СВОДКА ОТЗЫВОВ

на проект межгосударственного стандарта

ГОСТ ИСО/МЭК TS 19249 «Информационные технологии. Методы и средства обеспечения безопасности. Каталог принципов построения архитектуры и проектирования безопасных продуктов, систем и приложений»

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
1.	По проекту в целом	Национальный орган по стандартизации и метрологии Республики Армения	Замечания и предложения к проекту стандарта отсутствуют	Принято
2.	В целом по стандарту	Государственный комитет по стандартизации Республики Беларусь	Замечания и предложения к проекту стандарта отсутствуют	Принято
3.	В целом по стандарту	Госстандарт Республики Казахстан	Проводится дополнительное внутригосударственное согласование с субъектами национальной системы стандартизации Республики Казахстан	Принято. Замечания в течение срока публичного обсуждения не поступили.
4.	По проекту в целом (сокращения)	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	По тексту проекта стандарта используется значительное количество не раскрытых сокращений (аббревиатур), см. разделы 5 – 7. Согласно ГОСТ 1.3 (п. 6.2) для идентичного стандарта раздел «Обозначения и сокращения» подлежит обязательному переоформлению. Дополнить раздел «Обозначения и сокращения»	Принято, исправлено в соответствии с ГОСТ 1.3

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
			сокращениями, которые не раскрыты по тексту стандарта. При этом сокращение, приведенное на английском языке, раскрыть на английском и на русском языке	
5.	Раздел «Предисловие», пункт 4	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В тексте опечатка. Имеется «ISO/IEC TS 19896-1:2017», а должно быть «ISO/IEC TS 19249:2017». Исправить	Не найдено, вероятно, уже исправлено
6.	Раздел «Предисловие»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Удалить из раздела следующий избыточный текст: «Перевод с английского языка (en). Степень соответствия — идентичная (IDT)»	Удалено
7.	Раздел «Введение» 1-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается абзац изложить в редакции: «В настоящем стандарте описаны принципы построения архитектуры и проектирования средств, систем и приложений для обеспечения безопасности»	Такая редакция ограничивает область стандарта только специализированными продуктами, системами и приложениями для обеспечения безопасности, а стандарт относится к любым продуктам, системам и приложениям к которым предъявляются требования по безопасности.
8.	Раздел «Введение» 2-й абзац, 2-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается данное предложение изложить в редакции: «Настоящий стандарт может применяться при проведении оценки состояния информационной безопасности, выполняемой с использованием ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045»	Принимается в редакции: «Настоящий стандарт может применяться при проведении оценки информационной безопасности, выполняемой с использованием ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045»
9.	Раздел 1 2-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. №	Не ясно, что имеется в виду в данном абзаце: «Настоящий стандарт дает рекомендации по разработке безопасных продуктов, систем и приложений и нацелен на	Предлагается редакция: «Настоящий стандарт дает рекомендации по разработке

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
		3142 от 21.12.2020	более эффективную оценку в отношении свойств безопасности, которые они должны реализовывать». Стандарт должен быть высоко оценен, свойства безопасности должны проходить оценку и эта оценка должна быть выше, чем в других стандартах, или что-то другое имелось в виду	безопасных продуктов, систем и приложений и направлен на обеспечение более эффективной оценки свойств безопасности, которые должны реализовывать эти продукты, системы и приложения».
10.	Раздел 1 3-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Некорректный перевод или пропуск текста: «Настоящий стандарт относится к ИСО/МЭК 15408 и ИСО/МЭК 18045 и адресован как разработчикам, так и специалистам по оценке безопасности продуктов, систем и приложений». Не понятно, в какой мере «относится»: входит в серию стандартов, является дополнением или еще что-то	Предлагается редакция: «Настоящий стандарт относится к области применения стандартов ИСО/МЭК 15408 и ИСО/МЭК 18045 и адресован как разработчикам, так и специалистам по оценке безопасности продуктов, систем и приложений».
11.	Раздел 3 «Термины и определения»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Необходимо гармонизировать терминологию с нормативными правовыми актами ФСТЭК России. Совмещаются понятия «домен безопасности» и «сегмент»	Терминология, по общему правилу, определяется для конкретного стандарта. Какая либо гармонизация может привести к искажению сути применяемых терминов.
12.	Раздел 3 Термин 3.2 «Атрибут безопасности»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Определение не соответствует разделу 5 ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии обеспечения безопасности информационных техно-логий. Часть 2. Функциональные компоненты безопасности»	Применяемый в оригинальном стандарте ISO/IEC TS 19249:2017 термин отличается от термина, применяемого в оригинальном стандарте ISO/IEC T15408, поэтому он и введен в разделе 5.

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
13.	Раздел 3 Термин 3.3 «Привилегия»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Определение не соответствует п. 2.30 ГОСТ 34.321-96 «Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными»	Термин предназначен только для этого стандарта.
14.	Раздел 3 Термин 3.4 «Служба прозрачного шифрования»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Определение данного термина не согласовано. Предлагается словосочетание «служба шифрования» заменить на слово «услуга»	Противоречия нет. «Служба шифрования» это общепринятый термин. Службой предоставляется услуга.
15.	Раздел 4 «Условные обозначения и сокращения»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Приведенный перечень условных обозначений и сокращений не описывает все обозначения и сокращения, встречающиеся в тексте стандарта, например: ДВБ, ИТ, VPN, VLAN, RAID, СУБД и др. Откорректировать перечень условных обозначений и сокращений	Условные обозначения и сокращения соответствуют оригинальному стандарту.
16.	Раздел 5 «Принципы построения архитектуры безопасных продуктов, систем и приложений», подраздел 5.1, 1-й абзац, 1-е	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении предлагается заменить слово «проявлять» на слово «реализовывать»	«Проявлять» можно заменить на «осуществлять».

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
	предложение			
17.	подраздел 5.1, 1-й абзац, 4-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении словосочетание «вызванная использованием таких доменов» предлагается заменить на словосочетание «использующая таких доменов» или на словосочетание « построенная на базе таких доменов»	Словосочетание «вызванная использованием таких доменов» можно заменить на «использующая такие домены».
18.	подраздел 5.1, 1-й абзац, 6-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении слово «обсуждения» предлагается заменить на слово «разработки»	Речь идет именно об «обсуждении» принципов в этом разделе.
19.	подраздел 5.1, 2-й абзац, последнее перечисление	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается начало перечисления записать в редакции: «- часть средства, реализующего функции безопасности, должна быть достаточно мала, чтобы…»	После слова «часть» можно добавить «продукта, системы или приложения»
20.			В последнем перечислении предлагается заменить словосочетание «потенциально опасные возможности» на словосочетание «потенциальные угрозы	Термин «угрозы» применять нецелесообразно исходя из сути этого принципа. Более точный перевод: - часть продукта, системы или приложения, реализующая функции безопасности, должна быть достаточно мала, чтобы ее можно было проанализировать на корректность и возможные побочные эффекты, критичные для безопасности».
21.	подраздел 5.1, 3-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном абзаце предлагается заменить словосочетание «для обеспечения соблюдения» на слова «для выполнения»	Принимается
22.	подраздел 5.1,	ФАУ «ГНИИИ	В данном предложении предлагается заменить	Принимается

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
	последний абзац, 2-е предложение	ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	словосочетание «данная спецификация» на словосочетание «настоящий стандарт»	
23.	Раздел 5 пункт 5.2.1, 1-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Имеется некорректное выражение «Домен - это принцип …». Домен – это некая область, а не принцип. Предлагается уточнить перевод. Предлагаемая редакция: «Разделение на домены - это принцип …». При этом следует вести речь не о «домене», а о «домене безопасности» (п. 3.35 ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»	Редакция принимается. О доменах с точки зрения безопасности говорится в следующем абзаце пункта 5.2.1.
24.	Раздел 5 пункт 5.2.1, 1-й абзац, 2-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается данное предложение изложить в редакции: «Между доменами могут быть определены каналы связи, реализованные таким образом, чтобы контролировать взаимодействие между доменами, а также позволять домену, получающему запрос из другого домена по каналу связи, идентифицировать запрашивающий домен и соответствующе реагировать на полученный запрос»	Принимается
25.	Раздел 5 пункт 5.2.2, 1-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном абзаце предлагается заменить слово «соображения» на слово «требования», слово «здесь» на словосочетание «в настоящем стандарте»	В данном контексте употребляется термин именно «соображения». Замена «здесь» на словосочетание «в настоящем стандарте» принимается
26.	Раздел 5 пункт 5.2.3, 2-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Данное предложение предлагается изложить в редакции: «При оценке аспектов безопасности разделения доменов особенно важны механизмы, реализующие разделение доменов, степень изоляции доменов друг от друга, способы управление доменами (если используются), такие как создание, удаление доменов или изменение привилегий	Очевидно речь идет о Разделе 5 пункт 5.2.6, 2-й абзац, 1-е предложение Принимается редакция:

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
			доменов»	«При оценке аспектов безопасности разделения доменов особенно важны механизмы, обеспечивающие разделение доменов, степень изоляции доменов друг от друга, управление доменами (если используется), такие как создание, удаление доменов или изменение привилегий доменов».
27.	Раздел 5 пункт 5.2.6 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке аспектов безопасности». Заголовок раскрывает содержание	Принимается
28.	Раздел 5 подпункт 5.2.5.1	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Необходимо разделить понятия «домен безопасности» и «сегмент», учитывая нормативную базу Российской Федерации по ИБ, где сегментирование производится между автоматизированными/инфор-мационными системами и их частями разных классов защиты	Перевод соответствует оригиналу стандарта и используемой в нем терминологии.
29.	Раздел 5 подпункт 5.2.5.2, 1-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении словосочетание «физической системе» предлагается использовать в родительном падеже	Принимается
30.	Раздел 5 пункт 5.3.2 2-й абзац		Текст данного абзаца не согласован «Для того, чтобы защитить иерархически более низкие уровни, каждый уровень (или набор смежных уровней) может быть реализован как свой собственный домен с иерархически более низкими уровнями, имеющими больше привилегий, чем более высокие уровни».	Необходимо заменить «имеющими» на «имеющий».

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
			Как следует понимать выражение «домен с иерархически более низкими уровнями, имеющими больше привилегий, чем более высокие уровни»? Предлагается уточнить перевод	
31.	Раздел 5 пункты 5.3.2 и 5.3.3	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данных пунктах используется понятие «абстракции функций и объектов». Не ясно, что понимается под словом «абстракции». В стандарте предлагается либо дать пояснение используемому понятию, например, в примечании, либо заменить перевод этого слова на более понятный	Абстракция, это термин широко используемый в программировании. В частности: «Абстра́кция в объектно-ориентированном программировании — это использование только тех характеристик объекта, которые с достаточной точностью представляют его в данной системе. Основная идея состоит в том, чтобы представить объект минимальным набором полей и методов и при этом с достаточной точностью для решаемой задачи.» Предлагается заменить «абстракции» на «основные свойства».
32.	Раздел 5 пункт 5.4.1 2-й абзац, 2-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Имеется некорректное выражение: «…, чтобы функция инкапсуляции могла безопасно получать всю информацию, необходимую для принятия решения политикой безопасности, …». Решения принимаются не Политикой безопасности, а на основе Политики безопасности. Предлагается уточнить перевод. Предлагаемая редакция: «…, чтобы функция инкапсуляции могла безопасно получать всю информацию, необходимую для принятия решения на основе политики безопасности, …»	Принимается

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
33.	Раздел 5 пункт 5.4.2 1-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении словосочетание «по соображениям» предлагается заменить на словосочетание «для обеспечения»	Принимается
34.	Разделы 5 и 7, пункты 5.4.4 и 7.4	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В тексте данных пунктов слово «setuid» применяется как в составе выражения «механизм setuid», так и отдельно. Предлагается (для обеспечения однозначного восприятия положений проекта стандарта) по тексту стандарта слово «setuid» заключить в кавычки и использовать только в составе выражения «механизм setuid»	Принимается заключить setuid в кавычки – «setuid». Заменить везде на «механизм setuid» некорректно.
35.	Раздел 5 пункт 5.4.5 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке эффективности инкапсуляции». Заголовок раскрывает содержание	Принимается.
36.	Раздел 5 пункт 5.5.3, 1-й абзац, последнее предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении предлагается слово «откатить» заменить на слово «отменить»	Термин «откатить» в контексте возврата к исходному состоянию является общеупотребительным. Использование термина «отменить» может привести к некорректному восприятию рекомендаций, как к отмене выполнения обновления.
37.	Раздел 5 пункт 5.5.4, 2-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении предлагается словосочетание «эффект атаки» заменить на словосочетание «ущерб от атаки»	Принимается.
38.	Раздел 5 пункт 5.5.5, 2-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. №	В данном предложении предлагается слово «приостановкой» заменить на слово «отключением»	Использование термина «отключением» представляется неправильным, так, как он может

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
		3142 от 21.12.2020		пониматься по-разному. Предлагается уточнить термин «приостановкой», заменив на «приостановкой использования».
39.	Раздел 5 пункт 5.5.6 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке системы резервирования». Заголовок раскрывает содержание	Принимается
40.	Раздел 5 подраздел 5.6	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Устаревшее отнесение виртуализации к методам обеспечения безопасности. В настоящее время виртуализация является одним из методов, несущих дополнительные угрозы защищаемой системе	С абсолютизацией данного утверждения нельзя согласиться. Виртуализация, при правильном использовании, позволяет повысить безопасность. Но как и любой другой механизм, имеет и некоторые негативные моменты, которые необходимо учитывать при применении. Об этом, в частности, указывается в подразделе 5.6.5.
41.	Раздел 5 пункт 5.6.1 1-й абзац, 2-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Данное предложение не согласовано. Не ясно, к чему относится фраза «или абстрагироваться от сложной функциональности реальных компонентов»	«Абстрагироваться» нужно заменить на «абстрагирование».
42.	Раздел 5 пункт 5.6.4 1-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается данное предложение изложить в редакции: ««Виртуализация устройств, например, позволяет имитировать несколько устройств, которые в действительности соответствуют одному физическому устройству, и, таким образом, позволяет совместно использовать такое физическое устройство управляемым образом»	Частичное использование термина «физическое» только запутывает, т.к. становится неясным, а что же тогда просто «устройство».

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
43.	Раздел 5 пункт 5.6.4 последний абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Текст первого предложения в данном абзаце сформулирован некорректно: «Гипервизор - это пример, в котором виртуализация используется для эмуляции всей платформы». Предлагается изложить в редакции: «Примером использования виртуализации для эмуляции всей платформы может служить Гипервизор»	Принимается
44.	Раздел 5 пункт 5.6.5 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке уровня виртуализации». Заголовок раскрывает содержание	Принимается
45.	Раздел 6 «Принципы проектирования » п. 6.2.1	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном пункте используется понятие «сущность». Не ясно, что понимается под словом «сущность». В стандарте предлагается либо дать пояснение используемому понятию, например, в примечании, либо заменить перевод этого слова на другой более понятный, например, субъект	«Сущность (entity)» это термин широко используемый в международных стандартах, определяющий некоторое обобщённый предмет (субъект, объект и пр.), которое нельзя заменить конкретным предметом, в частности «субъектом».
46.	Раздел 6 подпункт 6.2.1.2, последний абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Текст данного абзаца не понятен: «Ограничение набора привилегий до минимального уровня требует обнаружения ошибок, а также ситуаций, когда недоверенные пользователи или недоверенный код получают доступ к ресурсам, к которым эта сущность не имеет доступа». Непонятно, кого следует понимать под «этой сущностью»? Предлагается абзац изложить в редакции: «Ограничение	В данном контексте совершенно очевидно, что речь идёт о получении доступа некоторой «сущностью», которой может быть недоверенный пользователь или недоверенный код.

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
			набора привилегий до минимального уровня требует обнаружения ошибок, а также ситуаций, когда сущности (недоверенные пользователи или недоверенный код) получают доступ к ресурсам, к которым эти сущности не имеют доступа»	
47.	Раздел 6, подпункт 6.2.1.3 2-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Текст первого предложения в данном абзаце сформулирован некорректно: «Большой набор привилегий может снизить этот риск, но обычно он значительно увеличивает сложность управления ими». Непонятно к чему следует относить слова «он» и «ими», к набору привилегий или к риску? Предлагается абзац изложить в редакции: «Большой набор привилегий может снизить этот риск, но обычно этот набор значительно увеличивает сложность управления рисками»	Предлагаемая редакция искажает суть, речь идёт об управлении привилегиями, а не рисками. Предлагается уточнение: «Большой набор привилегий может снизить этот риск, но обычно такой набор значительно увеличивает сложность управления привилегиями»
48.	Раздел 6, подпункт 6.2.1.5 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке структуры привилегий». Заголовок раскрывает содержание	Предлагается «Замечания по оценке привилегий».
49.	Раздел 6, подпункт 6.2.1.5 2-й абзац, 2-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении после слова «пути» предлагается поставить точку, остальную часть предложения удалить	Предложение только ухудшает редакцию.
50.	Раздел 6, подпункт		Предлагается название пункта записать в редакции: «Замечания по оценке поверхности атаки». Заголовок	Принимается

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
	6.2.2.6		раскрывает содержание	
51.	Раздел 6, подпункт 6.2.3.3 2-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Не понятен перевод данного предложения: «Довольно часто параметры интерфейса, принадлежащего поверхности атаки, преднамеренно создаются злоумышленником для тестирования или эксплуатации потенциальных уязвимостей». Требуется уточнить	Суть предложения довольно ясна. Речь идет о том, что злоумышленник, пытающийся использовать интерфейс для проведения атаки, создаёт для этого интерфейса набор параметров, позволяющий осуществить тестирование или эксплуатацию потенциальных уязвимостей. Слово «преднамеренно» можно заменить на «целенаправленно».
52.	Раздел 6, подпункт 6.2.3.6 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке централизованной проверки параметров». Заголовок раскрывает содержание	Принимается
53.	Раздел 6 подпункт 6.2.3.6, 1-й абзац 1-е перечисление	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном перечислении предлагается словосочетание «должно быть» заменить на «можно будет»	Принято
54.	Раздел 6 подпункт 6.2.3.6, 1-й абзац, 2-е перечисление	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается перечисление записать в редакции: «В противном случае, эту функцию возможно легко обойти или нейтрализовать». Функция безопасности не несёт вред, поэтому её невозможно обезвредить	Очевидно 1-е перечисление. Принимается
1.	Раздел 6,	ФАУ «ГНИИИ	По тексту пункта используется выражение «принцип	Принято

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
	пункт 6.2.4 в целом	ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	централизованных общих служб безопасности», которое в некоторой степени не совсем корректное. Предлагается (в случае, когда по тексту речь идет о принципе) данное выражение заменить выражением «принцип централизации общих служб безопасности»	
2.	Раздел 6 подпункт 6.2.4.5, 1-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном абзаце английскую аббревиатуру «PKI» необходимо перевести и, с учетом того, что она не употребляется в разделе 4 настоящего стандарта, расшифровать	Предлагается после PKI добавить «(служба открытых ключей)».
3.	Раздел 6 подпункт 6.2.4.5, 2-й абзац, 6-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении предлагается заменить слово «незамысловатые» на «упрощенные»	Принято
4.	Раздел 6 подпункт 6.2.4.5, 3-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается в данном абзаце заменить словосочетание «… что маловероятно…» на «…чтобы минимизировать вероятность того…»	Предлагается уточнить редакцию: «…чтобы сделать атаки по сторонним каналам невозможными или настолько трудными для эксплуатации, что злоумышленник, скорее всего, не будет тратить на это свои ресурсы.
5.	Раздел 6 подпункт 6.2.4.6 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке централизованных служб безопасности». Заголовок раскрывает содержание	Принято
6.	Раздел 6 п. 6.2.5 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В названии данного пункта предлагается заменить словосочетание «исключительная ситуация» на словосочетание «инцидент безопасности»	Замена нецелесообразна. Разработчики стандарта, скорее всего, сознательно использовали понятия «ошибки» и «исключительные

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
				ситуации», а не «инциденты безопасности», т.к. ошибки и исключительные ситуации не обязательно могут приводить к инцидентам безопасности.
7.	Раздел 6 подпункт 6.2.5.4, 1-й абзац, 1-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается данное предложение изложить в редакции: «В некоторых случаях система или средство способны отслеживать определенные события, которые приводят к ситуациям, когда с большой вероятностью могут возникнуть ошибки или инциденты безопасности, чтобы предпринять корректирующие действия еще до возникновения ошибки»	Целесообразно уточнить редакцию следующим образом: «В некоторых случаях система или продукт могут отслеживать определенные события, которые могут привести к состояниям, когда с большой вероятностью могут возникнуть ошибки или исключительные ситуации, и предпринимать корректирующие действия еще до их возникновения.»
8.	Раздел 6 подпункт 6.2.5.4, 2-й абзац, 2-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается данное предложение изложить в редакции: «Порождение такой же или подобной ошибки во время реагирования часто имеет критические последствия, например, такие, как полное отключение средства или системы»	Предлагается предложение изложить в редакции: «Порождение такой же или подобной ошибки во время реагирования часто имеет критические последствия, например, такие, как полное прекращение функционирования продукта или системы»
9.	Раздел 6 подпункт 6.2.5.6 Название	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается название пункта записать в редакции: «Замечания по оценке принципа обработки ошибок и инциденты безопасности». Заголовок раскрывает содержание	Предлагается название пункта записать в редакции: «Замечания по оценке обработки ошибок и исключительных ситуаций
10.	Раздел 6 подраздел 6.3	ФАУ «ГНИИИ ПТЗИ ФСТЭК	Предлагается данное предложение изложить в редакции: «Минимизация поверхности атаки затрудняет, но не	Принято

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
	15-й абзац, 2-е предложение	России» исх. № 3142 от 21.12.2020	исключает взлом системы»	
11.	Раздел 7 «Мероприятия по оценке архитектурных принципов» подраздел 7.1 1-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Имеется неоднозначный текст: «В этом разделе объясняются аспекты принципов построения архитектуры, описанных в разделе 5, и семейства требований доверия ADV_ARC, описанного в ИСО/МЭК 15408-3. Он предоставляет собой руководство, как принципы архитектуры, определенные в настоящей спецификации, соотносятся с описанием этого семейства требований доверия в ИСО/МЭК 15408-3 …».	Можно «Он» заменить на «Раздел»
			Непонятно к чему следует относить слово «Он», к разделу 7 или к стандарту ИСО/МЭК 15408-3? Предлагается уточнить перевод, исключив отмеченную неоднозначность	
12.	Раздел 7 подраздел 7.1, 1-й абзац, 2-е предложение	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	В данном предложении предлагается словосочетание «настоящей спецификации» заменить на словосочетание «настоящего стандарта»	Принято
13.	Раздел 7, подраздел 7.2 1-й абзац	ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается выражение «Концепция разделения доменов» заменить выражением «Концепция разделения на домены»	Принято
14.		ФАУ «ГНИИИ ПТЗИ ФСТЭК России» исх. № 3142 от 21.12.2020	Предлагается выражение «… разработчик может разбить ОО на подсистемы, состоящие из более чем одного домена, или домены, которые состоят из нескольких подсистем» заменить выражением «… разработчик может разбить ОО на подсистемы, состоящие из более чем одного домена, или	Принято

Номер п/п	Структурный элемент редакции стандарта	Наименование организации или иного лица (номер письма, дата)	Замечание, предложение, предлагаемая редакция	Заключение Разработчика
1	2		3	
			домены, которые охватывают несколько подсистем»	

Заместитель директора ФИЦ ИУ РАН А.А. Зацаринный