|  |  |
| --- | --- |
|  | Приложение № 3 |
| к аттестату аккредитации |
| № BY/112 2.5155 |
| от 04.10.2019 |
| на бланке № 0010980  на 5 листах |
| редакция 01 |

**ОБЛАСТЬ АККРЕДИТАЦИИ** от 11 июня 2025 года

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Испытательная лаборатория (BY/112 2.5155 от 04.10.2019)  Общество с ограниченной ответственностью «Секьюрити Лаб» | | | | | |
| № 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 |
| **г. Минск, ул. Могилевская, дом 1, пом. 17-13 (12-й этаж)** | | | | | |
| 11.1  \* | Средства  управления запросами на получение сертификата | 62.09/  37.077 | Формат запроса на получение сертификата | СТБ 34.101.17-2012 | ТМИ.СЕКМ.001-2025-01. |
| 12.1  \* | 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 | ТМИ.СЕКМ.002-2025-01 |
| 12.2  \* | Формат списка отозванных сертификатов и его расширений | СТБ 34.101.19-2012, разделы 7, 9, 10, приложения А – Г | ТМИ.СЕКМ.002-2025-01. |
| 12.3  \* | Верификация маршрута сертификации | СТБ 34.101.19-2012, разделы 8, 9, 10, приложения А – Г | ТМИ.СЕКМ.002-2025-01. |
| 13.1  \* | Средства криптографической защиты информации  Средства криптографической защиты информации  Средства криптографической защиты информации | 62.09/  37.077 | Проверка требований по криптографической поддержке (КП) | СТБ 34.101.27-2022, подраздел 5.1 | ТМИ.СЕКМ.005-2025-01. |
| 13.2  \* | Проверка требований по реализации сервисов (РС) | СТБ 34.101.27-2022, подраздел 5.2 | ТМИ.СЕКМ.005-2025-01. |
| 13.3  \* | Проверка требований по управлению доступом (УД) | СТБ 34.101.27-2022, подраздел 5.3 | ТМИ.СЕКМ.005-2025-01. |
| 13.4  \* | Проверка требований по защите объектов (ЗО) | СТБ 34.101.27-2022, подраздел 5.4 | ТМИ.СЕКМ.005-2025-01. |
| 13.5  \* | 62.09/  37.077 | Проверка требований по самотестированию (СТ) | СТБ 34.101.27-2022, подраздел 5.5 | ТМИ.СЕКМ.005-2025-01. |
| 13.6  \* | Проверка требований по аудиту (АУ) | СТБ 34.101.27-2022, подраздел 5.6 | ТМИ.СЕКМ.005-2025-01. |
| 13.7  \* | Проверка требований по физической безопасности (ФБ) | СТБ 34.101.27-2022, подраздел 5.7 | ТМИ.СЕКМ.005-2025-01. |
| 13.8  \* | Проверка требований по защите от воздействий (ЗВ) | СТБ 34.101.27-2022, подраздел 5.8 | ТМИ.СЕКМ.005-2025-01. |
| 13.9  \* | Проверка требований по защите от утечек (ЗУ) | СТБ 34.101.27-2022, подраздел 5.9 | ТМИ.СЕКМ.005-2025-01. |
| 13.10\* | Проверка требований по генерации случайных чисел (СЧ) | СТБ 34.101.27-2022, подраздел 5.10 | ТМИ.СЕКМ.005-2025-01,  ТМИ.СЕКМ.005-2025-02,  ТМИ.СЕКМ.005-2025-03. |
| 13.11\* | Проверка требований по обновлению программ (ОП) | СТБ 34.101.27-2022, подраздел 5.11 | ТМИ.СЕКМ.005-2025-01. |
| 13.12\* | Проверка требований по выводу из эксплуатации (ВЭ) | СТБ 34.101.27-2022, подраздел 5.12 | ТМИ.СЕКМ.005-2025-01. |
| 13.13\* | Проверка требований по идентификации и аутентификации (ИА) | СТБ 34.101.27-2022, подраздел 6.1 | ТМИ.СЕКМ.005-2025-01. |
| 13.14\* | Проверка требований по настройке среды (НС) | СТБ 34.101.27-2022, подраздел 6.2 | ТМИ.СЕКМ.005-2025-01. |
| 13.15\* | Проверка требований по доверенному каналу (ДК) | СТБ 34.101.27-2022, подраздел 6.3 | ТМИ.СЕКМ.005-2025-01. |
| 13.16\* | Проверка требований по проектированию и разработке (ПР) | СТБ 34.101.27-2022, подраздел 7.1 | ТМИ.СЕКМ.005-2025-01. |
| 13.17\* | Проверка требований по поддержке жизненного цикла (ЖЦ) | СТБ 34.101.27-2022, подраздел 7.2 | ТМИ.СЕКМ.005-2025-01. |
| 13.18\* | Проверка требований к руководствам (РД) | СТБ 34.101.27-2022, подраздел 7.3 | ТМИ.СЕКМ.005-2025-01. |
| 13.19\* | Проверка требований по программе испытаний (ПИ) | СТБ 34.101.27-2022, подраздел 7.4 | ТМИ.СЕКМ.005-2025-01. |
| 13.20\* | Проверка требований по анализу программ (АП) | СТБ 34.101.27-2022, подраздел 7.5 | ТМИ.СЕКМ.005-2025-01. |
| 13.21\* | Алгоритмы хэширования | СТБ 34.101.77-2020, раздел 7 | ТМИ.СЕКМ.012-2025-01. |
| 13.22\* | 62.09/  37.077 | Формат запроса на получение сертификата | СТБ 34.101.78-2019, подраздел 8.2 | ТМИ.СЕКМ.013-2025-01. Согласована с ОАЦ 26.05.2025 |
| 13.23\* | Формат сертификата открытого ключа | СТБ 34.101.78-2019, подраздел 8.3 | ТМИ.СЕКМ.013-2025-01. Согласована с ОАЦ 26.05.2025 |
| 13.24\* | Формат списка отозванных сертификатов и его расширений | СТБ 34.101.78-2019, подраздел 8.5 | ТМИ.СЕКМ.013-2025-01. Согласована с ОАЦ 26.05.2025 |
| 14.1  \* | Средства шифрования и контроля целостности | 62.09/  37.077 | Алгоритм шифрования в режиме простой замены | СТБ 34.101.31-2020, подраздел 7.1 | ТМИ.СЕКМ.006-2025-01. |
| 14.2  \* | Алгоритм шифрования  в режиме сцепления блоков | СТБ 34.101.31-2020, подраздел 7.2, приложение В | ТМИ.СЕКМ.006-2025-01. |
| 14.3  \* | Алгоритм шифрования в режиме гаммирования с обратной связью | СТБ 34.101.31-2020, подраздел 7.3, приложение В | ТМИ.СЕКМ.006-2025-01. |
| 14.4  \* | Алгоритм шифрования в режиме счетчика | СТБ 34.101.31-2020, подраздел 7.4, приложение В | ТМИ.СЕКМ.006-2025-01. |
| 14.5  \* | Алгоритм выработки имитовставки | СТБ 34.101.31-2020, подраздел 7.5 | ТМИ.СЕКМ.006-2025-01. |
| 14.6  \* | Алгоритмы аутентифициро­ванного шифрования данных | СТБ 34.101.31-2020, подраздел 7.6, приложение В | ТМИ.СЕКМ.006-2025-01. |
| 14.7  \* | Алгоритм  аутентифициро­ванного шифрования ключа | СТБ 34.101.31-2020, подраздел 7.7 | ТМИ.СЕКМ.006-2025-01. |
| 14.8  \* | Алгоритм хэширования | СТБ 34.101.31-2020, подраздел 7.8 | ТМИ.СЕКМ.006-2025-01. |
| 14.9  \* | Алгоритмы дискового шифрования | СТБ 34.101.31-2020, подраздел 7.9 | ТМИ.СЕКМ.006-2025-01. |
| 14.10\* | Алгоритмы шифрования с сохранением формата | СТБ 34.101.31-2020 подраздел 7.10 | ТМИ.СЕКМ.006-2025-01. |
| 14.11\* | Алгоритм расширения ключа | СТБ 34.101.31-2020, подраздел 8.1 | ТМИ.СЕКМ.006-2025-01. |
| 14.12\* | Алгоритм преобразования ключа | СТБ 34.101.31-2020, подраздел 8.2 | ТМИ.СЕКМ.006-2025-01. |
| 15.1  \* | 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 | ТМИ.СЕКМ.007-2025-01. |
| 15.2  \* | Алгоритмы генерации и проверки ключей | СТБ 34.101.45-2013, подраздел 6.2 | ТМИ.СЕКМ.007-2025-01. |
| 15.3  \* | Алгоритм генерации одноразового личного ключа | СТБ 34.101.45-2013, подраздел 6.3 | ТМИ.СЕКМ.007-2025-01. |
| 15.4  \* | Алгоритмы выработки и проверки электронной цифровой подписи | СТБ 34.101.45-2013, подраздел 7.1 | ТМИ.СЕКМ.007-2025-01. |
| 15.5  \* | Алгоритмы транспорта ключа | СТБ 34.101.45-2013, подраздел 7.2 | ТМИ.СЕКМ.007-2025-01. |
| 15.6  \* | Алгоритмы идентификационной электронной цифровой подписи | СТБ 34.101.45-2013, приложение В | ТМИ.СЕКМ.007-2025-01. |
| 16.1  \* | Средства генерации псевдослучай­ных чисел | 62.09/  37.077 | Алгоритм выработки имитовставки HMAC | СТБ 34.101.47-2017, подраздел 6.1 | ТМИ.СЕКМ.008-2025-01. |
| 16.2  \* | Алгоритмы генерации псевдослучайных чисел в режиме счетчика | СТБ 34.101.47-2017, подраздел 6.2 | ТМИ.СЕКМ.008-2025-01. |
| 16.3  \* | Алгоритм генерации псевдослучайных чисел в режиме HMAC | СТБ 34.101.47-2017, подраздел 6.3 | ТМИ.СЕКМ.008-2025-01. |
| 16.4  \* | Алгоритм генерации пароля в режиме HOTP | СТБ 34.101.47-2017, приложение А.7 | ТМИ.СЕКМ.008-2025-01. |
| 16.5  \* | Алгоритм генерации пароля в режиме TOTP | СТБ 34.101.47-2017, приложение А.8 | ТМИ.СЕКМ.008-2025-01. |
| 16.6  \* | Алгоритм генерации пароля в режиме OCRA | СТБ 34.101.47-2017, приложение А.9 | ТМИ.СЕКМ.008-2025-01. |
| 17.1  \* | Средства разделения секрета  Средства разделения секрета | 62.09/  37.077 | Алгоритм генерации общего открытого ключа | СТБ 34.101.60-2014, подраздел 6.4 | ТМИ.СЕКМ.009-2025-01. |
| 17.2  \* | Алгоритм генерации открытых ключей пользователей | СТБ 34.101.60-2014, подраздел 6.5 | ТМИ.СЕКМ.009-2025-01. |
| 17.3  \* | Алгоритм генерации открытого ключа пользователя по идентификатору | СТБ 34.101.60-2014, подраздел 6.6 | ТМИ.СЕКМ.009-2025-01. |
| 17.4  \* | 62.09/  37.077 | Алгоритм разделения секрета | СТБ 34.101.60-2014, подраздел 7.3 | ТМИ.СЕКМ.009-2025-01. |
| 17.5  \* | Алгоритм восстановления секрета | СТБ 34.101.60-2014, подраздел 7.4 | ТМИ.СЕКМ.009-2025-01. |
| 18.1  \* | Средства,  реализующие протокол защиты транспортного уровня (TLS) | 62.09/  37.077 | Криптонаборы и методы аутентификации | СТБ 34.101.65-2014, раздел 6 | ТМИ.СЕКМ.010-2025-01. |
| 18.2  \* | Протокол Record | СТБ 34.101.65-2014, раздел 7 | ТМИ.СЕКМ.010-2025-01. |
| 18.3  \* | Протокол Handshake | СТБ 34.101.65-2014, раздел 8 | ТМИ.СЕКМ.010-2025-01. |
| 18.4  \* | Протокол Change Cipher Spec | СТБ 34.101.65-2014, раздел 9 | ТМИ.СЕКМ.010-2025-01. |
| 18.5  \* | Протокол Alert | СТБ 34.101.65-2014, раздел 10 | ТМИ.СЕКМ.010-2025-01. |
| 19.1  \* | Средства формирования общего ключа на основе эллиптических кривых | 62.09/  37.077 | Протокол BMQV | СТБ 34.101.66-2014, подраздел 7.4 | ТМИ.СЕКМ.011-2025-01. |
| 19.2  \* | Протокол BSTS | СТБ 34.101.66-2014, подраздел 7.5 | ТМИ.СЕКМ.011-2025-01. |
| 19.3  \* | Протокол BPACE | СТБ 34.101.66-2014, подраздел 7.6 | ТМИ.СЕКМ.011-2025-01. |
| 19.4  \* | Протокол Диффи-Хеллмана | СТБ 34.101.66-2014, приложение А | ТМИ.СЕКМ.011-2025-01. |

**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» | Т.А. Николаева |