Таблица 1 ПЕРЕЧЕНЬ технических нормативных правовых актов, в которых определены требования к криптографическим механизмам

Условные обозначения криптографических механизмов	Криптографические механизмы	Наименование технических нормативных правовых актов
А	криптографические алгоритмы	
АШ	шифрование по алгоритму belt в режиме belt-cbc или belt-cfb или belt-ctr	СТБ 34.101.31-2011 (п. 6.3 или 6 4 или 6.5 раздела 6)
АИ1	выработка имитовставки по алгоритму belt-mac	СТБ 34.101.31-2011 (п. 6.6 раздела 6)
АИ2	выработка имитовставки по алгоритму hmac	СТБ 34.101.47-2017 (п. 6.1 раздела 6)
АШИ	шифрование и имитозащита	СТБ 34.101.31-2011 (п. 6.7 раздела 6)
АХ1	хэширование по алгоритму belt-hash	СТБ 34.101.31-2011 (п. 6.9 раздела 6)
АХ2	хэширование по алгоритму bash	СТБ 34.101.77-2016 (1=128 или 1=192 или 1=256)
АП1	электронная цифровая подпись на основе функции хэширования СТБ 1176.1-99	СТБ 1176.1-99, СТБ 1176.2-99 (разделы 5, 6), СТБ 34.101.50-2019 (приложение В)
АП2	электронная цифровая подпись на основе эллиптических кривых	СТБ 34.101.45-2013 (п. 7.1 раздела 7, таблица Б1 или Б2 или Б3 приложения Б, приложение Д)
П	криптографические протоколы	
ПФ1	формирование общего ключа по протоколу BPACE	СТБ 34.101.66-2014 (п. 7.6 раздела 7), СТБ 34.101.45-2013 (таблица Б1 или Б2 или Б3 приложения Б, приложение Д)
ПФ2	формирование общего ключа по алгоритму DHE_PSK_BIGN	СТБ 34.101.65-2014 (п В.2.5.3 приложения В), СТБ 34.101.45-2013 (таблица Б1 или Б2 или Б3 приложения Б, приложение Д)
ПФ3	формирование общего ключа по протоколам BSTS и BMQV	СТБ 34.101.66-2014 (п. 7.4 или 7.5 раздела 7)СТБ 34.101.45-2013 (таблица Б1 или Б2 или Б3 приложения Б, приложение Д)
ПФ4	формирование общего ключа по алгоритмам DHE_BIGN, DHT_BIGN и DHT_PSK_BIGN	СТБ 34.101.65-2014 (пп. В.2.5.1 или В.2.5.2 или В.2.5.4 приложения В)
ПФ5	формирование общего ключа по протоколу Диффи - Хеллмана	СТБ 34.101.66-2014 (приложение А), СТБ 34.101.45-2013 (таблица Б1 или Б2 или Б3 приложения Б, приложение Д)

ПА1	парольная аутентификация по протоколу BPACE	СТБ 34.101.79-2019 (п. 8.3 раздела 8)
ПА2	аутентификация по протоколу BAUTH	СТБ 34.101.79-2019 (п. 8.4 раздела 8)
ПТ	протокол защиты транспортного уровня TLS	СТБ 34.101.65-2014
ПИ	программный интерфейс взаимодействия с криптографическим токеном	СТБ 34.101.21-2009, СТБ 34.101.78-2019 (раздел 12)
У	управление криптографическими ключами	
УК1	преобразование ключа	СТБ 34.101.31-2011 (п. 7.2 раздела 7) или СТБ 34.101.31-2011 (п. 6.9 раздела 6)
УК2	шифрование и имитозащита ключа	СТБ 34.101.31-2011 (п. 6.8 раздела 6)
УК3	генерация личного и открытого ключей	СТБ 34.101.45-2013 (п. 6.2 раздела 6, таблица Б1 или Б2 или Б3 приложения Б, приложение Д)
УК4	генерация одноразового ключа	СТБ 34.101.45-2013 (п. 6.3 раздела 6)
УК5	транспорт ключа	СТБ 34.101.45-2013 (п. 7.2 раздела 7, таблица Б1 или Б2 или Б3 приложения Б, приложение Д)
УЗ1	разделение секрета	СТБ 34.101.60-2014 (раздел 7, таблица А1 приложения А)
УЗ2	ключевой контейнер	СТБ 34.101.78-2019 (пп. 11.2-11.5 раздела 11), СТБ 34.101.45-2013 (приложение Е)
УС1	запрос на получение сертификата открытого ключа	СТБ 34.101.17-2012, СТБ 34.101.78-2019 (п. 8.2 раздела 8)
УС2	распространение сертификата открытого ключа	СТБ 34.101.19-2012 (разделы 6, 8)СТБ 34.101.78-2019 (п. 8.3 раздела 8)
УС3	проверка статуса сертификата открытого ключа (списки отозванных сертификатов)	СТБ 34.101.19-2012 (раздел 7), СТБ 34.101.78-2019 (п. 8.5 раздела 8)
УС4	проверка статуса сертификата открытого ключа (онлайн)	СТБ 34.101.26-2012, СТБ 34.101.78-2019 (п. 8.8 раздела 8)
УС5	распространение атрибутного сертификата	СТБ 34.101.67-2014
УС6	запрос на отзыв сертификата открытого	СТБ 34.101.78-2019 (п. 8.4 раздела 8, п. 10.5 раздела 10)

	ключа	
УС7	распространение облегченного сертификата открытого ключа	СТБ 34.101.79-2019 (раздел 9)
УГ	генерация случайных или псевдослучайных чисел	СТБ 34.101.27-2011 (п. 5.6 раздела 5) или СТБ 34.101.47-2017 (п. 6.2 или 6.3 раздела 6)
Б	функциональные возможности безопасности	
Б1	программные СКЗИ	СТБ 34.101.27-2011 (класс 1 или 2)
Б2	программно-аппаратные СКЗИ	СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014, где в качестве основы для оценки СКЗИ используется задание по безопасности с учетом функциональных и гарантийных требований безопасности согласно таблице 3 настоящего приложения
Ф	форматы данных	
Ф1	формат конвертованных данных	СТБ 34.101.23-2012 (раздел 9 или 13)
Ф2	профилирование формата конвертованных данных в рамках инфраструктуры открытых ключей (далее - ИОК)	СТБ 34.101.23-2012 (раздел 9 или 13), СТБ 34.101.78-2019 (п. 8.7 раздела 8)
Ф3	формат подписанных данных	СТБ 34.101.23-2012 (раздел 8)
Ф4	профилирование формата подписанных данных в рамках ИОК	СТБ 34.101.23-2012 (раздел 8), СТБ 34.101.78-2019 (п. 8.6 раздела 8)
Ф5	формат расширенной ЭЦП	СТБ 34.101.80-2019 (п. 7.2 или 7.3 или 7.4 или 7.5 раздела 7 или приложение А, п. 8.1 или 8.2 раздела 8, раздел 9 или раздел 10 или раздел 11)
Ф6	формат запроса и ответа службы штампов времени	СТБ 34.101.82-2019, СТБ 34.101.78-2019 (п. 8.9 раздела 8)
Ф7	формат запроса и ответа службы заверения данных	СТБ 34.101.81-2019, СТБ 34.101.78-2019 (п. 8.10 раздела 8)

Таблица 2 ПРОФИЛИ ТРЕБОВАНИЙ к средствам криптографической защиты информации

Средства криптографической защиты информации	Требования к криптографическим алгоритмам	Требования к криптографическим протоколам и управлению ключами	Требования безопасности	Требования к форматам данных
Средства предварительного шифрования	(АШ, АИ1 или АИ2) или АШИ	*УГ, УК1 или УК5	Б1 или Б2	[Ф1], [Ф2]
		УГ, ПФ3 или УК5, УС2, УС3 или УС4		
Средства линейного шифрования, в том числе для использования в системах профессиональной радиосвязи Республики Беларусь	(АШ, АИ1 или АИ2) или АШИ	*УГ, ПФ1 или ПФ2 или УК1 или УК5	Б1 или Б2	
		УГ, ПФ3 или ПФ4 или ПФ5 или УК5, УС2, УС3 или УС4		
		УГ, ПТ		
		УГ, ПФ5, УК1, У31		
Средства выработки электронной цифровой подписи (далее-ЭЦП)	АП2, АХ1 или АХ2	УГ или УК4, У31, У32, [УС1]	Б1	[Ф3],[Ф4],[Ф5]
		УГ или УК4, [УС1]	Б2	
Криптографический токен	АШ, АИ1, АП2, АХ1 или АХ2	УГ, ПА1, ПИ, УК1, УК2, УК3, УК4, УК5, УС1, УС2, [ПА2, УС7]	Б2	[Ф1], [Ф2], [Ф3], [Ф4], [Ф5]
Средства проверки ЭЦП	АП1	УС2, УС3 или УС4, [УС5]	Б1 или Б2	[Ф3],[Ф4],[Ф5]
	АП2, АХ1 или АХ2			
Средства выработки личного ключа или открытого ключа		УГ, УК3	Б1 или Б2	
Средства контроля целостности	АХ1 или АХ2			
	АИ1 или АИ2	УГ, УК1	Б1 или Б2	
	АП2, АХ1 или АХ2	УГ, УК3, УК4	Б1 или Б2	

Примечания:

1. В таблице 2 используются условные обозначения криптографических механизмов в соответствии с таблицей 1.
2. Требования указанные в круглых скобах реализуются совместно. Квадратные скобки содержат требования, носящие рекомендательный характер, за исключением случаев, предусмотренных в пп.5-6.
3. Символом * обозначены наборы требований к криптографическим протоколам и управлению ключами предъявляемые к СКЗИ, в которых секреты предварительно распределены.
4. Средства выработки ЭЦП, средства проверки ЭЦП, средства генерации личных и открытых ключей и криптографический токен являются средством ЭЦП

соответствии с Законом Республики Беларусь от 28 декабря 2009 года "Об электронном документе и электронной цифровой подписи" (Национальный реестр правовых актов Республики Беларусь, 2010 г., N 15, 2/1665).

5. Для СКЗИ, обеспечивающих взаимодействие информационных систем, требования к форматам данных являются обязательными.
6. При необходимости использовать СКЗИ "Криптографический токен" в терминальном режиме в соответствии с СТБ 34.101.79, требования ПА2 и УС7 являются обязательными.
7. Требования к форматам данных Ф6 и Ф7 обязательны к выполнению при взаимодействии СКЗИ с соответствующими службами инфраструктуры открытых ключей.
8. Требование к управлению ключами УС6 обязательно к выполнению при реализации СКЗИ процедуры отзыва сертификата открытого ключа.

Таблица 3 ТРЕБОВАНИЯ к функциональным возможностям безопасности программно-аппаратных средств криптографической защиты информации

Обозначение функционального компонента	Название функционального компонента (в соответствии с СТБ 34.101.2-2014)
FCS_CKM.1	Генерация криптографических ключей
FCS_CKM.2	Распределение криптографических ключей
FCS_CKM.3	Доступ к криптографическим ключам
FCS_CKM.4	Уничтожение криптографических ключей
FCS_COP.1	Криптографические операции
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом на основе атрибутов безопасности
FDP_IFC.1	Ограниченное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_UAU.1	Выбор момента времени аутентификации
FIA_UAU.6	Повторная аутентификация
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.1	Выбор момента времени идентификации
FMT_MOF.1	Управление режимами работы функций безопасности функциональных возможностей безопасности СКЗИ
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.2	Безопасные атрибуты безопасности
FMT_MSA.3	Инициализация атрибутов безопасности
FMT_MTD.1	Управление данными функциональных возможностей безопасности СКЗИ
FMT_MTD.3	Безопасные данные функциональных возможностей безопасности СКЗИ
FMT_SMF.1	Определение функций управления
FMT_SMR.1	Роли безопасности

FPT_FLS.1	Сбой с сохранением безопасного состояния
FPT_PHP.3	Противодействие физической атаке
FPT_RCV.1	Ручное восстановление
FPT_RCV.4	Восстановление функции
FPT_RPL.1	Обнаружение повторного использования
FPT_TST.1	Тестирование функциональных возможностей безопасности СКЗИ
FTP_TRP. 1	Доверенный путь

Примечания:

1. При наличии в программно-аппаратных средствах криптографической защиты информации ввода ключей дополнительно добавляется компонент 1 "Прием данных пользователя без атрибутов безопасности", вывода ключей - компонент FDP_ETC.2 "Передача данных пользователя с атрибутами безопасности".
2. В случае обоснованной невозможности реализовать требования некоторых функциональных компонентов в программно-аппаратном средстве криптографической защиты информации, допускается их выборочное невыполнение.
3. Гарантийные требования безопасности для программно-аппаратных средств криптографической защиты информации должны соответствовать УГ04 по СТБ 34.101.3-2014 "Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности".
4. Компонент гарантии ASE_TSS.1 «Общая функциональная спецификация 00» задания по безопасности программно-аппаратного средства криптографической защиты информации для класса FCS "Криптографическая поддержка" должен подтверждать, что «Общая функциональная спецификация 00» соответствует требованиям СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» (раздел 5) в объеме реализуемом данным средством.