|  |  |  |
| --- | --- | --- |
|  | Приложение №1 |  |
| к аттестату аккредитации |  |
| № BY/112 1.0493 |  |
| от 11.09.2006 |  |
| на бланке № \_\_\_\_ |  |
| на 8 листах |  |
| редакция 01 |  |

|  |
| --- |
| **ОБЛАСТЬ АККРЕДИТАЦИИ** от 11 сентября 2024 года  научно-исследовательской лаборатории  проблем безопасности информационных технологий  Учреждения Белорусского государственного университета  «Научно-исследовательский институт  прикладных проблем математики и информатики» |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование объекта | Код | Наименование характеристики (показатель, параметры) | Обозначение документа, устанавливающего требования к объекту | Обозначение документа, устанавливающего метод исследований (испытаний) и измерений, в том числе правила отбора образцов |
| 1 | 2 | 3 | 4 | 5 | 6 |
| **пр-т Независимости, 4, к. 430, 220030, г. Минск** | | | | | |
| 1.1\* | Средства электронной цифровой подписи | 62.09/ 37.077 | Процедура вычисления функции хэширования | СТБ 1176.1-99, раздел 5 | Методика испытаний МИ.190159829.01.01. Согласована Оперативно-аналитическим центром при Президенте Республики Беларусь (ОАЦ) 09.01.2009 |
| 1.2\* | 62.09/ 37.077 | Процедура выработки ЭЦП | СТБ 1176.2-99, раздел 5 | Методика испытаний МИ.190159829.02.01. Согласована ОАЦ 09.01.2009 |
| 1.3\* | 62.09/ 37.077 | Процедура проверки ЭЦП | СТБ 1176.2-99, раздел 6 | Методика испытаний МИ.190159829.02.01. Согласована ОАЦ 09.01.2009 |
| 1.4\* | 62.09/ 37.077 | Процедуры получения параметров | СТБ 1176.2-99, раздел 7 | Методика испытаний МИ.190159829.03.01. Согласована ОАЦ 09.01.2009 |
| 2.1\* | Средства хэширования | 62.09/ 37.077 | Процедура вычисления функции хэширования | СТБ  1176.1-99 | Методика испытаний МИ.190159829.01.01. Согласована ОАЦ 09.01.2009 |
| 2.2\* | 62.09/ 37.077 | Алгоритмы  хэширования | СТБ 34.101.77-2020, раздел 7 | Методика испытаний МИ.190159829.27.02. Согласована ОАЦ 10.09.2021 |
| 3.1\* | Средства шифрования | 62.09/ 37.077 | Режим простой замены | ГОСТ 28147-89, раздел 2 | Методика испытаний МИ.190159829.04.01. Согласована ОАЦ 09.01.2009 |
| 3.2\* | 62.09/ 37.077 | Режим гаммирования | ГОСТ 28147-89, раздел 3 | Методика испытаний МИ.190159829.04.01. Согласована ОАЦ 09.01.2009 |
| 3.3\* | 62.09/ 37.077 | Режим гаммирования с обратной связью | ГОСТ 28147-89, раздел 4 | Методика испытаний МИ.190159829.04.01. Согласована ОАЦ 09.01.2009 |
| 3.4\* | 62.09/ 37.077 | Режим выработки имитовставки | ГОСТ 28147-89, раздел 5 | Методика испытаний МИ.190159829.04.01. Согласована ОАЦ 09.01.2009 |
| 4.1\* | Средства шифрования и контроля целостности | 62.09/ 37.077 | Алгоритм шифрования в режиме простой замены | СТБ 34.101.31-2020, подраздел 7.1 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.2\* | 62.09/ 37.077 | Алгоритм шифрования  в режиме сцепления блоков | СТБ 34.101.31-2020, подраздел 7.2, приложение В | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.3\* | 62.09/ 37.077 | Алгоритм шифрования в режиме гаммирования с обратной связью | СТБ 34.101.31-2020, подраздел 7.3, приложение В | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.4\* | 62.09/ 37.077 | Алгоритм шифрования в режиме счетчика | СТБ 34.101.31-2020, подраздел 7.4, приложение В | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.5\* | 62.09/ 37.077 | Алгоритм выработки имитовставки | СТБ 34.101.31-2020, подраздел 7.5 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.6\* | 62.09/ 37.077 | Алгоритмы аутентифициро­ванного шифрования данных | СТБ 34.101.31-2020, подраздел 7.6, приложение В | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.7\* | 62.09/ 37.077 | Алгоритм  аутентифициро­ванного шифрования ключа | СТБ 34.101.31-2020, подраздел 7.7 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 4.8\* | Средства шифрования и контроля целостности | 62.09/ 37.077 | Алгоритм хэширования | СТБ 34.101.31-2020, подраздел 7.8 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.9\* | 62.09/ 37.077 | Алгоритмы дискового шифрования | СТБ 34.101.31-2020, подраздел 7.9 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.10\* | 62.09/ 37.077 | Алгоритмы шифрования с сохранением формата | СТБ 34.101.31-2020 подраздел 7.10 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.11\* | 62.09/ 37.077 | Алгоритм расширения ключа | СТБ 34.101.31-2020, подраздел 8.1 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.12\* | 62.09/ 37.077 | Алгоритм преобразования ключа | СТБ 34.101.31-2020, подраздел 8.2 | Методика испытаний МИ.190159829.05.03.  Согласована ОАЦ 10.09.2021 |
| 4.13\* | 62.09/ 37.077 | Программируе­мые алгоритмы | СТБ 34.101.77-2020, раздел 8 | Методика испытаний МИ.190159829.27.02. Согласована ОАЦ 10.09.2021 |
| 5.1\* | Средства криптографи­ческой защиты информации | 62.09/ 37.077 | Проверка требований по криптографической поддержке (КП) | СТБ 34.101.27-2022, подраздел 5.1 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.2\* | 62.09/ 37.077 | Проверка требований по реализации сервисов (РС) | СТБ 34.101.27-2022, подраздел 5.2 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.3\* | 62.09/ 37.077 | Проверка требований по управлению доступом (УД) | СТБ 34.101.27-2022, подраздел 5.3 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.4\* | 62.09/ 37.077 | Проверка требований по защите объектов (ЗО) | СТБ 34.101.27-2022, подраздел 5.4 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.5\* | 62.09/ 37.077 | Проверка требований по самотестированию (СТ) | СТБ 34.101.27-2022, подраздел 5.5 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.6\* | 62.09/ 37.077 | Проверка требований по аудиту (АУ) | СТБ 34.101.27-2022, подраздел 5.6 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.7\* | Средства криптографи­ческой защиты информации | 62.09/ 37.077 | Проверка требований по физической безопасности (ФБ) | СТБ 34.101.27-2022, подраздел 5.7 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.8\* | 62.09/ 37.077 | Проверка требований по защите от воздействий (ЗВ) | СТБ 34.101.27-2022, подраздел 5.8 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.9\* | 62.09/ 37.077 | Проверка требований по защите от утечек (ЗУ) | СТБ 34.101.27-2022, подраздел 5.9 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.10\* | 62.09/ 37.077 | Проверка требований по генерации случайных чисел (СЧ) | СТБ 34.101.27-2022, подраздел 5.10 | Методики испытаний МИ.10127.10.01, МИ.10127.10.02, МИ.10127.10.03.  Рекомендованы приказом ОАЦ от 29.12.2022 № 212. |
| 5.11\* | 62.09/ 37.077 | Проверка требований по обновлению программ (ОП) | СТБ 34.101.27-2022, подраздел 5.11 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.12\* | 62.09/ 37.077 | Проверка требований по выводу из эксплуатации (ВЭ) | СТБ 34.101.27-2022, подраздел 5.12 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.13\* | 62.09/ 37.077 | Проверка требований по идентификации и аутентификации (ИА) | СТБ 34.101.27-2022, подраздел 6.1 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.14\* | 62.09/ 37.077 | Проверка требований по настройке среды (НС) | СТБ 34.101.27-2022, подраздел 6.2 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.15\* | 62.09/ 37.077 | Проверка требований по доверенному каналу (ДК) | СТБ 34.101.27-2022, подраздел 6.3 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.16\* | 62.09/ 37.077 | Проверка требований по проектированию и разработке (ПР) | СТБ 34.101.27-2022, подраздел 7.1 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.17\* | Средства криптографи­ческой защиты информации | 62.09/ 37.077 | Проверка требова­ний по поддержке жизненного цикла (ЖЦ) | СТБ 34.101.27-2022, подраздел 7.2 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.18\* | 62.09/ 37.077 | Проверка требова­ний к руководствам (РД) | СТБ 34.101.27-2022, подраздел 7.3 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.19\* | 62.09/ 37.077 | Проверка требований по программе испытаний (ПИ) | СТБ 34.101.27-2022, подраздел 7.4 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 5.20\* | 62.09/ 37.077 | Проверка требований по анализу программ (АП) | СТБ 34.101.27-2022, подраздел 7.5 | Методика испытаний МИ.10127.10.01.  Рекомендована приказом ОАЦ от 29.12.2022 № 212 |
| 6.1\* | Средства разделения секрета | 62.09/ 37.077 | Алгоритм генерации общего открытого ключа | СТБ 34.101.60-2014, подраздел 6.4 | Методика испытаний МИ.190159829.09.02.  Согласована ОАЦ 22.10.2013 |
| 6.2\* | 62.09/ 37.077 | Алгоритм генерации открытых ключей пользователей | СТБ 34.101.60-2014, подраздел 6.5 | Методика испытаний МИ.190159829.09.02.  Согласована ОАЦ 22.10.2013 |
| 6.3\* | 62.09/ 37.077 | Алгоритм генерации открытого ключа пользователя по идентификатору | СТБ 34.101.60-2014, подраздел 6.6 | Методика испытаний МИ.190159829.09.02.  Согласована ОАЦ 22.10.2013 |
| 6.4\* | 62.09/ 37.077 | Алгоритм разделения секрета | СТБ 34.101.60-2014, подраздел 7.3 | Методика испытаний МИ.190159829.09.02.  Согласована ОАЦ 22.10.2013 |
| 6.5\* | 62.09/ 37.077 | Алгоритм восстановления секрета | СТБ 34.101.60-2014, подраздел 7.4 | Методика испытаний МИ.190159829.09.02.  Согласована ОАЦ 22.10.2013 |
| 7.1\* | Средства электронной цифровой подписи и транспорта ключа | 62.09/ 37.077 | Алгоритмы генерации и проверки параметров эллиптической кривой | СТБ 34.101.45-2013,  подраздел 6.1 | Методика испытаний МИ.190159829.11.02.  Согласована ОАЦ  22.10.2013 |
| 7.2\* | 62.09/ 37.077 | Алгоритмы генерации и проверки ключей | СТБ 34.101.45-2013, подраздел 6.2 | Методика испытаний МИ.190159829.11.02.  Согласована ОАЦ  22.10.2013 |
| 7.3\* | Средства электронной цифровой подписи и транспорта ключа | 62.09/ 37.077 | Алгоритм генерации одноразового личного ключа | СТБ 34.101.45-2013, подраздел 6.3 | Методика испытаний МИ.190159829.11.02.  Согласована ОАЦ  22.10.2013 |
| 7.4\* | 62.09/ 37.077 | Алгоритмы выработки и проверки электронной цифровой подписи | СТБ 34.101.45-2013, подраздел 7.1 | Методика испытаний МИ.190159829.11.02.  Согласована ОАЦ  22.10.2013 |
| 7.5\* | 62.09/ 37.077 | Алгоритмы транспорта ключа | СТБ 34.101.45-2013, подраздел 7.2 | Методика испытаний МИ.190159829.11.02.  Согласована ОАЦ  22.10.2013 |
| 7.6\* | 62.09/ 37.077 | Алгоритмы идентификационной электронной цифровой подписи | СТБ 34.101.45-2013, приложение В | Методика испытаний МИ.190159829.11.02.  Согласована ОАЦ  22.10.2013 |
| 8.1\* | Средства генерации псевдослучай­ных чисел | 62.09/ 37.077 | Алгоритм выработки имитовставки HMAC | СТБ 34.101.47-2017, подраздел 6.1 | Методика испытаний МИ.190159829.15.02.  Согласована ОАЦ 08.11.2017 |
| 8.2\* | 62.09/ 37.077 | Алгоритмы генерации псевдослучайных чисел в режиме счетчика | СТБ 34.101.47-2017, подраздел 6.2 | Методика испытаний МИ.190159829.15.02.  Согласована ОАЦ 08.11.2017 |
| 8.3\* | 62.09/ 37.077 | Алгоритм генерации псевдослучайных чисел в режиме HMAC | СТБ 34.101.47-2017, подраздел 6.3 | Методика испытаний МИ.190159829.15.02.  Согласована ОАЦ 08.11.2017 |
| 8.4\* | 62.09/ 37.077 | Алгоритм генерации пароля в режиме HOTP | СТБ 34.101.47-2017, приложение А.7 | Методика испытаний МИ.190159829.15.02.  Согласована ОАЦ 08.11.2017 |
| 8.5\* | 62.09/ 37.077 | Алгоритм генерации пароля в режиме TOTP | СТБ 34.101.47-2017, приложение А.8 | Методика испытаний МИ.190159829.15.02.  Согласована ОАЦ 08.11.2017 |
| 8.6\* | 62.09/ 37.077 | Алгоритм генерации пароля в режиме OCRA | СТБ 34.101.47-2017, приложение А.9 | Методика испытаний МИ.190159829.15.02.  Согласована ОАЦ 08.11.2017 |
| 9.1\* | Средства формирования общего ключа на основе эллиптических кривых | 62.09/ 37.077 | Протокол BMQV | СТБ 34.101.66-2014, подраздел 7.4 | Методика испытаний МИ.190159829.19.01.  Согласована ОАЦ 07.07.2014 |
| 9.2\* | 62.09/ 37.077 | Протокол BSTS | СТБ 34.101.66-2014, подраздел 7.5 | Методика испытаний МИ.190159829.19.01.  Согласована ОАЦ 07.07.2014 |
| 9.3\* | Средства формирования общего ключа на основе эллиптических кривых | 62.09/ 37.077 | Протокол BPACE | СТБ 34.101.66-2014, подраздел 7.6 | Методика испытаний МИ.190159829.19.01.  Согласована ОАЦ 07.07.2014 |
| 9.4\* | 62.09/ 37.077 | Протокол Диффи-Хеллмана | СТБ 34.101.66-2014, приложение А | Методика испытаний МИ.190159829.19.01.  Согласована ОАЦ 07.07.2014 |
| 10.1\* | Средства  управления запросами на получение сертификата | 62.09/ 37.077 | Формат запроса на получение сертификата | СТБ 34.101.17-2012 | Методика испытаний МИ.190159829.24.01.  Согласована ОАЦ 07.10.2016 |
| 11.1\* | Средства управления открытыми ключами | 62.09/ 37.077 | Формат сертификата и расширений сертификата | СТБ 34.101.19-2012, разделы 6, 9, 10, приложения А - Г | Методика испытаний МИ.190159829.21.01.  Согласована ОАЦ 23.11.2015 |
| 11.2\* | 62.09/ 37.077 | Формат списка отозванных сертификатов и его расширений | СТБ 34.101.19-2012, разделы 7, 9, 10, приложения А - Г | Методика испытаний МИ.190159829.21.01.  Согласована ОАЦ 23.11.2015 |
| 11.3\* | 62.09/ 37.077 | Верификация маршрута сертификации | СТБ 34.101.19-2012, разделы 8, 9, 10, приложения А - Г | Методика испытаний МИ.190159829.21.01.  Согласована ОАЦ 23.11.2015 |
| 12.1\* | Средства управления криптографи­ческими сообщениями | 62.09/ 37.077 | Формат неструктурирован­ных данных | СТБ 34.101.23-2012, разделы 6, 7, 14, 15, приложения А, Б | Методика испытаний МИ.190159829.25.01.  Согласована ОАЦ 07.02.2017 |
| 12.2\* | 62.09/ 37.077 | Формат подписанных данных | СТБ 34.101.23-2012, разделы 6, 8, 14, 15, приложения А, Б | Методика испытаний МИ.190159829.25.01.  Согласована ОАЦ 07.02.2017 |
| 12.3\* | 62.09/ 37.077 | Формат конвертованных данных | СТБ 34.101.23-2012, разделы 6, 9, 14, 15, приложения А, Б | Методика испытаний МИ.190159829.25.01.  Согласована ОАЦ 07.02.2017 |
| 12.4\* | 62.09/ 37.077 | Формат хэшированных данных | СТБ 34.101.23-2012, разделы 6, 10, 14, 15, приложения А, Б | Методика испытаний МИ.190159829.25.01.  Согласована ОАЦ 07.02.2017 |
| 12.5\* | 62.09/ 37.077 | Формат шифрованных данных | СТБ 34.101.23-2012, разделы 6, 11, 14, 15, приложения А, Б | Методика испытаний МИ.190159829.25.01.  Согласована ОАЦ 07.02.2017 |
| 12.6\* | 62.09/ 37.077 | Формат аутентифици­руемых данных | СТБ 34.101.23-2012, разделы 6, 12, 14, 15, приложения А, Б | Методика испытаний МИ.190159829.25.01.  Согласована ОАЦ 07.02.2017 |
| 12.7\* | 62.09/ 37.077 | Формат аутентифици­руемых конвертованных данных | СТБ 34.101.23-2012, разделы 6, 13, 14, 15, приложения А, Б | Методика испытаний МИ.190159829.25.01.  Согласована ОАЦ 07.02.2017 |
| 13.1\* | Средства онлайновой проверки статуса сертификата | 62.09/ 37.077 | Онлайновый протокол проверки статуса сертификата | СТБ 34.101.26-2012 | Методика испытаний МИ.190159829.26.02.  Согласована ОАЦ 16.03.2017 |

**Примечание:**

\* – деятельность осуществляется непосредственно в ООС;  
\*\* – деятельность осуществляется непосредственно в ООС и за пределами ООС;  
\*\*\* – деятельность осуществляется за пределами ООС.

Руководитель органа

по аккредитации

Республики Беларусь –

директор государственного

предприятия «БГЦА» Е.В. Бережных