуации или ошибки, проверяется наличие и корректность обработки исключительной ситуации.

4 Если в документации на функцию указано, что до и после вызова функции должны выполняться определенные действия, то проверяется наличие и корректность выполнения требуемых действий.

6.3.6 Корректность вызова функций программы

Эксперт проверяет, что в документации или комментариях исходных текстов программ для каждой функции программы указана информация, определяющая:

– допустимые входные параметры и возвращаемые значения функции;

– условия, при выполнении которых в ходе работы функции могут возникать исключительные ситуации (при наличии);

– действия, которые должны выполняться до и(или) после вызова функции (при наличии).

Для каждого вызова функции программы эксперт выполняет следующие проверки:

1 Типы и значения параметров, фактически переданных в функцию, соответствуют типам и допустимым значениям параметров функции (с учетом стандартных правил преобразования типов языка программирования).

2 Если функция возвращает значение, то проводится анализ корректности использования возвращаемого значения, например, корректность использования в операторе присваивания, допустимость игнорирования возвращаемого значения и т.п.

3 Если вызов функции может привести к возникновению исключительной ситуации или ошибки, проверяется наличие и корректность обработки исключительной ситуации.

4 Если до и после вызова функции должны выполняться определенные действия, то проверяется наличие и корректность выполнения требуемых действий.

5 Если функция использует глобальные переменные, то проверяется наличие инициализации данных переменных.

6.3.7 Корректность обработки исключительных ситуаций

Под исключительной ситуацией понимается ошибочная ситуация, возникающая при выполнении программы и требующая специальной обработки. Данному термину в языках программирования соответствует такие понятия как «ошибка», «исключение» и т.п.

Для анализа корректности обработки исключительных ситуаций эксперт формирует список функций, включающий стандартные функции и функции программы, вызов которых может приводить к возникновению исключительной ситуации.

Для каждого вызова функции из составленного списка эксперт проверяет:

1 После каждого вызова функции имеются проверка на случай возникновения исключительной ситуации и соответствующая обработка исключительной ситуации.

2 При проверке и обработке исключительной ситуации учтены все возможные виды исключительных ситуаций, возникновение которых возможно для вызываемой функции.

3 Исключительные ситуации обрабатываются адекватно (возвращаются верные коды ошибок и сообщения об ошибках и т.п.).

6.3.8 Корректность реализации криптографических примитивов

Криптографический примитив — это определенное в СТБ 1176.2 вспомогательное преобразование, являющееся композиционной частью некоторого криптографического алгоритма.

В СТБ 1176.2 определены следующие криптографические примитивы:

– алгоритмы арифметики больших чисел (вычитание, сравнение, умножение, деление, умножение по модулю, возведение в степень по модулю);

– реализация датчика случайных чисел, описанного в п. 7.2.2 СТБ 1176.2;

– алгоритм хэширования СТБ 1176.1. Проверка алгоритма должна проводиться по согласованной с Органом по сертификации методике испытаний программы, реализующей криптографический алгоритм СТБ 1176.1. Проверка может не проводиться, если реализация алгоритма уже прошла испытания по указанной методике. В таких случаях эксперт может зачесть результаты испытаний реализации алгоритма предварительно проверив совпадение испытанной ранее реализации с проверяемой.

Примечание – Алгоритмы арифметики больших чисел задаются в СТБ 1176.2 не как алгоритмическая последовательность шагов, а как отображение «аргументы $\rightarrow$ результат», т.е. функционально. Функционально эквивалентные алгоритмы могут быть устроены поразному, поэтому требуется оценка соответствия алгоритмического описания функциональному.

Анализируя структуру программы и используя документацию, эксперт формирует список криптографических примитивов, реализованных в программе. Для каждого примитива $g : A \rightarrow B$, осуществляющего отображение множества A в множество B, эксперт проверяет:

– наличие реализации примитива g в виде отдельной функции, части функции или композиции нескольких функций;

– тождественность реализации примитива g спецификации;

– отсутствие в g операций, не используемых для реализации примитива (наличие операций, не предусмотренных спецификацией на примитив, отражается в приложении к протоколу результатов анализа исходных текстов).

Допускается, что действие отображения g определено на множестве A^*, которое является подмножеством A. В этом случае эксперт дополнительно проверяет, что при выполнении программы прообразы отображения g всегда являются элементами A^*.

6.3.9 Корректность реализации криптографических алгоритмов

В СТБ 1176.2 определены следующие криптографические алгоритмы:

– алгоритм выработки ЭЦП (п. 5 СТБ 1176.2);
– алгоритм проверки ЭЦП (п. 6 СТБ 1176.2);
– алгоритм генерации параметров p и q (п. 7.2 СТБ 1176.2);
– алгоритм генерации параметра a (п. 7.3 СТБ 1176.2).

Анализируя структуру программы и используя документацию, эксперт формирует список криптографических алгоритмов, реализованных в программе. Для каждого алгоритма $f : X \times \Theta \to Y$, который ставит в соответствие входным данным $x \in X$ и параметру $\theta \in \Theta$ результат криптографического преобразования $y \in Y$, эксперт проверяет наличие соответствующей реализации алгоритма. Затем эксперт определяет множества функций реализации, в которых:

1) задаются параметры $\theta \in \Theta$;
2) задаются входные данные $x \in X$;
3) реализуется отображение f;
4) возвращается результат $y \in Y$.

Данные множества функций обозначаются соответственно F_1, F_2, F_3, F_4. Множества могут пересекаться или совпадать.

Для функций из множества F_1 эксперт проверяет корректность задания параметров $\theta \in \Theta$. При этом допустимым является использование в программном компоненте множества параметров Θ^*, которое является подмножеством Θ. Однако, использованное сужение множества Θ не должно состоять в ограничении области значений секретных параметров.

Для функций из множества F_2 эксперт проверяет корректность задания входных данных $x \in X$. При этом допускается, что множество входных данных X^* алгоритма является подмножеством X. Однако, использованное сужение множества входных данных должно быть оговорено в документации.

Примечание – Программа может обрабатывать не все допустимые входные данные. Например, могут шифроваться сообщения только определенной длины.

Для функций из множества F_3 эксперт проверяет тождественность отображения, реализуемого функциями, спецификации на алгоритм f (при возможных ограничениях на параметры и входные данные, использованные в реализации отображения). Для этого, по результатам анализа элементов множества F_3, составляются использованные в реализации f композиции криптографических примитивов. Затем проверяется тождественность реализованных композиций композициям криптографических примитивов, заданным в спецификации и реализующим анализируемый криптографический алгоритм. Кроме этого, эксперт проводит проверку корректности реализации вспомогательных алгоритмов, использованных в программе и не описанных в спецификации. Если такой анализ провести не удается (алгоритм не описан в документации или описан не полно, без указания использованных источников), то по данному пункту проверки выдается отрицательное заключение по причине недостаточности данных. Если использованы простые вспомогательные алгоритмы, призванные оптимизировать выполнение программы и понятные эксперту, то их описание в документации не требуется.

Для функций из множества F_4 эксперт проверяет корректность выдачи результатов $y \in Y$ выполнения криптографического алгоритма. Сужение в реализации алгоритма f множества результатов Y является недопустимым.

6.3.10 Корректность управления секретными данными

Секретные данные — это ключи, параметры и другие данные криптографических алгоритмов, значения которых в соответствии со стандартом или документацией на СКЗИ должны быть защищены от раскрытия, т.е. должны храниться в секрете.

Секретными данными СТБ 1176.2 являются:

– личный ключ;

– секретный параметр;

– подписываемые сообщения (если в соответствии с документацией реализация может использоваться для подписи критических данных).

Эксперт проверяет, что секретные данные используются в строгом соответствии с криптографическим алгоритмом. Допускается использование секретных данных во вспомогательных операциях с целью повышения быстродействия программной реализации криптоалгоритма. Другие операции с секретными данными не допускаются.

Эксперт проверяет, что все копии секретных данных в открытом виде уничтожаются при завершении работы с ними, при этом:

– значение секретных данных, размещенное в области памяти глобальной переменной, уничтожается перед каждым выходом из программы;

– значение секретных данных, размещенное в области памяти локальной переменной функции, уничтожается перед каждым выходом из данной функции;

– значение секретных данных, размещенное в динамической памяти, уничтожается перед каждым освобождением динамической памяти.

Примечание – Под уничтожением понимается такое изменение данных, хранящихся в электронных устройствах (оперативная память, память на магнитных носителях и др.), которое предотвращает их последующее восстановление. Например, уничтожение может состоять в записи в области памяти, занимаемой значениями секретных данных, фиксированных или случайно выбранных значений.

6.3.11 Отсутствие недокументированных возможностей

Эксперт определяет отсутствие недокументированных возможностей по результатам проверок, выполненных в п. 6.3.1 – 6.3.10.

Обнаруженные недокументированные возможности отражаются в протоколе анализа исходных текстов или в приложении к нему.

Приложение А
Форма протокола анализа документации

Экз. {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
результатов анализа документации
объекта испытаний {Поле 4}, реализующего криптографические алгоритмы
согласно СТБ 1176.2-99

1. Документы:

№	Название документа	Номер
1	{Поле 5}	{Поле 6}
2	{Поле 7}	{Поле 8}
3	{Поле 9}	{Поле 10}
4	{Поле 11}	{Поле 12}

2. При анализе документации были выполнены следующие проверки:

№	Название проверки	Отметка о выполнении
1	Проверка документа «Спецификация»	{Поле 13}
2	Проверка документа «Текст программы»	{Поле 13}
3	Проверка документа «Описание программы»	{Поле 13}
4	Проверка документа «Руководство программиста»	{Поле 13}

3. Заключение по результатам анализа документации: документация {Поле 6}, {Поле 8}, {Поле 10}, {Поле 12} соответствует (не соответствует) программе объекта испытаний в части реализации криптографических алгоритмов согласно СТБ 1176.2-99.

Эксперт, {Поле 15} {Поле 16}
{Поле 14}

В поле 1 указывается номер экземпляра протокола.

В поле 2 указывается номер, однозначно идентифицирующий протокол.

В поле 3 указывается дата составления протокола.

В поле 4 указывается название объекта испытаний в соответствии с представленной к испытаниям документацией.

В полях 5 и 6 указываются соответственно полное название документа «Спецификация» и его идентификационный/децимальный номер.

В полях 7 и 8 указываются соответственно полное название документа «Текст программы» и его идентификационный/децимальный номер.

В полях 9 и 10 указываются соответственно полное название документа «Описание программы» и его идентификационный/децимальный номер.

В полях 11 и 12 указываются соответственно полное название документа «Руководство программиста» и его идентификационный/децимальный номер.

В поле 13 указывается результат выполнения проверки: «положительно» — результат проверки положительный, «отрицательно» — результат проверки отрицательный. После завершения анализа документации и заполнения таблицы делается вывод о соответствии (не соответствии) документации программе объекта испытаний в части реализации криптографических алгоритмов согласно СТБ 1176.2. Вывод о соответствии делается только тогда, когда результаты всех проверок являются положительными.

В полях 14 и 16 указываются соответственно должность и Ф. И. О. эксперта.

В поле 15 ставится собственноручная подпись эксперта.

Информация об обнаруженных несоответствиях приводится в протоколе или приложении к протоколу в произвольной форме.

Приложение Б
Форма протокола тестирования

Экз. {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
результатов тестирования
объекта испытаний {Поле 4}, реализующего криптографические алгоритмы
согласно СТБ 1176.2-99

1. Файлы исходных текстов программ:

№	Имя файла	Хэш-значение
1	{Поле 5}	{Поле 6}
2	{Поле 5}	{Поле 6}
...	...	...

Хэш-значения для файлов вычислены согласно {Поле 7}.

2. В ходе тестирования объекта испытаний были выполнены следующие тесты:

№	Название теста	Отметка о выполнении
1	SIGN.L01.1	{Поле 8}
2	SIGN.L01.2	{Поле 8}
...	...	...

3. Заключение по результатам тестирования: объект испытаний {Поле 4} соответствует (не соответствует) требованиям, установленным в СТБ 1176.2-99.

Эксперт, {Поле 10} {Поле 11}
{Поле 9}

В поле 1 указывается номер экземпляра протокола.

В поле 2 указывается номер, однозначно идентифицирующий протокол.

В поле 3 указывается дата составления протокола.

В поле 4 указывается название объекта испытаний в соответствии с представленной к испытаниям документацией.

В поле 5 указываются имена исходных файлов программ объекта испытаний.

В поле 6 указывается значение функции хэширования для тестируемых файлов, вычисленное в соответствии со стандартом, указанным в поле 7. Разрешается использовать функции хэширования, определенные в СТБ 34.101.31 или СТБ 34.101.77.

В поле 8 указывается результат выполнения теста: «положительно» — тест завершен успешно, «отрицательно» — тест завершен с ошибкой; «не проводился» — тест не проводился, так как программа не поддерживает алгоритм или режим, определенный в тесте.

После завершения тестирования и заполнения таблицы делается вывод о соответствии (не соответствии) программной реализации объекта испытаний СТБ 1176.2. Вывод о соответствии делается только тогда, когда все проводимые тесты выполнены успешно.

В полях 9, 11 указываются соответственно должность и Ф. И. О. эксперта.

В поле 10 ставится собственноручная подпись эксперта.

Приложение В
Форма протокола анализа исходных текстов

Экз. {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
результатов анализа исходных текстов программ
объекта испытаний {Поле 4}, реализующего криптографические алгоритмы
согласно СТБ 1176.2-99

1. Файлы исходных текстов программ:

№	Имя файла	Хэш-значение
1	{Поле 5}	{Поле 6}
2	{Поле 5}	{Поле 6}
	...	...

Хэш-значения для файлов вычислены согласно {Поле 7}.

2. В ходе анализа исходных текстов программ были выполнены следующие проверки:

№	Название проверки	Результат проверки
1	Корректность использования локальных переменных	{Поле 8}
2	Корректность использования глобальных переменных	{Поле 8}
3	Корректность использования констант	{Поле 8}
4	Корректность программной логики функций программы	{Поле 8}
5	Корректность вызова стандартных функций	{Поле 8}
6	Корректность вызова функций программы	{Поле 8}
7	Корректность обработки исключительных ситуаций	{Поле 8}
8	Корректность реализации криптографических примитивов	{Поле 8}
9	Корректность реализации криптографических алгоритмов	{Поле 8}
10	Корректность управления секретными данными	{Поле 8}
11	Отсутствие недокументированных возможностей	{Поле 8}

3. Заключение по результатам анализа исходных текстов программ: объект испытаний {Поле 4} соответствует требованиям, установленным в СТБ 1176.2-99.

Эксперт, {Поле 9} {Поле 10} {Поле 11}

В поле 1 указывается номер экземпляра протокола.

В поле 2 указывается номер, однозначно идентифицирующий протокол.

В поле 3 указывается дата составления протокола.

В поле 4 указывается название объекта испытаний в соответствии с представленной к испытаниям документацией.

В поле 5 указываются имена исходных файлов программ объекта испытаний.

В поле 6 указывается значение функции хэширования для исходных файлов программ, вычисленное в соответствии со стандартом, указанным в поле 7. Разрешается использовать функции хэширования, определенные в СТБ 34.101.31 или СТБ 34.101.77.

В поле 8 указывается результат выполнения проверки: «положительно» — результат проверки положительный, «отрицательно» — результат проверки отрицательный, «не проводилась» — проверка не требуется по причине специфики реализации программ объекта испытаний (например, в программе не используются глобальные переменные). После завершения анализа исходных текстов программ и заполнения таблицы делается вывод о соответствии (не соответствии) объекта испытаний СТБ 1176.2. Вывод о соответствии делается только тогда, когда результаты всех проводимых проверок являются положительными.

В полях 9, 11 указываются соответственно должность и Ф. И. О. эксперта.

В поле 10 ставится собственноручная подпись эксперта.

Информация об обнаруженных ошибках и недокументированных возможностях приводится в протоколе или приложении к протоколу в произвольной форме и должна включать:

1) описание ошибки или недокументированной возможности;
2) имя файла и номера строк программы, содержащих ошибку.