|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|  | Приложение №1 |
|  | к аттестату аккредитации  |
| № BY/112 2.5000 |
| от 26.01.2018 |
| на бланке № \_\_\_\_на 9 листах |
| редакция 01 |

**ОБЛАСТЬ АККРЕДИТАЦИИ** от25 января 2023 годаиспытательной лаборатории средств защиты информации закрытого акционерного общества «НТЦ КОНТАКТ» |
| № 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 пер. Студенческий, 7 |
| 1.1\* | Задание по безопасности  | 62.09/37.117 | ASE «Оценка задания по безопасности»  | ТР 2013/027/BY;СТБ 34.101.1-2014;СТБ 34.101.2-2014;СТБ 34.101.3-2014;НПА, в том числе ТНПА, на конкретный вид продукции | МИ ЗБ-05 «Методика оценки задания по безопасности объектов информационных технологий» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 01.06.2014  |
| 2.1\* | Профиль защиты  | 62.09/37.117 | APE «Оценка профиля защиты» | ТР 2013/027/BY;СТБ 34.101.1-2014;СТБ 34.101.2-2014;СТБ 34.101.3-2014;НПА, в том числе ТНПА, на конкретный вид продукции | МИ ПЗ-07 «Методика оценки профиля защиты объектов информационных технологий» (cогласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 17.10.2014) |
| 3.1\* | Продукты и системы информационных технологий | 62.09/37.117 | Испытания объектов оценки по требованиям безопасности на соответствие уровням гарантии оценки | ТР 2013/027/BY;СТБ 34.101.1-2014;СТБ 34.101.2-2014;СТБ 34.101.3-2014;НПА, в том числе ТНПА, на конкретный вид продукции (задание по безопасности) | ТМИ ОИТ-09 «Типовая методика испытаний продуктов и систем информационных техно-логий на соответствие уровням гарантии оценки (УГО1-УГО5)» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 05.06.2017) |
| 4.1\* | Средства криптографической защиты информации, реализующие алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых | 62.09/37.077 | Алгоритмы генерации и проверки параметров эллиптической кривой | ТР 2013/027/BY;СТБ 34.101.45-2013;НПА, в том числе ТНПА, на конкретный вид продукции  | МИ ЭЦПиТК ЭК-03 «Методика испытаний средств криптографической защиты информации, реализующих алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 16.01.2015) |
| 4.2\* | 62.09/37.077 | Алгоритмы генерации и проверки ключей |
| 4.3\* | 62.09/37.077 | Алгоритмы генерации и проверки ЭЦП |
| 4.4\* | 62.09/37.077 | Алгоритмы транспорта ключа |
| 5.1\* | Средства криптографической защиты информации, реализующие форматы сертификатов и списки отозванных сертификатов инфраструктуры открытых ключей | 62.09/37.077 | Форматы сертификата  | ТР 2013/027/BY;СТБ 34.101.19-2012;НПА, в том числе ТНПА, на конкретный вид продукции | МИ СОС ИОК-02«Методика испытаний средств криптографической защиты информации, реализующих форматы сертификатов и списки отозванных сертификатов инфраструктуры открытых ключей» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 16.04.2015) |
| 5.2\* | 62.09/37.077 | Форматы списка отозванных сертификатов |
| 5.3\* | 62.09/37.077 | Маршруты сертификации |
| 5.4\* | 62.09/37.077 | Интернационализированные имена |
| 5.5\* | 62.09/37.077 | Исходный текст программы |
| 6.1\* | Средства криптографической защиты информации, формирующие и (или) обрабатывающие запрос на получение сертификата инфраструктуры открытых ключей | 62.09/37.077 | Синтаксис запроса на получение сертификата | ТР 2013/027/BY;СТБ 34.101.17-2012;НПА, в том числе ТНПА, на конкретный вид продукции | МИ СЗ СОК-12«Методика испытанийсредств криптографической защиты информации на соответствие требованиям государственного стандарта СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 15.08.2017) |
| 6.2\* | 62.09/37.077 | Исходный текст программы |
| 7.1\* | Средства криптографической защиты информации, использующие технологии электронной цифровой подписи и формирующие карточку открытого ключа | 62.09/37.077 | Карточка открытого ключа | СТБ 34.101.49‑2012;НПА, в том числе ТНПА, на конкретный вид продукции | МИ КОК-13 «Методика испытаний средств криптографической защиты информации на соответствие требованиям государственного стандарта СТБ 34.101.49‑2012 «Информационные технологии и безопасность. Формат карточки открытого ключа» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 15.08.2017) |
| 8.1\* | Средства криптографической защиты информации, реализующие онлайновый протокол проверки статуса сертификата инфраструктуры открытых ключей | 62.09/37.077 | Исходный текст программы | ТР 2013/027/BY;СТБ 34.101.26‑2012;НПА, в том числе ТНПА, на конкретный вид продукции | МИ OCSP-14 «Методика испытаний средств криптографической защиты информации на соответствие требованиям государственного стандарта СТБ 34.101.26‑2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 15.08.2017) |
| 8.2\* | 62.09/37.077 | Исходный текст программы |
| 9.1\* | Средства криптографической защиты информации, позволяющие пользователю импортировать, экспортировать и использовать единый набор идентифицированных данных | 62.09/37.077 | Синтаксис обмена персональной информацией | ТР 2013/027/BY;СТБ 34.101.18‑2009;НПА, в том числе ТНПА, на конкретный вид продукции | МИ PFX-15 «Методика испытаний средств криптографической защиты информации на соответствие требованиям государственного стандарта СТБ 34.101.18‑2009 «Информационные технологии. Синтаксис обмена персональной информацией» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 15.08.2017) |
| 9.2\* | 62.09/37.077 | Исходный текст программы |
| 10.1\* | Средства криптографической защиты информации, позволяющие пользователю создавать и обрабатывать криптографические сообщения для обеспечения конфиденциальности, контроля целостности данных | 62.09/37.077 | Синтаксис криптографических сообщений | ТР 2013/027/BY;СТБ 34.101.23‑2012;НПА, в том числе ТНПА, на конкретный вид продукции | МИ CMS-16 «Методика испытаний средств криптографической защиты информации на соответствие требованиям государственного стандарта СТБ 34.101.23‑2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»(согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 15.08.2017) |
| 10.2\* | 62.09/37.077 | Исходный текст программы |
| 11.1\* | Средства криптографической защиты информации, содержащие общие требования, предъявляемые к программным средствам, которые используются для криптографической защиты информации ограниченного распространения  | 62.09/37.077 | Общие требования безопасности | ТР 2013/027/BY;СТБ 34.101.27‑2011;НПА, в том числе ТНПА, на конкретный вид продукции | МИ СКЗИ-17 «Методика испытаний средств криптографической защиты информации на соответствие требованиям государственного стандарта СТБ 34.101.27‑2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»(согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 15.08.2017) |
| 12.1\* | Средства защиты информации, применяемые в инфраструктуре управления привилегиями | 62.09/37.117 | Атрибутные сертификаты | ТР 2013/027/BY;СТБ 34.101.67‑2014; НПА, в том числе ТНПА, на конкретный вид продукции | МИ ИАС-19 «Методика испытаний средств защиты информации, применяемых в инфраструктуре управления привилегиями, на соответствие требованиям СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 29.08.2017) |
| 12.2\* | 62.09/37.117 | Исходный текст программы |
| 13.1\*\* | Средства защиты речевой информации от утечки по каналам высокочастотного навязывания | 62.09/37.078 | Активные методы защиты | ТР 2013/027/BY;СТБ 2352-2013 (п.п.4.3.3, 4.3.4); НПА, в том числе ТНПА, на конкретный вид продукции | СТБ 2352-2013 (п.п.5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.6, 5.4.7, 5.4.8, 5.4.9);МИ ККШ-10 «Методика испытаний средств активной защиты информации на соответствие требованиям к коэффициенту качества шума» (cогласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 07.09.2017) |
| 13.2\*\* | 62.09/37.078 | Время непрерывной работы |
| 14.1\*\* | Генераторы линейного зашумления (ГЛЗ) | 62.09/37.078 | Стабильность параметров  | ТР 2013/027/BY;СТБ 2256-2012 (п.п.4.1.1, 4.1.2.2, 4.1.2.5, 4.1.2.7, 4.1.2.8, 4.1.2.10);НПА, в том числе ТНПА, на конкретный вид продукции | МИ ГЛЗ-11 «Методика испытаний генераторов линейного зашумления на соответствие требованиям государственного стандарта СТБ 2256-2012 «Средства защиты информации. Генераторы линейного зашумления. Общие технические требования и методы испытаний» (согласована с оперативно-аналитическим центром при Президенте Республики Беларусь 07.09.2017);МИ ККШ-10 «Методика испытаний средств активной защиты информации на соответствие требованиям к коэффициенту качества шума» (cогласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 07.09.2017) |
| 14.2\*\* | 62.09/37.078 | Требование к источникам помех |
| 14.3\*\* | 62.09/37.078 | Спектральная плотность шума |
| 14.4\*\* | 62.09/37.078 | Коэффициент качества шума |
| 14.5\*\* | 62.09/37.078 | Контроль работоспособности |
| 14.6\*\* | 62.09/37.078 | Требования к ЭШС в рабочем режиме |
| 14.7\*\*\* | 62.09/37.078 | Предотвращение НСД к органам управления |
| 14.8\*\* | 62.09/37.078 | Отсутствие модуляции |
| 14.9\*\* | 62.09/37.078 | Регулировка уровней помехи |
| 15.1\* | Средства криптографической защиты информации, реализующих формат запроса на получение сертификата | 62.09/37.077 | Проверка синтаксиса запроса на получение сертификата | ТР 2013/027/BY;CТБ 34.101.17-2012;CТБ 34.101.78-2019;НПА, в том числе ТНПА на конкретный вид продукции | МИ СЗ СОК-24«Методика испытаний средств криптографической защиты информации, реализующих формат запроса на получение сертификата, на соответствие требованиям государственных стандартов СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата» и СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»(cогласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 24.11.2020) |
| 15.2\* | 62.09/37.077 | Проверка типа Certification Reguest |
| 15.3 | 62.09/37.077 | Проверка типа Certification Reguest Info |
| 15.4\* | 62.09/37.077 | Анализ исходных текстов программы |
| 15.5\* | 62.09/37.077 | Корректность реализации программной логики функций программы |
| 16.1\* | Средства криптографической защиты информации, реализующие форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей  | 62.09/37.077 | Проверка формата сертификата и расширений сертификата | ТР 2013/027/BY;CТБ 34.101.19-2012;CТБ 34.101.78-2019;НПА, в том числе ТНПА на конкретный вид продукции   | МИ СОС ИОК-25«Методика испытаний средств криптографической защиты информации, реализующих форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей, на соответствие требованиям государственных стандартов;СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей» и СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей» (cогласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 24.11.2020) |
| 16.2\* | 62.09/37.077 | Проверка формата списка отозванных сертификатов и его расширений |
| 16.3\* | 62.09/37.077 | Проверка верификации маршрута сертификации |
| 16.4\* | 62.09/37.077 | Проверка обработки интернационализированных имён |
| 16.5\* | 62.09/37.077 | Анализ исходных текстов программы |
| 16.6\* | 62.09/37.077 | Корректность реализации программной логики функций программы |
| 17.1\* | Программные средства маршрутизатора | 62.09/37.076 | Проверка подсистемы администрирования | ТР 2013/027/BY;CТБ 34.101.14-2017;НПА, в том числе ТНПА на конкретный вид продукции | МИ ПСМ-21 «Методика испытаний программных средств маршрутизатора на соответствие требованиям государственного стандарта СТБ 34.101.14-2017 «Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 21.12.2020) |
| 17.2\* | 62.09/37.076 | Проверка подсистемы управления потоками данных |
| 17.3\* | 62.09/37.076 | Проверка подсистемы аудита безопасности |
| 17.4\* | 62.09/37.076 | Проверка подсистемы обеспечения безопасного функционирования |
| 17.5\* | 62.09/37.076 | Проверка подсистемы восстановления после сбоев и отказов |
| 17.6\* | 62.09/37.076 | Проверка подсистемы тестирования |
| 18.1\* | Межсетевые экраны (МЭ) | 62.09/37.076 | Проверка подсистемы администрирования | ТР 2013/027/BY;CТБ 34.101.73-2017;НПА, в том числе ТНПА на конкретный вид продукции | МИ МЭ-22 «Методика испытаний межсетевых экранов на соответствие требованиям государственного стандарта СТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 21.12.2020) |
| 18.2\* | 62.09/37.076 | Проверка подсистемы управления потоками данных |
| 18.3\* | 62.09/37.076 | Проверка подсистемы аудита безопасности |
| 18.4\* | 62.09/37.076 | Проверка подсистемы обеспечения безопасного функционирования |
| 18.5\* | 62.09/37.076 | Проверка подсистемы восстановления после сбоев и отказов |
| 18.6\* | 62.09/37.076 | Проверка подсистемы тестирования |
| 19.1\* | Комплекс программно-аппаратный криптографической защиты информации «БАС» | 62.09/37.077 | Проверка подсистемы администрирования | ТР 2013/027/BY;CТБ 34.101.73-2017;НПА, в том числе ТНПА на конкретный вид продукции | ЧМИ МЭ-БАС 23/1«Частная методика испытаний комплекса криптографической защиты информации «БАС» на соответствие требованиям государственного стандарта СТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования» (согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 22.03.2021) |
| 19.2\* | 62.09/37.077 | Проверка подсистемы управления потоками данных |
| 19.3 | 62.09/37.077 | Проверка подсистемы аудита безопасности |
| 19.4\* | 62.09/37.077 | Проверка подсистемы обеспечения безопасного функционирования |
| 19.5\* | 62.09/37.077 | Проверка подсистемы восстановления после сбоев и отказов |
| 19.6\* | 62.09/37.077 | Проверка подсистемы тестирования |
| 20.1\* | Комплекс программный виртуальный криптографической защиты информации «БАС-V» | 62.09/37.077 | Проверка подсистемы администрирования | ТР 2013/027/BY;CТБ 34.101.73-2017;НПА, в том числе ТНПА на конкретный вид продукции | ЧМИ МЭ-БАС-V 23/2«Частная методика испытаний комплекса программного виртуального криптографической защиты информации «БАС-V» на соответствие требованиям государственного стандартаСТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования» (согласована с ОАЦ 22.03.2021) |
| 20.2\* | 62.09/37.077 | Проверка подсистемы управления потоками данных |
| 20.3\* | 62.09/37.077 | Проверка подсистемы аудита безопасности |
| 20.4\* | 62.09/37.077 | Проверка подсистемы обеспечения безопасного функционирования |
| 20.5\* | 62.09/37.077 | Проверка подсистемы восстановления после сбоев и отказов |
| 20.6\* | 62.09/37.077 | Проверка подсистемы тестирования |
| 21.1\* | Системы обнаружения и предотвращения вторжений | 62.09/37.076 | Проверка систем обнаружения вторжений | ТР 2013/027/BY;CТБ 34.101.75-2017;НПА, в том числе, ТНПА на конкретный вид продукции | МИ СОПВ-26 «Методика испытаний систем обнаружения и предотвращения вторжений на соответствие требованиям государственного стандарта СТБ 34.101.75-2017 «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения вторжений. Общие требования»(согласована с Оперативно-аналитическим центром при Президенте Республики Беларусь 22.12.2021) |
| 21.2\* | 62.09/37.076 | Проверка систем предотвращения вторжений |

**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