О СЕРТИФИКАЦИИ

Что означают сертификаты ФСТЭК России и ФСБ России Для чего они нужны

Михаил Зубов

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Новости сертификации и импортозамещения

Планируется увеличение штрафов по КИИ

28.01.2021

Госдума приняла в первом чтении законопроект, который устанавливает административную ответственность за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры (КИИ). Изменения в КоАП предполагают за нарушение требований безопасности таких объектов штраф: для должностных лиц – от 10 тыс. до 50 тыс. рублей, а для юрлиц – от 50 тыс. до 100 тыс. рублей

ГИСы обяжут использовать СКЗИ

02.12.2020

В государственных информационных системах (ГИС) появится криптография. Федеральная служба безопасности РФ разработала проект приказа об утверждении требований о защите информации, содержащейся в ГИС, с использованием средств криптографической защиты информации (СКЗИ).

Новости сертификации и импортозамещения

Установлены требования к ПО на объектах КИИ
15.01.2021

Минцифры подготовило проект постановления правительства, которым утверждаются критерии требований к программному обеспечению (ПО), телекоммуникационному оборудованию и радиоэлектронной продукции, используемым на объектах критической информационной инфраструктуры (КИИ). Кроме того, в документе прописан порядок перехода на преимущественное использование российского ПО и оборудования.

Опубликованы требования согласия на обработку ПДн
29.01.2021

Роскомнадзор разработал требования к содержанию согласия на обработку персональных данных (ПДн). Согласие потребуют оформлять на русском языке. Оно должно содержать ФИО, номер телефона, адрес электронной почты или почтовый адрес субъекта ПДн, а также наименование и адрес оператора, получающего согласие.

Плюсы сертификации

- Сертификат – это свидетельство проведения независимой экспертизы квалифицированными государственными органами

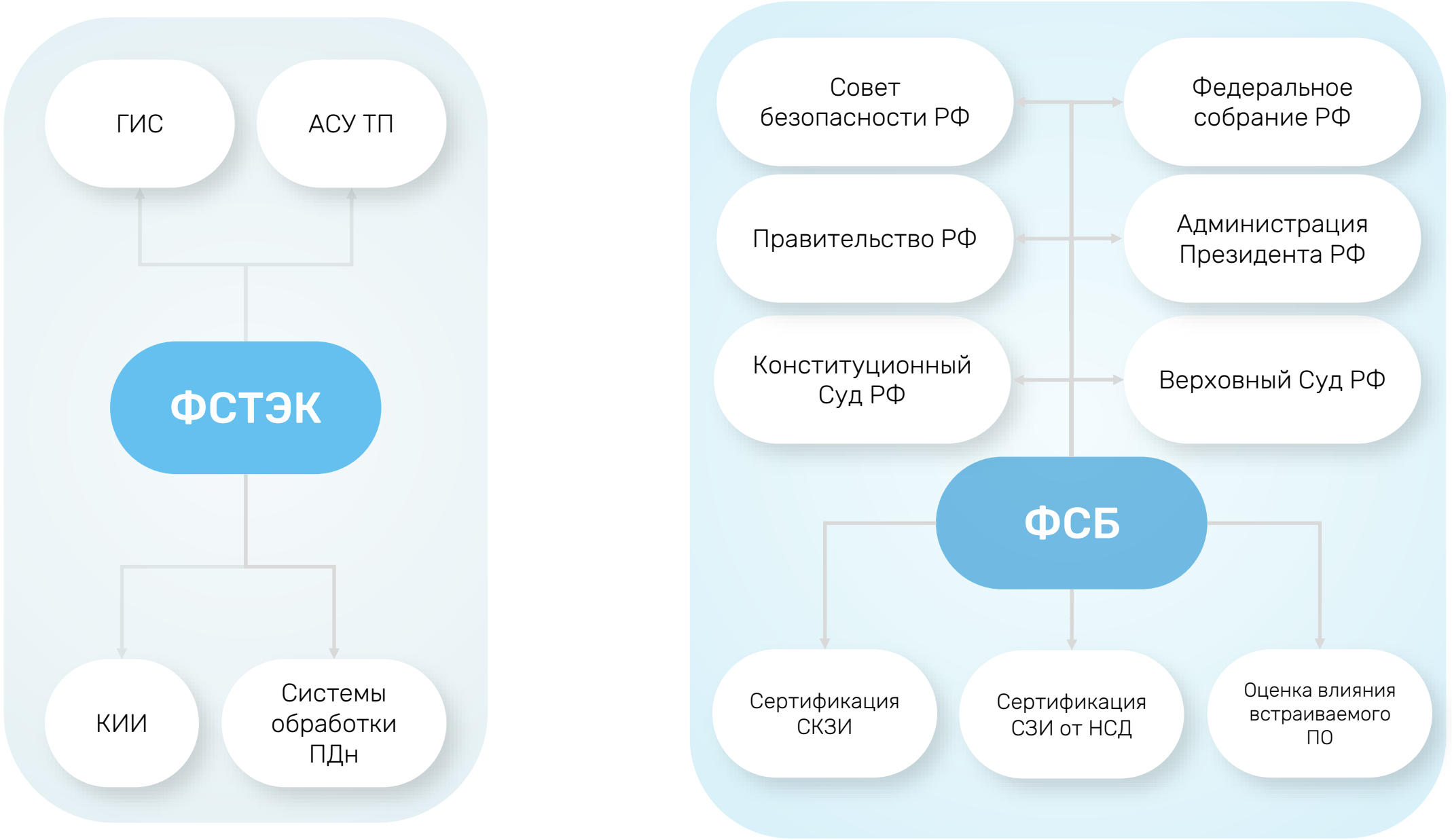
- Прохождение тестирований на проникновение и подтверждение устойчивости продукта к различным атакам, направленным на нарушение ИБ

- Свидетельство о доверии государства такому средству и возможность использования таких СЗИ в различных государственных структурах

Плюсы сертификации

- Подтверждение зрелости и налаженного жизненного цикла продукта, как следствие гарантия защищенности от угроз как существующих, так и потенциальных
- Прогнозируемая политика обновлений продукта
- Защита инвестиций

СИСТЕМЫ СЕРТИФИКАЦИИ В РФ



Сертификация ФСТЭК

- ФСТЭК России выдвигает различные требования к различным типам программного и аппаратного обеспечения. К некоторым типам продуктов (ОС, антивирусы, межсетевые экраны, TEE, и т.д.) требования стандартизированы и называются «профили защиты».

- ПО не подпадающее под профили защиты сертифицируется на соответствие техническим условиям (ТУ). Перечень сертифицируемых функций выбирает разработчик ПО (напр., функции безопасности, аутентификация, разграничение доступа и т.д.)

Сертификация ФСТЭК

- ФСТЭК России приложил много усилий для стандартизации требований к сертифицированным изделиям (в частности, требуется):
  - безопасная разработка
  - работающая линия технической поддержки
  - гарантия отсутствия недекларированных возможностей (НДВ)
  - правила поведения разработчика при обнаружении новых уязвимостей
- Как результат продукт может быть сертифицирован на соответствие одному из уровней доверия (от 1 до 6)

Сертификация ФСТЭК – уровни доверия

Устанавливается 6 уровней доверия. Самый низкий уровень 6–ой, самый высокий 1–ый.
Уровни доверия 1–3 относятся к работе с гос.тайной и выходят за рамки данного вебинара

Уровень доверия	ГИС	ИСПДн	КИИ	АСУ ТП	Классы защиты СЗИ
4	1 класса	1 уровня	1 категории	1 класса	4
5	2 класса	2 уровня	2 категории	2 класса	5
6	3 класса	3 уровня	3 категории	3 класса	6

Государственные информационные системы

- Государственные информационные системы – это федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

- **ФЗ №149 от 27.07.2006 г.** «Об информации, информационных технологиях и о защите информации»
- **Приказ №17 ФСТЭК от 11.02.2013 г.** «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

В ГИС должны использоваться сертифицированные СЗИ, в соответствии с пунктами 11 и 15.1 приказа №17

Информационные системы персональных данных

ИСПДн – это информационная система персональных данных. К персональным относятся общие, биометрические, специальные и обезличенные данные.

- **ФЗ №152 от 27.07.2006 г.** «О персональных данных»
- **Постановление правительства №1119 от 01.11.2012 г.** «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- **Приказ №21 ФСТЭК от 18.02.2013 г.** «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

В ИСПДн должны использоваться сертифицированные СЗИ, в соответствии с пунктом 4 приказа №21.

Классификация информационных систем ПДн

Категории ПДн		Специальные			Биометрические	Иные			Общедоступные		
Собственные работники		Нет	Нет	Да		Нет	Нет	Да	Нет	Нет	да
Количество субъектов		Более 100 тыс.	Менее 100 тыс.			Более 100 тыс.	Менее 100 тыс.		Более 100 тыс.	Мнее 100 тыс.	
		Минимальный уровень доверия для используемых продуктов									
Тип актуальных угроз	1	4	4	4	4	4	5	5	5	5	5
	2	4	5	5	5	5	6	6	5	6	6
	3	5	6	6	6	6	6	6	6	6	6

- угрозы 1-го типа связанны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн
- угрозы 2-го типа связанны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн
- угрозы 3-го типа не связаны с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн

Автоматизированные системы управления технологическими процессами

В частности, регулируется функционирование АСУ ТП на объектах топливно–энергетического комплекса, транспорта, атомной энергетики, гидротехнических сооружениях, опасных производственных объектах и т.д.

- **Приказ №31 ФСТЭК от 14.03.2014 г.** «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

В АСУ ТП **применяются СЗИ, прошедшие оценку соответствия**, в соответствии с пунктом 11 приказа №31

Критическая информационная инфраструктура

К объектам КИИ относятся – информационные системы, информационно–телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

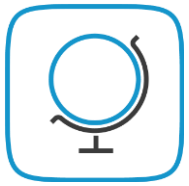
- **ФЗ №187 от 26.07.2017 г.** «О безопасности критической информационной инфраструктуры Российской Федерации»
- **Приказ №235 ФСТЭК от 21.12.2017 г.** «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования»
- **Приказ №239 ФСТЭК от 25.12.2017 г.** «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»

На объектах КИИ должны использоваться сертифицированные СЗИ, в соответствии с пунктами 18 и 28 приказа №235

Субъекты КИИ: На кого распространяется 187-ФЗ?

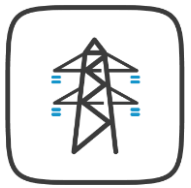
Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (187-ФЗ) распространяется на:


Здравоохранение


Наука

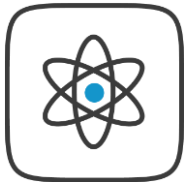

Транспорт


Связь


Энергетика


Финансы


Металлургическая промышленность


Атомная энергетика


Оборонная промышленность


Ракетно-космическая промышленность


Горнодобывающая промышленность


Химия


ТЭК

Как определить принадлежность субъекту к КИИ?

Рекомендуется следующий подход для определения сферы деятельности компании:

- воспользоваться общероссийским классификатором видов экономической деятельности (ОКВЭД) и каталогом организаций России
- определить виды деятельности из лицензий, сертификатов и иных разрешительных документов на виды деятельности
- воспользоваться перечнями видов деятельности из учредительных документов, устава, положения организации

Если хотя бы в одном из приведенных выше документов присутствует указание на упомянутые в №187–ФЗ сферы деятельности, то организация является субъектом КИИ

Категорирование объектов КИИ

Комиссия по категорированию

Перечень объектов подлежащих категорированию

Категорирование объектов КИИ

Акт категорирования объекта КИИ

Направление результатов в ФСТЭК России

Внедрение системы обеспечения безопасности объекта КИИ

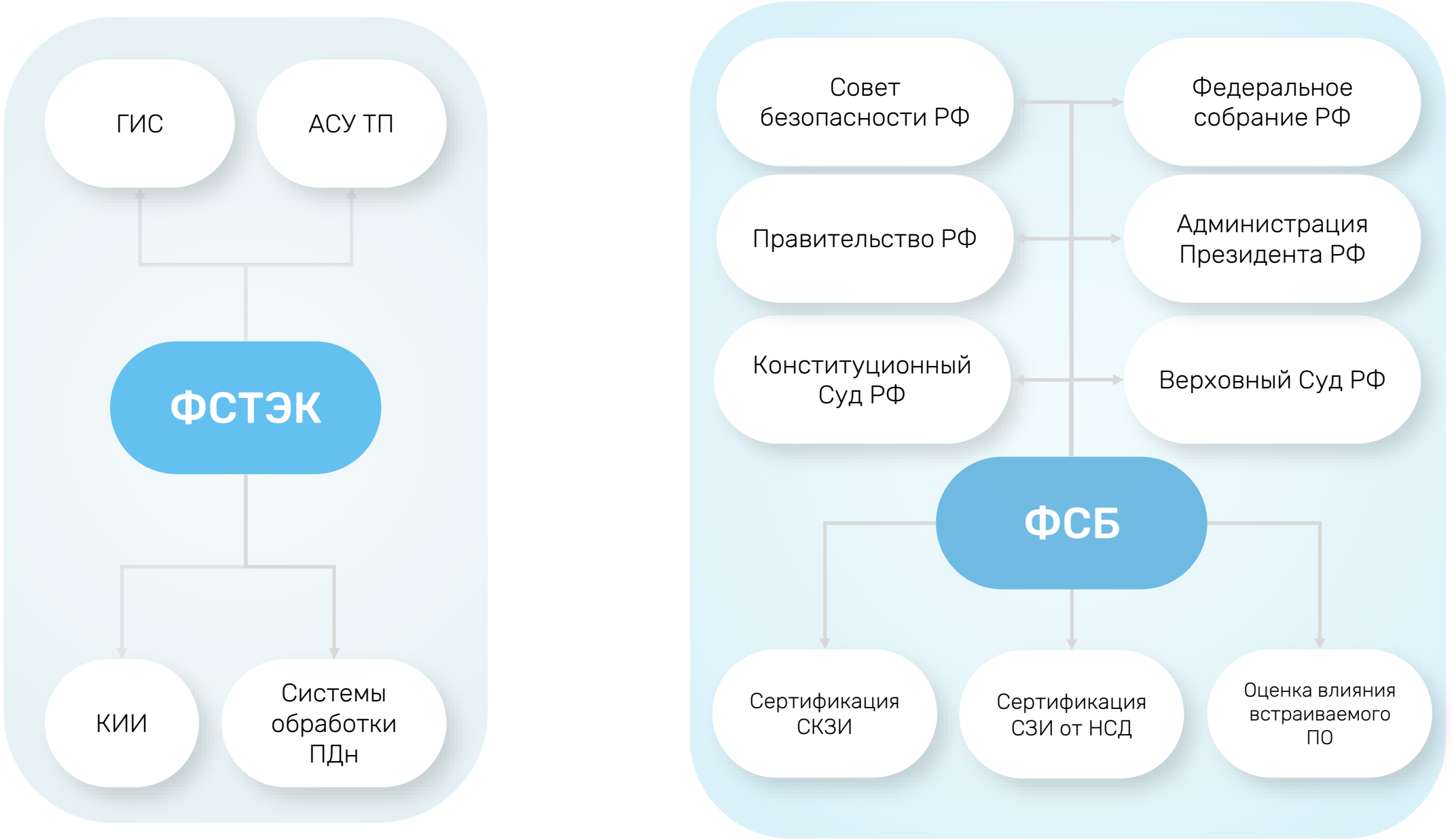
Краткий итог по сертификации ФСТЭК

ОС Аврора и ПО Аврора Центр является программным обеспечением с встроенными механизмами защиты информации от несанкционированного доступа (далее – НСД) и сертифицированы по 4 уровню доверия. Данные продукты могут использоваться:

- В ГИС **1 класса** защищенности и ниже
- На значимых объектах КИИ **1 категории** и ниже
- В АСУ ТП **1 класса** защищенности и ниже
- В ИСПДн при необходимости обеспечения **1 уровня** защищенности и ниже

Таким образом, ОС Аврора и ПО Аврора Центр **могут быть использованы в ИС любого масштаба и значимости инфраструктуры.**

СИСТЕМЫ СЕРТИФИКАЦИИ В РФ



В каких случаях применяется нормативная база ФСБ?

- При необходимости обеспечения безопасности данных с использованием криптосредств
- При обеспечении безопасности обработки данных в ИСах, отнесенных к компетенции ФСБ

При защите информации в ИС, отнесенных к компетенции ФСБ, используются СЗИ сертифицированные по Требованиям ФСБ. Необходимый класс защиты СЗИ устанавливается исходя из возможностей нарушителя:

КС1

Внешний нарушитель, проводит атаки за пределами контролируемой зоны

КС2

Внутренний нарушитель, не имеющий доступа к СКЗИ (прим. уборщица)

КС3

Внутренний нарушитель, имеющий доступ к СКЗИ (пользователь)

КВ

Нарушитель, действующий в интересах группы лиц по предварительному сговору, является пользователем СКЗИ

КА

Иностранная техническая разведка

Сертификация СКЗИ

Основной нормативный документ:

- **ПКЗ–2005** «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»

ОС Аврора имеет сертификат соответствия «Требованиям к средствам защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа» по классу АК2

СКЗИ СледопытSSL имеет сертификат соответствия «Требованиям к СКЗИ» по классу КС2

Продукты компании могут использоваться в ИС, для которых угрозу представляет внутренний нарушитель, не имеющий непосредственного доступа к СКЗИ

СЕРТИФИКАЦИЯ

ОС Аврора:

- Сертификат ФСБ АК2/КС2
- Сертификат ФСТЭК А4/УД4

Платформа управления:

- Сертификат ФСТЭК ТУ+УД4

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4220

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
10 февраля 2020 г.

Выдан: 10 февраля 2020 г. Переоформлен: 28 января 2021 г.
Действителен до: 10 февраля 2025 г.

Настоящий сертификат удостоверяет, что **операционная система Аврора**, разработанная и производимая ООО «Открытая мобильная платформа», является операционной системой, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016), «Профиль защиты операционных систем типа А четвертого класса защиты. ИТ.ОС.А4.ПЗ» (ФСТЭК России, 2017) при выполнении указаний по эксплуатации, приведенных в формуляре АДМГ.10034-02 30 01.

Сертификат выдан на основании технического заключения от 09.12.2019, оформленного по результатам сертификационных испытаний испытательной лабораторией ПФ АО «НТЦ «Атлас» (аттестат аккредитации от 21.11.2017 № СЗИ RU.0001.01БИ00.Б024), экспертного заключения от 30.12.2019, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001), и технических заключений от 10.02.2020, 18.05.2020 и 16.12.2020, оформленных по результатам испытаний испытательной лаборатории ПФ АО «НТЦ «Атлас».

Заявитель: ООО «Открытая мобильная платформа»
Адрес: 420500, Республика Татарстан, Верхнеуслонский район, г. Иннополис, ул. Университетская, д. 7, офис 59
Телефон: (495) 269-0979

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Применение:

- Объекты критической инфраструктуры (ФЗ–187) 1 класса
- Государственные информационные системы 1 класса защищенности
- Информационные системы персональных данных 1 уровня, включая медицинские данные

Заключение

Парадигма «сертификат – это просто бумажка, которую требуют» устарела

Почему сертифицированные решения – это хорошо?

- Вы заказчик, владелец ИС – получаете уверенность, что через непродолжительное время не придётся перестраивать ИС заново
- Вы интегратор – сохраняете репутацию и лояльность заказчиков, клиент не придёт к вам с вопросом «почему ты мне продал что-то, что надо менять?»
- Вы разработчик ПО – выстраиваете жизненный цикл своего продукта, повышаете его качество
- Вы представитель регулирующих органов – спасибо, продолжайте пожалуйста свою работу. Ваша и наша (разработчиков ПО) совместная работа насытит рынок качественными безопасными продуктами.

СПАСИБО!

info@omprussia.ru
m.zubov@omprussia.ru

https://omp.ru
https://auroraos.ru

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА