РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА
10 ЛЕТ

ФЕДЕРАЛЬНАЯ ТЕРРИТОРИЯ «СИРИУС»

24 - 27 сентября 2024

10 лет вместе!

НЕОБХОДИМОСТЬ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ ИТ- ИНФРАСТРУКТУРЫ КАК ОСНОВА РАЗВИТИЯ ОТРАСЛИ

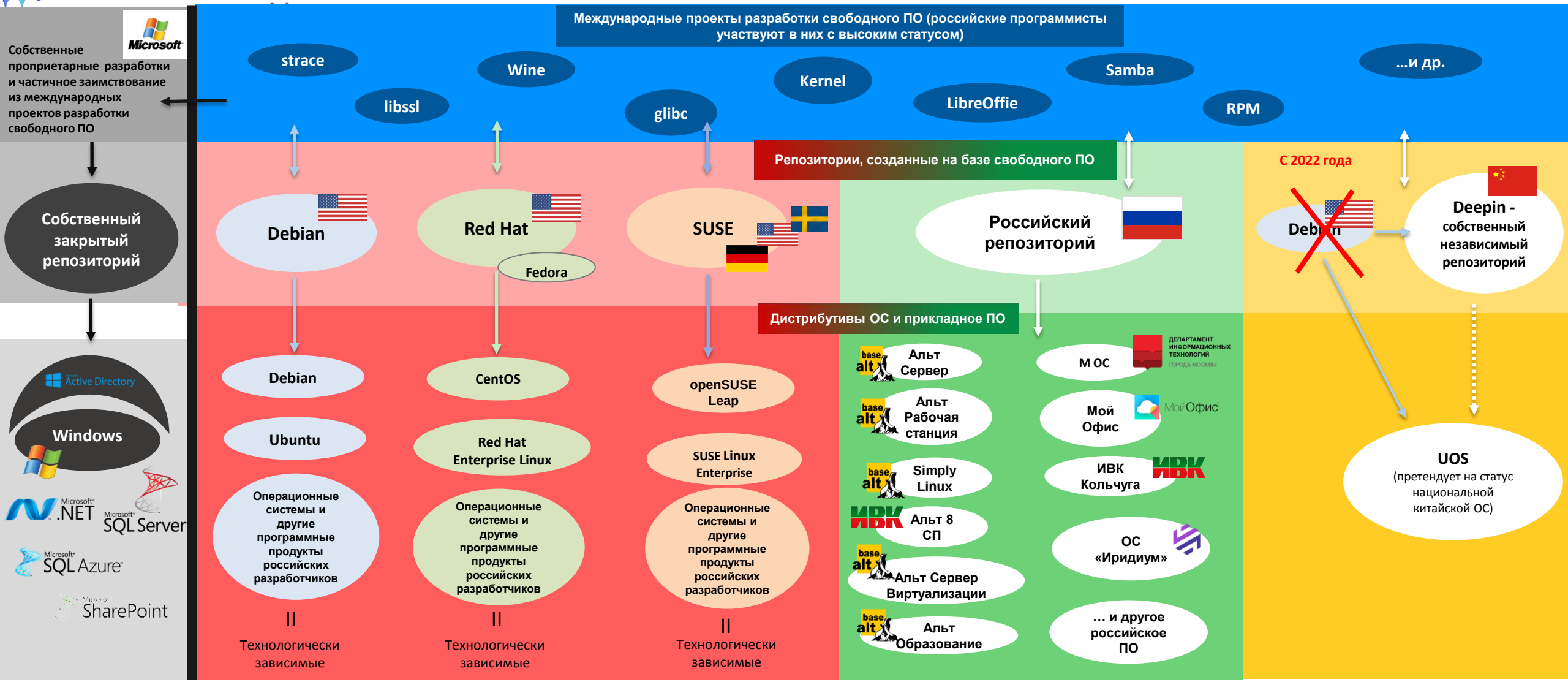
ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

- **В сфере информационных технологий базовой основой технологической независимости являются наличие у государства технологий разработки и производства собственных микропроцессоров и операционных систем.**
- Применительно к микропроцессорам: **технологическая независимость** — это способность государства проводить исследования и разработку архитектуры микропроцессоров и осуществлять проектирование и производство на базе этой архитектуры собственных микропроцессоров.
- Жизненный цикл разработки и интеллектуальные права на архитектуру должны принадлежать Российской Федерации либо российским юридическим лицам и быть локализованы в российской юрисдикции.
- Применительно к инфраструктуре разработки операционных систем (репозиториям) : **технологическая независимость** — это способность государства развить технологии и создать на их основе собственную инфраструктуру разработки, позволяющую управлять проектированием, производством, модернизацией и обеспечением требуемого жизненного цикла системного программного обеспечения для любых целевых процессорных архитектур, находящихся на территории и в юрисдикции Российской Федерации.

ОТЕЧЕСТВЕННЫЙ РЕПОЗИТОРИЙ – ОСНОВА ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ



Windows

Российские технологически зависимые ОС

Российские технологически независимые ОС и прикладное ПО

Китайская технологически независимая ОС

КРУПНЕЙШИЕ В МИРЕ РЕПОЗИТОРИИ СВОБОДНОГО ПО

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

Зарубежные репозитории	Правовая принадлежность	Отечественный репозиторий	Правовая принадлежность
Debian 	Ассоциация разработчиков СПО. Финансирование и юридическая поддержка - фонд Software in the Public Interest (SPI) (зарегистрирован в штате Нью-Йорк, США). Регистрационное свидетельство SPI  Согласно Конституции Debian, SPI – единственная организация, которой доверено хранить собственность и деньги Проекта Debian.	Сизиф «Sysiphus» 	
Red Hat 	Собственник - компания IBM (США). Программные продукты на основе Red Hat регулируются правилами экспортного управления США и другими законами США, и не могут быть экспортированы в страну, охваченную запретительными санкциями		
SuSE 	Собственник - EQT, консультационный фонд по частным инвестициям, основанный Swedish industrial holding (Швеция) и AEA Investors (США). (Штаб-квартира SUSE располагается в Нюрнберге (Германия)		

ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС СОЗДАНИЯ ДИСТРИБУТИВОВ НА РЕПОЗИТОРИИ ПРОГРАММНЫХ ПАКЕТОВ И БИБЛИОТЕК (ФАБРИКИ)



Каждый репозиторий имеет свою уникальную технологию по производству конечного продукта (дистрибутивов) на всех этапах технологического процесса

СЕРТИФИКАТ ФСТЭК ≠ ТЕХНОЛОГИЧЕСКАЯ НЕЗАВИСИМОСТЬ

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

СЕРТИФИКАЦИЯ ФСТЭК НЕРЕДКО ВЫДАЕТСЯ ЗА ТЕХНОЛОГИЧЕСКУЮ НЕЗАВИСИМОСТЬ ПРОГРАММНОГО ПРОДУКТА.

НО ЭТО ПОДМЕНА ПОНЯТИЙ!

СЕРТИФИКАТ ФСТЭК ПОДТВЕРЖДАЕТ ТОЛЬКО БЕЗОПАСНОСТЬ ПРОДУКТА

ПОЛНОМОЧИЯ ФСТЭК РОССИИ

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;
2) противодействия иностранным техническим разведкам на территории Российской Федерации;
3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
5) осуществления экспортного контроля.

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (РБПО)

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

Процессы жизненного цикла Разработки Безопасного Программного Обеспечения (РБПО или Security Development Lifecycle – SDL) должны являться неотъемлемой частью процесса создания и сопровождения разрабатываемых компанией ИТ-продуктов.

Этапы РБПО

Этап	Описание
Анализ угроз и уязвимостей	Определяются потенциальные угрозы и уязвимости, которые могут повлиять на безопасность ПО
Проектирование безопасных систем	Разработка архитектуры и дизайна ПО, которые учитывают безопасность, включая использование безопасных архитектурных шаблонов и принципов, а также механизмов защиты
Разработка безопасного кода	Создание ПО таким образом, чтобы оно было (с определенной долей условности) безопасным, включая соблюдение методик (методологии) РБПО
Тестирование на наличие уязвимостей	Тестирование исходного кода созданного ПО на наличие уязвимостей, включая проведение статического и динамического анализа исходного кода, а также тестирование на проникновение
Развертывание безопасных систем	Внедрение ПО в информационной инфраструктуре. Обеспечение безопасности самой инфраструктуры и данных, а также обучение сотрудников по вопросам безопасности

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (РБПО)

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

Организации (стейкхолдеры) , заинтересованные в создании процессов РБПО (см. табл. 2) .

Стейкхолдер	Чем обосновано?
Разработчики ПО	Пункт 29.3 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25.12.2017 № 239)
Субъекты КИИ	Пункт 29.4 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25.12.2017 № 239)
Владельцы ГИС/МИС	Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. приказом ФСТЭК России от 11.02.2013 № 17)
Организации финансового сектора	Требования Банка России: 382–П, 683–П, 684–П, 719–П
Владельцы ИСПДн	Пункт 11[1] Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. приказом ФСТЭК России от 18.02.2013 № 21)

МЕТОДИЧЕСКАЯ БАЗА ДЛЯ РБПО

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

- ГОСТ Р 50922–2006 Защита информации. Основные термины и определения.
- ГОСТ Р 56939–2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования.
- ГОСТ Р 58412–2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения.
- ГОСТ Р ИСО/МЭК 12207–2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.
- ГОСТ Р ИСО/МЭК 15408–1–2012 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий (1–3 части).
- ГОСТ Р 58412–2019 Разработка безопасного программного обеспечения. угрозы безопасности информации при разработке программного обеспечения.
- ГОСТ Р 58143–2018 Тестирование проникновения.
- ГОСТ Р ИСО/МЭК 18045–2013 Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
- ГОСТ Р 56545–2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.
- ГОСТ Р 56546–2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.
- ГОСТ Р 56939–2016 Разработка безопасного программного обеспечения. общие требования.
- Методические документы ФСТЭК России (по РБПО и управлению уязвимостями).
- Практики РБПО других компаний.

РБПО – это непрерывный процесс. Необходимо регулярно пересматривать и обновлять меры безопасности в соответствии с новыми угрозами и уязвимостями.

Безопасность инфраструктуры и данных является важным аспектом РБПО.

ПРОБЛЕМАТИКА В РЕГУЛИРОВАНИИ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ В СФЕРЕ ИТ

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

- Отсутствие регулятора
- Отсутствие нормативно утвержденных критериев технологической независимости программного обеспечения

ЧТО СДЕЛАНО

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

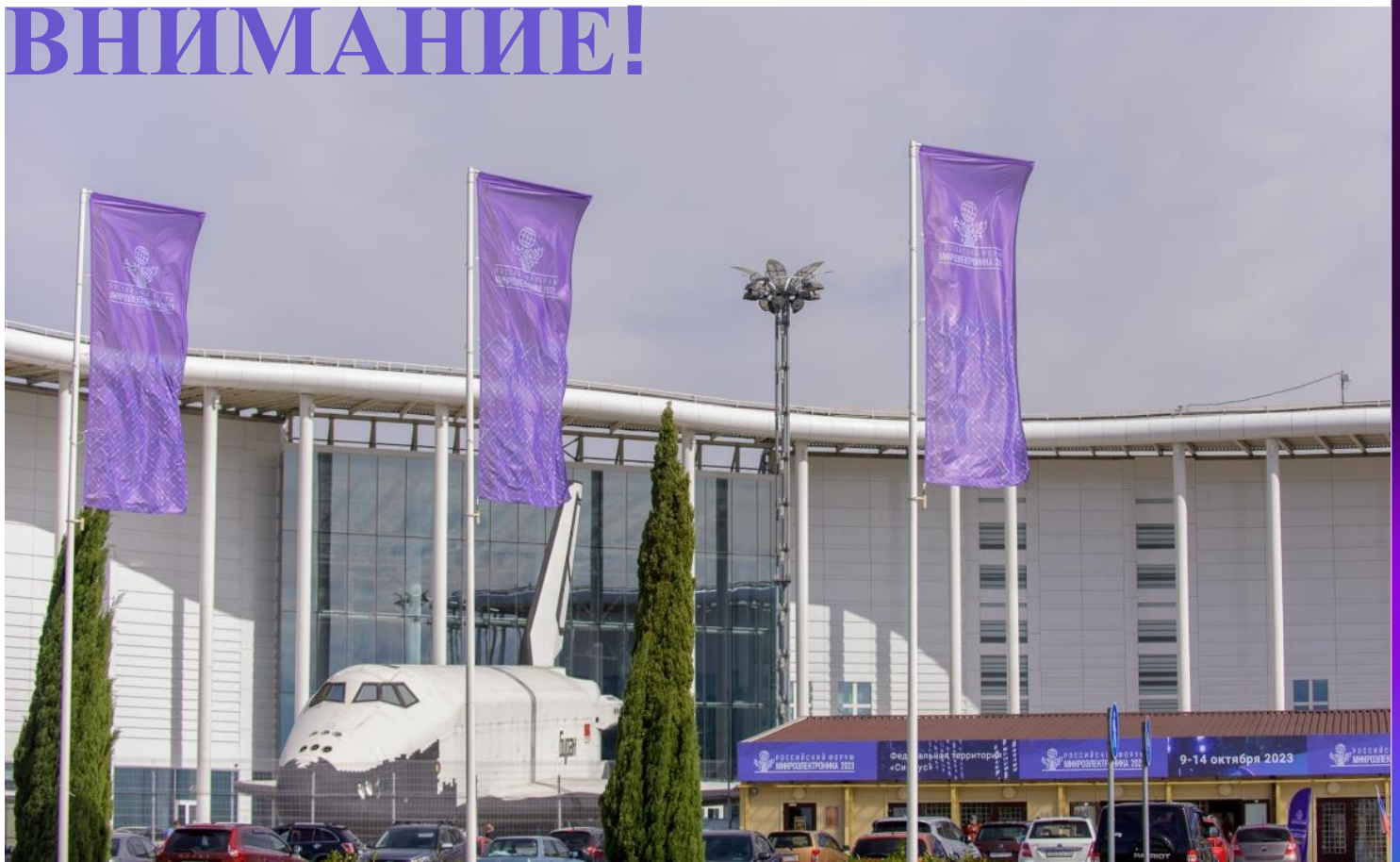
- Указ Президента Российской Федерации №166 от 30 марта 2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».
- Указ «Основы государственной политики РФ в области развития электронной промышленности на период до 2030 года»
- Постановление Правительства №1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно- аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации».
- Готовится национальный стандарт «Инфраструктура информационная критическая. Программное обеспечение для доверенных программно-аппаратных комплексов. Общие положения»

РЕШЕНИЕ ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ В СФЕРЕ ИТ

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2024 10 ЛЕТ

- Создать либо определить полномочия регулятора обеспечения технологической независимости РФ в сфере ИТ.
- Создать межведомственную рабочую группу с участием Минцифры РФ, ФСТЭК РФ, Минпромторга РФ, ФСБ России, основных разработчиков системного ПО и общественных организаций с целью определения критериев технологической независимости репозиториев, на основе которых разрабатываются российские операционные системы.
- Данной рабочей группе - подготовить проект нормативного акта, в котором определить критерии технологической независимости ПО и репозиториев для создания программных продуктов, используемых в КИИ.

СПАСИБО ЗА ВНИМАНИЕ!



РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА
10 ЛЕТ

ФЕДЕРАЛЬНАЯ ТЕРРИТОРИЯ «СИРИУС»

23-28 сентября 2024

microelectronica.pro

@FORUM_MICROELECTRONICA

Подписывайтесь на нас в телеграм-канале и будьте в курсе всех последних новостей!

10 ЛЕТ – КАК ОДИН МИГ

2015 Алушта




2016 Алушта





2017 Алушта





2018 Алушта





2019 Алушта







2020 Ялта



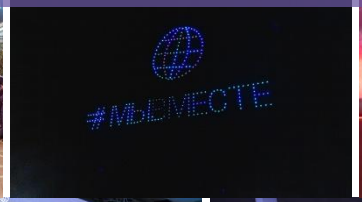


2021 Алушта




2022 Роза Хутор











2023 Федеральная территория « Сириус»





