

ПРИКАЗ
Оперативно-аналитического центра
при Президенте Республики Беларусь

10 сентября 2021 г. № 145

Об изменении приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 марта 2020 г. № 77

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,

ПРИКАЗЫВАЮ:

1. Перечень государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ), утвержденный приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12 марта 2020 г. № 77, изложить в новой редакции (прилагается).

2. Установить, что документы об оценке соответствия средств защиты информации, выданные (принятые) в Национальной системе подтверждения соответствия Республики Беларусь до вступления в силу настоящего приказа, действительны до окончания срока их действия.

3. Настоящий приказ вступает в силу после его официального опубликования.

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

10.09.2021 №145)

ПЕРЕЧЕНЬ

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

№ 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)	

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
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. 16.1.	Средства предварительного 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, приложение В), и (или) 7.10),	Требования к криптографическим алгоритмам

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
		<p>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))* и (или) СТБ 34.101.31 ((пункт 7.6 схема 1 и (или) 2, приложение В), и (или) пункт 7.9)</p> <p>СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.31 (пункты 7.8 и (или) 8.2), и (или) СТБ 34.101.77-2020 «Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции» (раздел 7, и (или) пункт 8.12), и (или) СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (пункт 7.2)</p> <p>СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»,</p> <p>СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»,</p> <p>СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности»)</p>	<p>Требования к криптографическим протоколам и управлению криптографическими ключами при условии предварительного распределения криптографических ключей</p> <p>Требования по безопасности В качестве основы для оценки программно-аппаратных средств криптографической защиты информации используется задание по безопасности с учетом следующих функциональных и гарантийных требований безопасности FCS_CKM.1,; FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.6, FIA_UAU.7, FIA_UID.1, FIA_USB.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.3, FMT_SMF.1, FMT_SMR.1, FPT_FLS.1, FPT_PHP.3, FPT_RCV.1, FPT_RCV.4, FPT_RPL.1, FPT_TST.1</p>

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
16.2.		<p>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) (СТБ 34.101.23 (разделы 9 и (или) 13), СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей» (пункт 8.7)) (СТБ 34.101.31 ((пункты 7.2 и (или) 7.3, и (или) 7.4, приложение В), и (или) 7.10), СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1) и (или) СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2, приложение В) СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы аутентификации и выработки общего ключа на основе эллиптических кривых» (пункты 7.4 и (или) 7.5), и (или) СТБ 34.101.45 (пункт 7.2), (СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей» (разделы 6, 8), СТБ 34.101.78 (пункт 8.3)), (СТБ 34.101.19 (раздел 7), СТБ 34.101.78 (пункт 8.5)) и (или) (СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайн-протокол проверки статуса сертификата (OCSP)», СТБ 34.101.78 (пункт 8.8)) (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)) СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p>	<p>(при наличии в программно-аппаратных средствах криптографической защиты информации ввода ключей добавляется компонент FDP_ITS.1, вывода ключей – компонент FDP_ETC.2) Гарантийные требования безопасности – УГО4 Требования к форматам данных обязательны при обеспечении взаимодействия между информационными системами</p> <p>сторонами инфраструктуры открытых ключей</p> <p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Обязательно при формировании запроса на издание сертификата открытого ключа Требования по безопасности</p>

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
		СТБ 34.101.23 (разделы 9 и (или) 13), и (или) СТБ 34.101.50 (приложение Е) (СТБ 34.101.23 (разделы 9 и (или) 13), СТБ 34.101.78 (пункт 8.7))	Требования к форматам данных обязательны при обеспечении взаимодействия между информационными системами сторонами инфраструктуры открытых ключей
17. 17.1. 17.2.	Средства линейного шифрования, в том числе для использования в системах профессиональной радиосвязи Республики Беларусь	<p>(СТБ 34.101.31 (пункты 7.2 и (или) 7.3, и (или) 7.4, приложение В), СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1)) и (или) СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2, приложение В), и (или) СТБ 34.101.77 (пункт 8.13))</p> <p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.66 (пункт 7.6) и (или) СТБ 34.101.65-2014</p> <p>«Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)» (пункт В.2.5.3 приложения В), и (или) СТБ 34.101.31 (пункты 7.8, 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)</p> <p>СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p> <p>(СТБ 34.101.31 (пункты 7.2 и (или) 7.3, и (или) 7.4, приложение В), СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1)) и (или) СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2, приложение В), и (или) СТБ 34.101.77 (пункт 8.13))</p> <p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.66 (пункты 7.4 и (или) 7.5, и (или) приложение А), и (или) СТБ 34.101.65 (пункты В.2.5.1, и (или) В.2.5.2, и (или) В.2.5.4 приложения В), и (или) СТБ 34.101.45 (пункт 7.2), (СТБ 34.101.19 (разделы 6, 8), СТБ 34.101.78 (пункт 8.3)), (СТБ 34.101.19 (раздел 7), СТБ 34.101.78 (пункт 8.5)) и (или) (СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8)), (СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2))</p> <p>СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p>	<p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами при условии предварительного распределения криптографических ключей</p> <p>Требования по безопасности</p> <p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Обязательно при формировании запроса на издание сертификата открытого ключа</p> <p>Требования по безопасности</p>

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
17.3. 17.4.		<p>(СТБ 34.101.31 (пункты 7.2 и (или) 7.3, и (или) 7.4, приложение В), СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1)) и (или) СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2, приложение В), и (или) СТБ 34.101.77 (пункт 8.13)</p> <p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.65</p> <p>СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3) (СТБ 34.101.31 (пункты 7.2 и (или) 7.3, и (или) 7.4, приложение В), СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1)) и (или) СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2, приложение В), и (или) СТБ 34.101.77 (пункт 8.13)</p> <p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.66 (приложение А), СТБ 34.101.31 (пункты 7.8 и (или) 8.2), и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12), СТБ 34.101.60-2014 «Информационные технологии и безопасность. Алгоритмы разделения секрета» (раздел 7, таблица А1 приложения А)</p> <p>СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p>	<p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Требования по безопасности</p> <p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Требования по безопасности</p>
18. 18.1.	Средства выработки электронной цифровой подписи (далее – ЭЦП)	<p>СТБ 34.101.45 (пункт 7.1), СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12)</p> <p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2), и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), и (или) СТБ 34.101.45 (пункт 6.3), (СТБ 34.101.78 (раздел 11), СТБ 34.101.45 (приложение Е))</p> <p>(СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2))</p> <p>(СТБ 34.101.81-2019 «Информационные технологии и безопасность. Протоколы службы заверения данных», СТБ 34.101.78 (пункт 8.10))</p> <p>(СТБ 34.101.82-2019 «Информационные технологии и безопасность. Протокол постановки штампа времени», СТБ 34.101.78 (пункт 8.9))</p> <p>СТБ 34.101.27 (класс 1 или 2)</p>	<p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Обязательно при формировании запроса на издание сертификата открытого ключа</p> <p>Обязательно при взаимодействии со службой заверения данных</p> <p>инфраструктуры открытых ключей</p> <p>Обязательно при взаимодействии со службой штампа времени</p> <p>инфраструктуры открытых ключей</p> <p>Требования по безопасности</p>

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
18.2.		<p>СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е), и (или) 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, пункты 8.1 и (или) 8.2, разделы 9 и (или) 10, и (или) 11) (СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6))</p> <p>СТБ 34.101.45 (пункт 7.1), СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), и (или) СТБ 34.101.45 (пункт 6.3), (СТБ 34.101.45 (пункт 6.2), СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2)), (СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10)) (СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9)) (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p>	<p>Требования к форматам данных обязательны при обеспечении взаимодействия между: информационными системами</p> <p>сторонами инфраструктуры открытых ключей</p> <p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Обязательно при формировании запроса на издание сертификата открытого ключа</p> <p>Обязательно при взаимодействии со службой заверения данных инфраструктуры открытых ключей</p> <p>Обязательно при взаимодействии со службой штампа времени инфраструктуры открытых ключей</p> <p>Требования по безопасности</p> <p>Требования к форматам данных обязательны при обеспечении взаимодействия между: информационными системами</p>
18.3. 18.3.1.	<p>Инфраструктура криптографических токенов Криптографические токены</p>	<p>СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е), и (или) 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) (СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6))</p> <p>СТБ 34.101.45 (пункт 7.1)</p>	<p>сторонами инфраструктуры открытых ключей</p> <p>Требования к криптографическим алгоритмам</p>

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
18.3.2.	Клиентская программа для взаимодействия с криптографическим токеном	<p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), (СТБ 34.101.66 (пункт 7.6), СТБ 34.101.79-2019 «Информационные технологии и безопасность. Криптографические токены» (пункт 8.3)), СТБ 34.101.79 (пункт 8.5), СТБ 34.101.45 (пункты 6.2, 6.3, 7.2) (СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2))</p> <p>СТБ 34.101.79 (пункт 8.4, раздел 9)</p> <p>(СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p> <p>СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12)</p> <p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), (СТБ 34.101.66 (пункт 7.6), СТБ 34.101.79 (пункт 8.3)), СТБ 34.101.79 (пункт 8.5), (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)), (СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2))</p> <p>(СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10))</p> <p>(СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9))</p> <p>СТБ 34.101.27 (класс 1 или 2)</p> <p>СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е), и (или) 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) (СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6))</p>	<p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Обязательно при формировании запроса на издание сертификата открытого ключа</p> <p>Обязательно в терминальном режиме работы в соответствии с СТБ 34.101.79</p> <p>Требования по безопасности</p> <p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Обязательно при формировании запроса на издание сертификата открытого ключа</p> <p>Обязательно при взаимодействии со службой заверения данных инфраструктуры открытых ключей</p> <p>Обязательно при взаимодействии со службой штампа времени инфраструктуры открытых ключей</p> <p>Требования по безопасности</p> <p>Требования к форматам данных обязательны при обеспечении взаимодействия между информационными системами</p> <p>сторонами инфраструктуры открытых ключей</p>

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
18.3.3.	Терминал взаимодействия с криптографическим токеном	<p>СТБ 34.101.31 (пункты 7.3, 7.5, приложение В)</p> <p>СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.79 (пункты 8.4, 8.5, раздел 9)</p> <p>СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p>	Требования к криптографическим алгоритмам Требования к криптографическим протоколам и управлению криптографическими ключами Требования по безопасности
19.	Средства проверки ЭЦП	<p>(СТБ 34.101.45 (пункт 7.1), 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», СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» (разделы 5,6), СТБ 34.101.50 (приложение В))</p> <p>(СТБ 34.101.19 (разделы 6, 8), СТБ 34.101.78 (пункт 8.3)), (СТБ 34.101.19 (раздел 7), СТБ 34.101.78 (пункт 8.5)) и (или) (СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8))</p> <p>СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутивных сертификатов» (раздел 6, 9) (СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10))</p> <p>(СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9))</p> <p>СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)</p> <p>СТБ 34.101.23 (раздел 8) и (или) СТБ 34.101.50 (приложение Е), и (или) 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) (СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6))</p>	<p>Требования к криптографическим алгоритмам</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Обязательно при работе с атрибутивными сертификатами</p> <p>Обязательно при взаимодействии со службой заверения данных инфраструктуры открытых ключей</p> <p>Обязательно при взаимодействии со службой штампа времени инфраструктуры открытых ключей</p> <p>Требования по безопасности</p> <p>Требования к форматам данных обязательны при обеспечении взаимодействия между информационными системами</p> <p>сторонами инфраструктуры открытых ключей</p>

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
20.	Средства выработки личного ключа или открытого ключа	СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.45 (пункт 6.2) СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)	Требования к криптографическим протоколам и управлению криптографическими ключами Требования по безопасности
21. 21.1. 21.2. 21.3.	Средства контроля целостности	СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47 (пункт 6.1), СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3) СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3) СТБ 34.101.45 (пункт 7.1), СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.45 (пункты 6.2, 6.3) СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3)	Требования к криптографическим алгоритмам Требования к криптографическим алгоритмам Требования к криптографическим протоколам и управлению криптографическими ключами Требования по безопасности Требования к криптографическим алгоритмам Требования к криптографическим протоколам и управлению криптографическими ключами Требования по безопасности
22.	Удостоверяющий центр инфраструктуры открытых ключей	СТБ 34.101.45 (пункт 7.1), СТБ 34.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.45 (пункты 6.2, 6.3), СТБ 34.101.60 (раздел 7, таблица А1), (СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2)), (СТБ 34.101.19 (разделы 6, 8), СТБ 34.101.78 (пункт 8.3)), (СТБ 34.101.19 (раздел 7), СТБ 34.101.78 (пункт 8.5)), (СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8)), СТБ 34.101.67 (раздел 6, 9), СТБ 34.101.78 (пункт 8.4), СТБ 34.101.79 (раздел 9), (СТБ 34.101.81, СТБ 34.101.78 (пункт 8.10)), (СТБ 34.101.82, СТБ 34.101.78 (пункт 8.9)), (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3) (СТБ 34.101.23 (разделы 9 и (или) 13), СТБ 34.101.78 (пункт 8.7)), (СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6))	Требования к криптографическим алгоритмам Требования к криптографическим протоколам и управлению криптографическими ключами Обязательно для республиканского удостоверяющего центра Требования по безопасности Требования к форматам данных

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
23.	Регистрационный центр инфраструктуры открытых ключей	СТБ 34.101.45 (пункт 7.1), СТБ 4.101.31 (пункт 7.8) и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12) СТБ 34.101.27 (пункт 5.6 класс 1 или 2) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3), СТБ 34.101.45 (пункты 6.2, 6.3), (СТБ 34.101.17 (раздел 5), СТБ 34.101.78 (пункт 8.2)), (СТБ 34.101.19 (разделы 6, 8), СТБ 34.101.78 (пункт 8.3)), (СТБ 34.101.19 (раздел 7), СТБ 34.101.78 (пункт 8.5)), (СТБ 34.101.26, СТБ 34.101.78 (пункт 8.8)), СТБ 34.101.67 (раздел 6, 9) СТБ 34.101.27 (класс 1 или 2) или (СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3) (СТБ 34.101.23 (разделы 9 и (или) 13), СТБ 34.101.78 (пункт 8.7)), (СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6))	Требования к криптографическим алгоритмам Требования к криптографическим протоколам и управлению криптографическими ключами Требования по безопасности Требования к форматам данных
24.	Иные программные, программно-аппаратные средства защиты информации	СТБ 34.101.1, СТБ 34.101.2, СТБ 34.101.3	В качестве основы для оценки средств защиты информации используется задание по безопасности

* Требования государственных стандартов, обозначения и (или) наименования которых в пунктах 16 – 23 настоящего перечня указаны в скобках, должны быть реализованы совместно.