ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

12 марта 2020 г. № 77

О подтверждении соответствия средств защиты информации

Изменения и дополнения:

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10 сентября 2021 г. № 145 (зарегистрировано в Национальном реестре - № 7/4856 от 17.09.2021 г.) <T62104856>;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 28 декабря 2022 г. № 207 (зарегистрировано в Национальном реестре - № 7/5250 от 29.12.2022 г.) <T62205250>

На основании подпункта 6.5 и абзаца третьего подпункта 6.6 пункта 6 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, и в целях реализации части первой статьи 5 и части второй пункта 3 статьи 6 технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (TP 2013/027/BY), утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375, ПРИКАЗЫВАЮ:

1. Утвердить перечень государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (TP 2013/027/BY) (прилагается).

2. Признать утратившими силу:

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 29 августа 2014 г. № 66 «О внесении дополнений и изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 11 октября 2017 г. № 64 «О внесении изменений в некоторые приказы Оперативно-аналитического центра при Президенте Республики Беларусь»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 декабря 2017 г. № 86 «О внесении дополнения в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 марта 2018 г. № 41 «О внесении изменений и дополнения в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94».

3. Настоящий приказ вступает в силу с 14 марта 2020 г.

|  |  |
| --- | --- |
| Начальник | А.Ю.Павлюченко |

|  |  |
| --- | --- |
|  | УТВЕРЖДЕНО  Приказ Оперативно-аналитического  центра при Президенте  Республики Беларусь 12.03.2020 № 77 (в редакции приказа  Оперативно-аналитического  центра при Президенте  Республики Беларусь 28.12.2022 № 207) |

ПЕРЕЧЕНЬ  
государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (TP 2013/027/BY)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование средств защиты информации | Обозначение и наименование государственного стандарта (применяемые требования) | Примечание |
| 1 | Генераторы электромагнитного шума | СТБ 1875-2011 «Средства защиты информации. Генераторы электромагнитного шума. Общие технические требования и методы испытаний» (пункты 5.1.1, 5.1.2.2, 5.1.2.5, 5.1.2.10, 5.1.2.11, 5.1.2.15, 5.1.3) |  |
| 2 | Фильтры помехоподавляющие | СТБ 1966-2012 «Средства защиты информации. Фильтры помехоподавляющие. Общие технические требования и методы испытаний» (пункты 4.1.1.4–4.1.1.6, 4.1.4.3) |  |
| 3 | Генераторы линейного зашумления | СТБ 2256-2012 «Средства защиты информации. Генераторы линейного зашумления. Общие технические требования и методы испытаний» (пункты 4.1.1, 4.1.2.2, 4.1.2.5, 4.1.2.7, 4.1.2.8, 4.1.2.10, 4.1.3.1) |  |
| 4 | Фильтры-ограничители | СТБ 2296-2012 «Средства защиты информации. Фильтры-ограничители. Общие технические требования и методы испытаний» (пункты 4.1.1.1, 4.1.1.2) |  |
| 5 | Средства защиты речевой информации от утечки по акустическому и виброакустическому каналам | СТБ 34.101.28-2011 «Информационные технологии. Средства защиты речевой информации от утечки по акустическому и виброакустическому каналам. Общие технические требования» (пункты 4.2, 4.3.1, 4.3.2, 4.3.5–4.3.10) |  |
| 6 | Средства контроля защищенности речевой информации | СТБ 34.101.29-2011 «Информационные технологии. Средства контроля защищенности речевой информации. Общие технические требования» (пункт 4.2) |  |
| 7 | Средства защиты речевой информации от утечки по каналам высокочастотного навязывания | СТБ 2352-2013 «Информационные технологии. Средства защиты речевой информации от утечки по каналам высокочастотного навязывания. Общие технические требования и методы испытаний» (пункты 4.3.2–4.3.4, 4.7.1.1–4.7.1.4, 4.7.2.1, 4.7.2.2) |  |
| 8 | Средства пассивной технической защиты цифровых телефонных аппаратов от утечки речевой информации по каналам акустоэлектрического преобразования и высокочастотного навязывания | СТБ 34.101.84-2019 «Информационные технологии. Средства пассивной технической защиты цифровых телефонных аппаратов от утечки речевой информации по каналам акустоэлектрического преобразования и высокочастотного навязывания в двухпроводной цифровой линии связи. Общие технические требования и методы испытаний» (пункты 5.3.3–5.3.5, 5.3.7, 5.4.6, 5.5) |  |
| 9 | Средства защиты от воздействия вредоносных программ и антивирусные программные средства | СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования» (пункты 6.2 и (или) 6.3, и (или) 6.4, и (или) 6.5, и (или) 6.6, и (или) 6.7, и (или) 6.8, и (или) 6.9) |  |
| 10 | Маршрутизаторы и коммутаторы, выполняющие функцию маршрутизации | СТБ 34.101.14-2017 «Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования» |  |
| 11 | Операционные системы для использования на автоматизированных рабочих местах органов государственного управления при обработке государственных секретов | СТБ 34.101.51-2011 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы для использования на автоматизированных рабочих местах органов государственного управления при обработке государственных секретов» | Номенклатура контролируемых показателей должна быть определена в задании по безопасности на продукцию, разработанном в соответствии с профилем защиты |
| 12 | Межсетевые экраны | СТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) 7.6) |  |
| 13 | Системы сбора и обработки данных событий информационной безопасности | СТБ 34.101.74-2017 «Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования» (пункты 7.2 и (или) 7.3) |  |
| 14 | Системы обнаружения и предотвращения вторжений | СТБ 34.101.75-2017 «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) 7.6, и (или) 7.7, и (или) 7.8, и (или) 7.9) |  |
| 15 | Системы обнаружения и предотвращения утечек информации из информационных систем | СТБ 34.101.76-2017 «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5) |  |
| 16 | Средства предварительного шифрования |  | Требования к криптографическим алгоритмам (обязательно должен быть реализован один из алгоритмов шифрования) |
| СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.9, и (или) 7.10) | Алгоритмы шифрования |
| СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2), и (или) СТБ 34.101.77-2020 «Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции» (пункт 8.13) | Алгоритмы аутентифицированного шифрования |
| СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (пункт 6.1) | Обязательно при обеспечении контроля целостности (алгоритмы имитозащиты) |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности» (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.31 (пункты 7.8 и (или) 8.1, и (или) 8.2), и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12), и (или) СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых» (пункт 6.1) | Обязательно при предварительном распределении криптографических ключей |
| СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (пункт 7.2) | Обязательно при транспорте криптографических ключей |
| СТБ 34.101.66 (пункты 7.4 и (или) 7.5, и (или) 7.6) | Обязательно при согласовании общего криптографического ключа |
| СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей» (разделы 6, 7, 8), СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей» (пункты 8.3, 8.5) | Обязательно при распространении открытых ключей в виде сертификатов открытых ключей |
| СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)», СТБ 34.101.78 (пункт 8.8) | Обязательно при проверке статуса сертификата открытого ключа в режиме реального времени |
| СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата» (раздел 5), СТБ 34.101.78 (пункт 8.2) | Обязательно при формировании запроса на издание сертификата открытого ключа |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 1 или 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
|  | Требования к форматам |
| СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений» (разделы 9 и (или) 13), и (или) СТБ 34.101.50-2019 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий» (приложение Е) | Обязательно при обеспечении взаимодействия между информационными системами |
| СТБ 34.101.23 (раздел 9), СТБ 34.101.78 (пункт 8.7) | Обязательно при обеспечении взаимодействия между сторонами инфраструктуры открытых ключей |
| 17 | Средства линейного шифрования, в том числе для использования в системах профессиональной радиосвязи Республики Беларусь |  | Требования к криптографическим алгоритмам (обязательно должен быть реализован один из алгоритмов шифрования и имитозащиты или аутентифицированного шифрования) |
|  | СТБ 34.101.31 (пункты 7.2 и (или) 7.3, и (или) 7.4) | Алгоритмы шифрования |
| СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2), и (или) СТБ 34.101.77 (пункт 8.13) | Алгоритмы аутентифицированного шифрования |
| СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1) | Алгоритмы имитозащиты |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.31 (пункты 7.8 и (или) 8.1, и (или) 8.2), и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12), и (или) СТБ 34.101.45 (пункт 7.2), и (или) СТБ 34.101.66 (пункт 6.1) | Обязательно при предварительном распределении криптографических ключей |
| СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)» (пункты В.2.5.1 и (или) B.2.5.2, и (или) В.2.5.3, и (или) В.2.5.4 приложения В), и (или) СТБ 34.101.66 (пункты 7.4 и (или) 7.5, и (или) 7.6, и (или) приложение А), и (или) СТБ 34.101.79-2019 «Информационные технологии и безопасность. Криптографические токены» (пункт 8.4) | Обязательно при согласовании общего криптографического ключа |
| СТБ 34.101.65 | Обязательно при организации защищенного соединения по протоколу защиты транспортного уровня (TLS) версии 1.2 |
| СТБ 34.101.19 (разделы 6, 7, 8), СТБ 34.101.78 (пункты 8.3, 8.5) | Обязательно при распространении открытых ключей в виде сертификатов открытых ключей |
| СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8) | Обязательно при проверке статуса сертификата открытого ключа в режиме реального времени |
| СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2) | Обязательно при формировании запроса на издание сертификата открытого ключа |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 1 или 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
| 18 | Средства выработки электронной цифровой подписи (далее – ЭЦП) |  | Требования к криптографическим алгоритмам |
|  | СТБ 34.101.45 (пункт 7.1) | Алгоритм ЭЦП |
| СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) | Алгоритмы хэширования |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.45 (пункт 6.3), и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.78 (раздел 11), СТБ 34.101.45 (приложение Е) | Обязательно при отсутствии аппаратных методов защиты личного ключа |
| СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2) | Обязательно при формировании запроса на издание сертификата открытого ключа |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
|  | Требования к форматам |
| СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е) | Обязательно при обеспечении взаимодействия между информационными системами |
| СТБ 34.101.80-2019 «Информационные технологии и безопасность. Расширенные электронные цифровые подписи» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) приложение А, пункт 8.1, разделы 9 и (или) 10, и (или) 11) | Обязательно при формировании расширенной электронной цифровой подписи |
| СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6) | Обязательно при обеспечении взаимодействия между сторонами инфраструктуры открытых ключей |
| СТБ 34.101.81-2019 «Информационные технологии и безопасность. Протоколы службы заверения данных», СТБ 34.101.78 (пункт 8.10) | Обязательно при взаимодействии со службой заверения данных инфраструктуры открытых ключей |
| СТБ 34.101.82-2019 «Информационные технологии и безопасность. Протокол постановки штампа времени», СТБ 34.101.78 (пункт 8.9) | Обязательно при взаимодействии со службой штампа времени инфраструктуры открытых ключей |
| 19 | Средства проверки ЭЦП |  | Требования к криптографическим алгоритмам |
| СТБ 34.101.45 (пункт 7.1) и (или) (СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» (разделы 5, 6), СТБ 34.101.50 (приложение В)) | Алгоритмы ЭЦП |
| СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12), и (или) СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования» | Алгоритмы хэширования |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.19 (разделы 6, 7, 8), СТБ 34.101.78 (пункты 8.3, 8.5) | Распространение открытых ключей в виде сертификатов открытых ключей |
| СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8) | Обязательно при проверке статуса сертификата открытого ключа в режиме реального времени |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 1 или 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
|  | Требования к форматам |
| СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е) | Обязательно при обеспечении взаимодействия между информационными системами |
| СТБ 34.101.80 (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) приложение А, пункт 8.2, разделы 9 и (или) 10, и (или) 11) | Обязательно при проверке расширенной электронной цифровой подписи |
| СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6) | Обязательно при обеспечении взаимодействия между сторонами инфраструктуры открытых ключей |
| СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов» (разделы 6, 9) | Обязательно при проверке полномочий подписанта, представленных в виде атрибутного сертификата |
| СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10) | Обязательно при взаимодействии со службой заверения данных инфраструктуры открытых ключей |
| СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9) | Обязательно при взаимодействии со службой штампа времени инфраструктуры открытых ключей |
| 20 | Средства выработки личного ключа или открытого ключа |  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
| 21 | Инфраструктура криптографических токенов |  |  |
| 21.1 | Криптографические токены |  | Требования к криптографическим алгоритмам |
| СТБ 34.101.45 (пункт 7.1) | Алгоритмы ЭЦП |
| СТБ 34.101.45 (пункт 7.2) | Алгоритм транспорта ключа |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.66 (пункт 7.6), СТБ 34.101.79 (пункт 8.3 и 8.5) | Требования к базовому режиму работы в соответствии с СТБ 34.101.79 |
| СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2) | Обязательно при формировании запроса на издание сертификата открытого ключа |
| СТБ 34.101.79 (пункт 8.4, раздел 9) | Обязательно в терминальном режиме работы в соответствии с СТБ 34.101.79 |
| СТБ 34.101.27 (уровень 3 или 4) | Требования по безопасности |
| 21.2 | Клиентская программа для взаимодействия с криптографическим токеном |  | Требования к криптографическим алгоритмам |
| СТБ 34.101.31 (пункт 7.3) | Алгоритм шифрования |
| СТБ 34.101.31 (пункт 7.5) | Алгоритм имитозащиты |
| СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) | Алгоритмы хэширования |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.66 (пункт 7.6), СТБ 34.101.79 (пункты 8.3, 8.5) | Требования к базовому режиму работы в соответствии с СТБ 34.101.79 |
| СТБ 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)» (разделы 6–11, 13), СТБ 34.101.78 (раздел 12) | Обязательно при предоставлении программного интерфейса управления с криптографическим токеном |
| СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2) | Обязательно при формировании запроса на издание сертификата открытого ключа |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 1 или 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
|  | Требования к форматам |
| СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е) | Обязательно при обеспечении взаимодействия между информационными системами |
| СТБ 34.101.80 (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) приложение А, пункты 8.1 и (или) 8.2, разделы 9 и (или) 10, и (или) 11) | Обязательно при формировании расширенной электронной цифровой подписи |
| СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6) | Обязательно при обеспечении взаимодействия между сторонами инфраструктуры открытых ключей |
| СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10) | Обязательно при взаимодействии со службой заверения данных инфраструктуры открытых ключей |
| СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9) | Обязательно при взаимодействии со службой штампа времени инфраструктуры открытых ключей |
| 21.3 | Терминал взаимодействия с криптографическим токеном |  | Требования к криптографическим алгоритмам |
| СТБ 34.101.31 (пункт 7.3) | Алгоритм шифрования |
| СТБ 34.101.31 (пункт 7.5) | Алгоритм имитозащиты |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.79 (пункты 8.4, 8.5, раздел 9) | Требования к терминальному режиму работы в соответствии с СТБ 34.101.79 |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 1 или 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
|  | Требования к форматам |
| СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е) | Обязательно при обеспечении взаимодействия между информационными системами |
| СТБ 34.101.80 (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) приложение А, пункты 8.1 и (или) 8.2, разделы 9 и (или) 10, и (или) 11) | Обязательно при формировании расширенной электронной цифровой подписи |
| СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6) | Обязательно при обеспечении взаимодействия между сторонами инфраструктуры открытых ключей |
| СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10) | Обязательно при взаимодействии со службой заверения данных инфраструктуры открытых ключей |
| СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9) | Обязательно при взаимодействии со службой штампа времени инфраструктуры открытых ключей |
| 22 | Средства контроля целостности |  | Требования к криптографическим алгоритмам (допускается реализация только одного криптографического алгоритма) |
| СТБ 34.101.45 (пункт 7.1) | Алгоритм ЭЦП |
| СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1) | Алгоритмы имитовставки |
| СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) | Алгоритмы хэширования |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами (не требуется выполнения если реализованы только алгоритмы хэширования) |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.45 (пункты 6.2, 6.3) | Обязательно при использовании алгоритма ЭЦП |
|  | Требования по безопасности (не требуется выполнения если реализованы только алгоритмы хэширования) |
| СТБ 34.101.27 (уровень 1 или 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
| 23 | Инфраструктура открытых ключей |  |  |
| 23.1 | Удостоверяющий центр |  | Требования к криптографическим алгоритмам |
| СТБ 34.101.45 (пункт 7.1) | Алгоритм ЭЦП |
| СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) | Алгоритмы хэширования |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.45 (пункт 6.3) | Требования к генерации одноразового личного ключа |
| СТБ 34.101.60-2014 «Информационные технологии и безопасность. Алгоритмы разделения секрета» (раздел 7, таблица А1 приложения А) | Требования к разделению секретов |
| СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2) | Требования к запросу на издание сертификата открытого ключа |
| СТБ 34.101.19 (разделы 6, 8), СТБ 34.101.78 (пункт 8.3) | Требования к сертификату открытого ключа |
| СТБ 34.101.19 (раздел 7), СТБ 34.101.78 (пункт 8.5) | Требования к списку отозванных сертификатов открытых ключей |
| СТБ 34.101.79 (раздел 9) | Требования к сертификату терминала криптографического токена |
| СТБ 34.101.67 (разделы 6, 9) | Требования к атрибутным сертификатам |
| СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8) | Требования к проверке статуса сертификата открытого ключа в режиме реального времени |
| СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9) | Требования к протоколу службы штампа времени |
| СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10) | Требования к протоколу службы заверения данных |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
|  | Требования к форматам |
| СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6) | Требования к подписанным данным |
| СТБ 34.101.23 (разделы 9), СТБ 34.101.78 (пункт 8.7) | Требования к конвертованным данным |
| 23.2 | Регистрационный центр |  | Требования к криптографическим алгоритмам |
| СТБ 34.101.45 (пункт 7.1) | Алгоритм ЭЦП |
| СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) | Алгоритмы хэширования |
|  | Требования к криптографическим протоколам и управлению криптографическими ключами |
| СТБ 34.101.27 (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) | Требования к генерации случайных (псевдослучайных) чисел |
| СТБ 34.101.45 (пункт 6.3) | Требования к генерации одноразового личного ключа |
| СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2) | Требования к запросу на издание сертификата открытого ключа |
| СТБ 34.101.19 (разделы 6, 8), СТБ 34.101.78 (пункт 8.3) | Требования к сертификату открытого ключа |
| СТБ 34.101.19 (раздел 7), СТБ 34.101.78 (пункт 8.5) | Требования к списку отозванных сертификатов открытых ключей |
| СТБ 34.101.67 (разделы 6, 9) | Требования к атрибутным сертификатам |
| СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8) | Обязательно при проверке статуса сертификата открытого ключа в режиме реального времени |
|  | Требования по безопасности |
| СТБ 34.101.27 (уровень 2) | Обязательно для программных средств криптографической защиты информации |
| СТБ 34.101.27 (уровень 3 или 4) | Обязательно для программно-аппаратных средств криптографической защиты информации |
| СТБ 34.101.27 (пункт 5.11) | Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ |
| СТБ 34.101.27 (пункт 5.12) | Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде |
| СТБ 34.101.27 (пункт 6.3) | Обязательно при наличии удаленного доступа к средству криптографической защиты информации |
|  | Требования к форматам |
| СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6) | Требования к подписанным данным |
| СТБ 34.101.23 (раздел 9), СТБ 34.101.78 (пункт 8.7) | Требования к конвертованным данным |
| 24 | Иные программные, программно-аппаратные средства защиты информации | СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности», СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности» | В качестве основы для оценки средств защиты информации используется задание по безопасности |