itsec ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

Отечественные ИТ-платформы и ПО для объектов критической информационной инфраструктуры: готовность предприятий к 1 января 2025 года

Тема: Проблемные вопросы кибербезопасности объектов КИИ предприятий ВПК в условиях санкций и пути их решения

Начальник Управления по противодействию иностранным техническим разведкам и технической защиты информации
АО «Уральский завод гражданской авиации»
Алиев Александр Анатольевич

Влияние санкций иностранных государств на промышленность Российской Федерации в вопросах информационных технологий

Уход крупных поставщиков оборудования и программного обеспечения (ПО) с Российского рынка (Cisco, Siemens, IBM и др.)

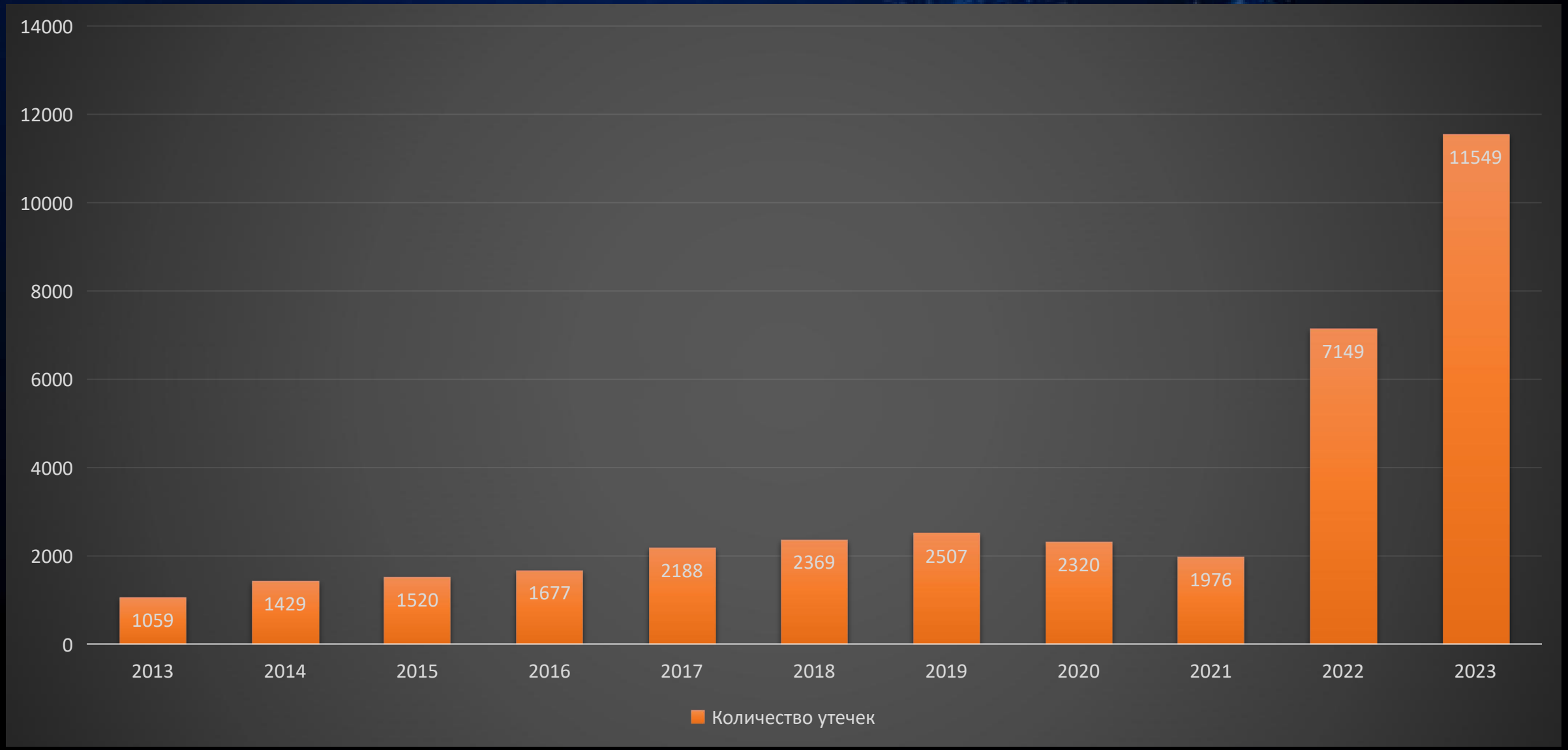
Отключение лицензий и оборудования

Запрет на экспорт услуг в сфере ИТ-консультирования, в результате чего оборудование и ПО из ЕС осталось без технического обслуживания производителей и разработчиков

Отключение функций обновления ПО (накопления «багов» и уязвимостей систем)

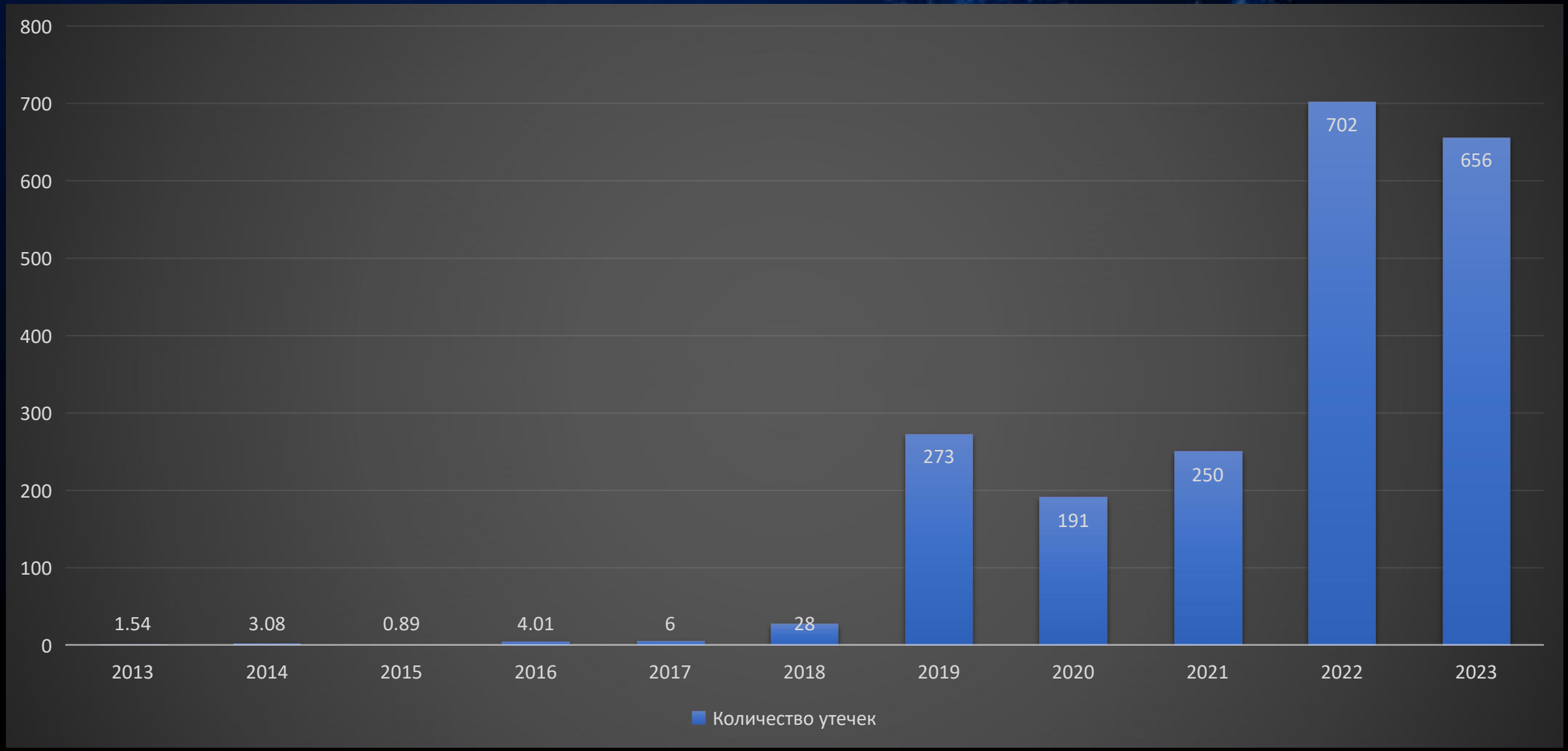
Экспорт отечественных ИТ-продуктов за рубеж

Количество выявленных утечек информации, млн.



Экспертно-аналитический центр ГК InfoWatch (ЭАЦ)

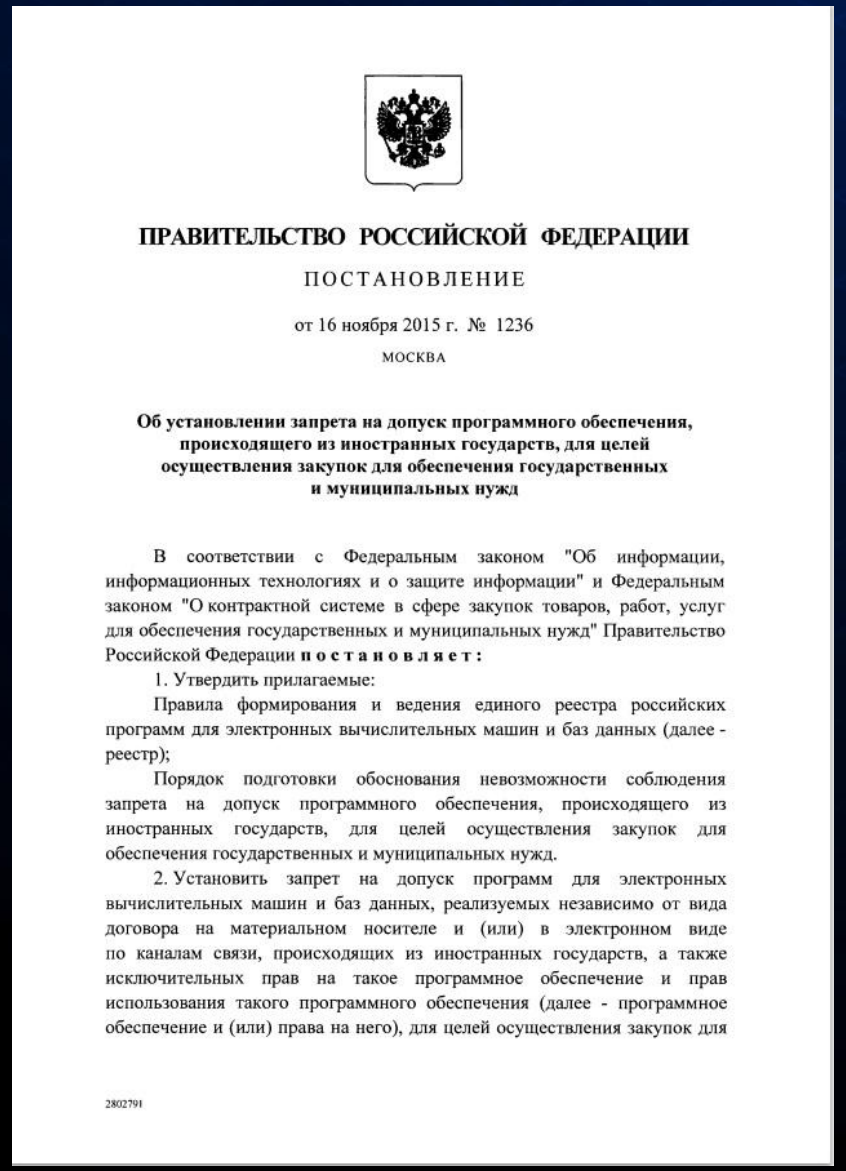
Утекшие записи ПДН, млн.



Экспертно-аналитический центр ГК InfoWatch (ЭАЦ)

Анализ перехода предприятий России на отечественные ПО к 2025 году (ИИМР)

Запрет на допуск импортного ПО для государственных и муниципальных нужд



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 16 ноября 2015 г. № 1236

МОСКВА

Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд

В соответствии с Федеральным законом "Об информации, информационных технологиях и о защите информации" и Федеральным законом "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые:

Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных (далее - реестр);

Порядок подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд.

2. Установить запрет на допуск программ для электронных вычислительных машин и баз данных, реализуемых независимо от вида договора на материальном носителе и (или) в электронном виде по каналам связи, происходящих из иностранных государств, а также исключительных прав на такое программное обеспечение и прав использования такого программного обеспечения (далее - программное обеспечение и (или) права на него), для целей осуществления закупок для

2802791

2. Установить запрет на допуск программ для электронных вычислительных машин и баз данных, реализуемых независимо от вида договора на материальном носителе и (или) в электронном виде по каналам связи, происходящих из иностранных государств (за исключением программного обеспечения, включенного в единый реестр программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации (далее - реестр евразийского программного обеспечения) , а также исключительных прав на такое программное обеспечение и прав использования такого программного обеспечения (далее - программное обеспечение и (или) права на него) , для целей осуществления закупок для обеспечения государственных и муниципальных нужд…

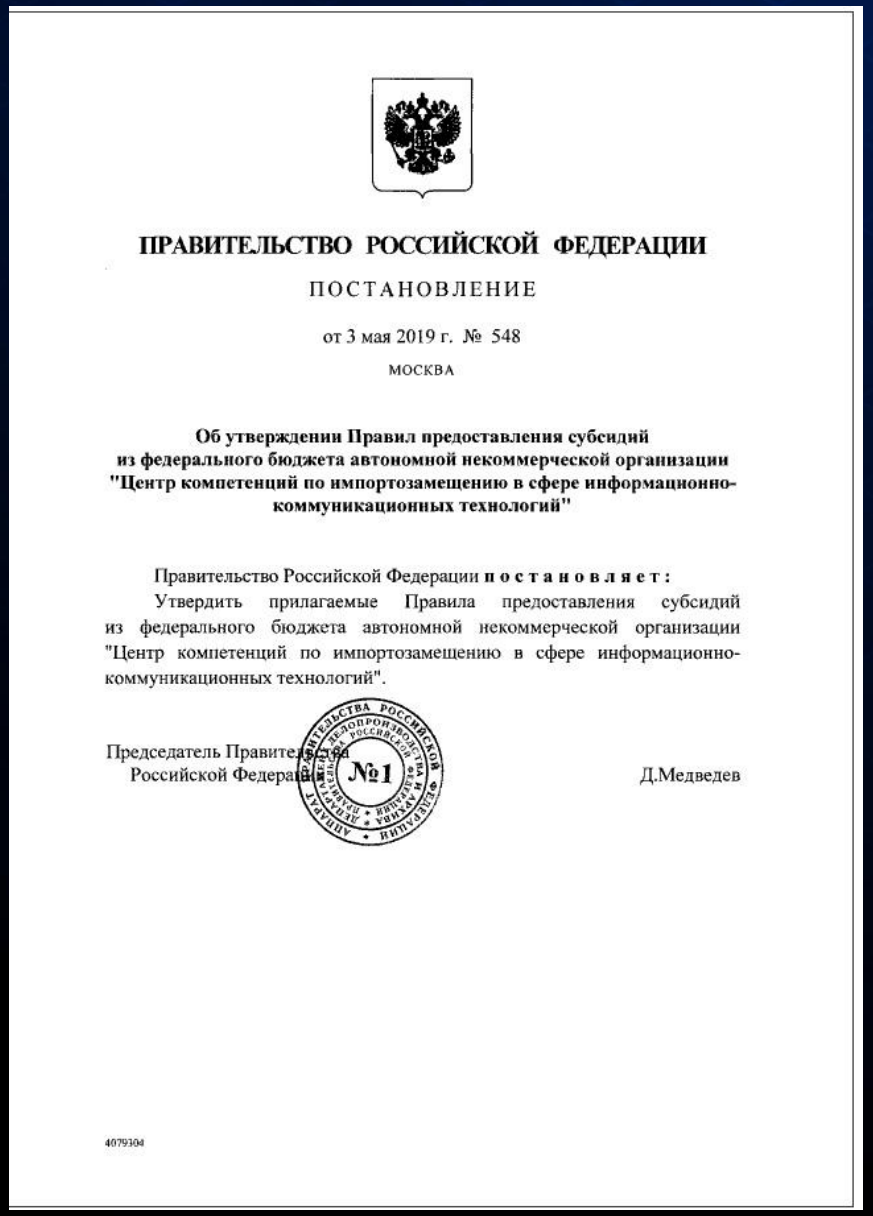
Поручение об обеспечении господдержки по созданию и функционированию центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий (далее – ИКТ)

от 25 мая 2016 года

Обеспечьте необходимую государственную поддержку по созданию и функционированию центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий, определив его правовой статус, полномочия и порядок учёта государственными органами выпускаемых им решений.

При оказании государственной поддержки исходите из необходимости сохранения независимости принимаемых центром решений от субъектов предпринимательской деятельности в сфере информационно-коммуникационных технологий и отраслевых органов государственной власти.

О субсидиях для федерального проекта «Информационная безопасность»



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 3 мая 2019 г. № 548

МОСКВА

Об утверждении Правил предоставления субсидий из федерального бюджета автономной некоммерческой организации "Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий"

Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые Правила предоставления субсидий из федерального бюджета автономной некоммерческой организации "Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий".

Председатель Правительства Российской Федерации Д.Медведев

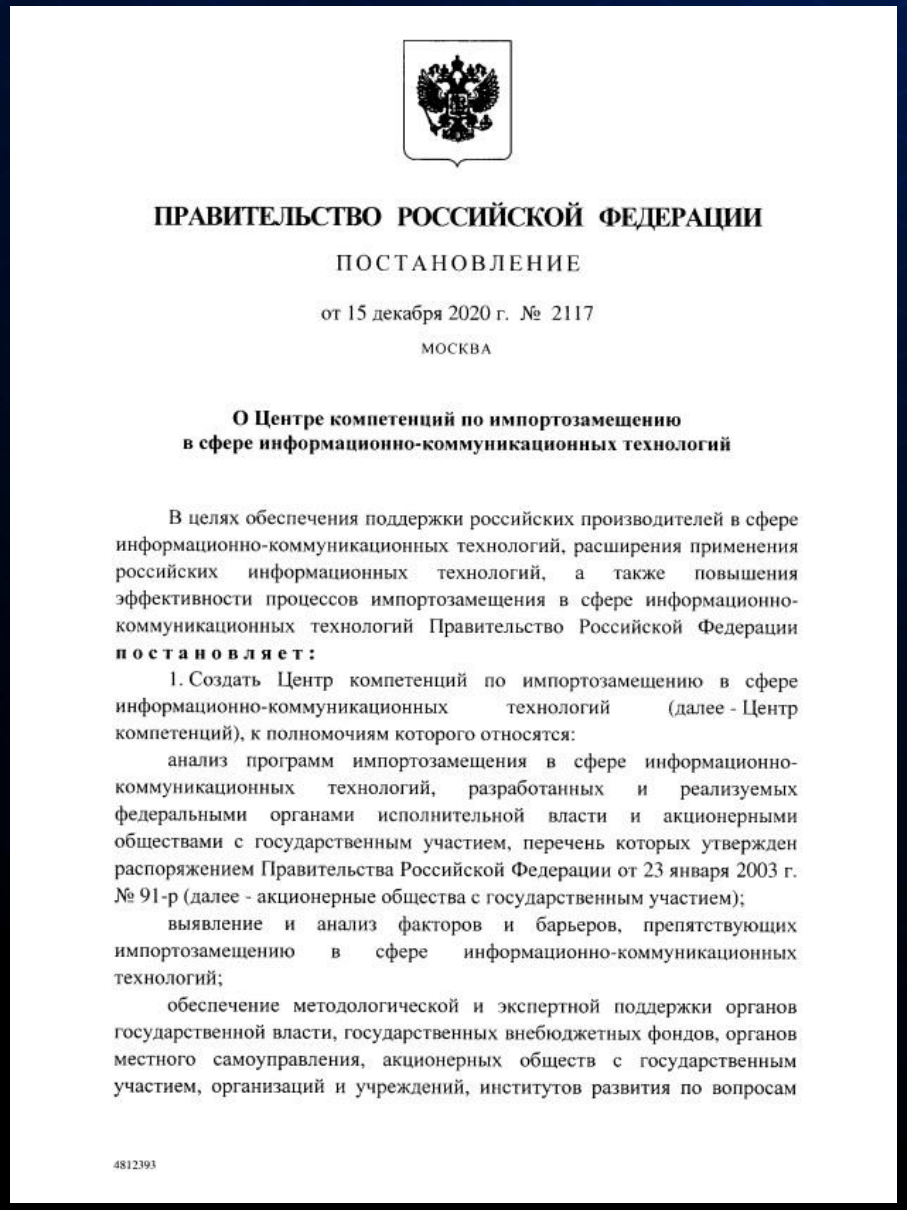
4079304

2. Субсидия предоставляется в целях достижения организацией следующих результатов федерального проекта "Цифровые технологии" национальной программы "Цифровая экономика Российской Федерации":

а) осуществление методологического сопровождения разработки стратегий цифровой трансформации акционерных обществ с государственным участием и мониторинга их реализации, а также оценка мер по импортозамещению в сфере информационно-коммуникационных технологий;

б) осуществление поддерживающих работ, предусмотренных "дорожной картой" развития высокотехнологической области "Новые производственные технологии".

О создании Центра компетенции по импортозамещению в сфере информационно-коммуникационных технологий (далее – Центр компетенций)



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 15 декабря 2020 г. № 2117

МОСКВА

О Центре компетенций по импортозамещению в сфере информационно-коммуникационных технологий

В целях обеспечения поддержки российских производителей в сфере информационно-коммуникационных технологий, расширения применения российских информационных технологий, а также повышения эффективности процессов импортозамещения в сфере информационно-коммуникационных технологий Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Создать Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий (далее - Центр компетенций), к полномочиям которого относятся:

анализ программ импортозамещения в сфере информационно-коммуникационных технологий, разработанных и реализуемых федеральными органами исполнительной власти и акционерными обществами с государственным участием, перечень которых утвержден распоряжением Правительства Российской Федерации от 23 января 2003 г. № 91-р (далее - акционерные общества с государственным участием);

выявление и анализ факторов и барьеров, препятствующих импортозамещению в сфере информационно-коммуникационных технологий;

обеспечение методологической и экспертной поддержки органов государственной власти, государственных внебюджетных фондов, органов местного самоуправления, акционерных обществ с государственным участием, организаций и учреждений, институтов развития по вопросам

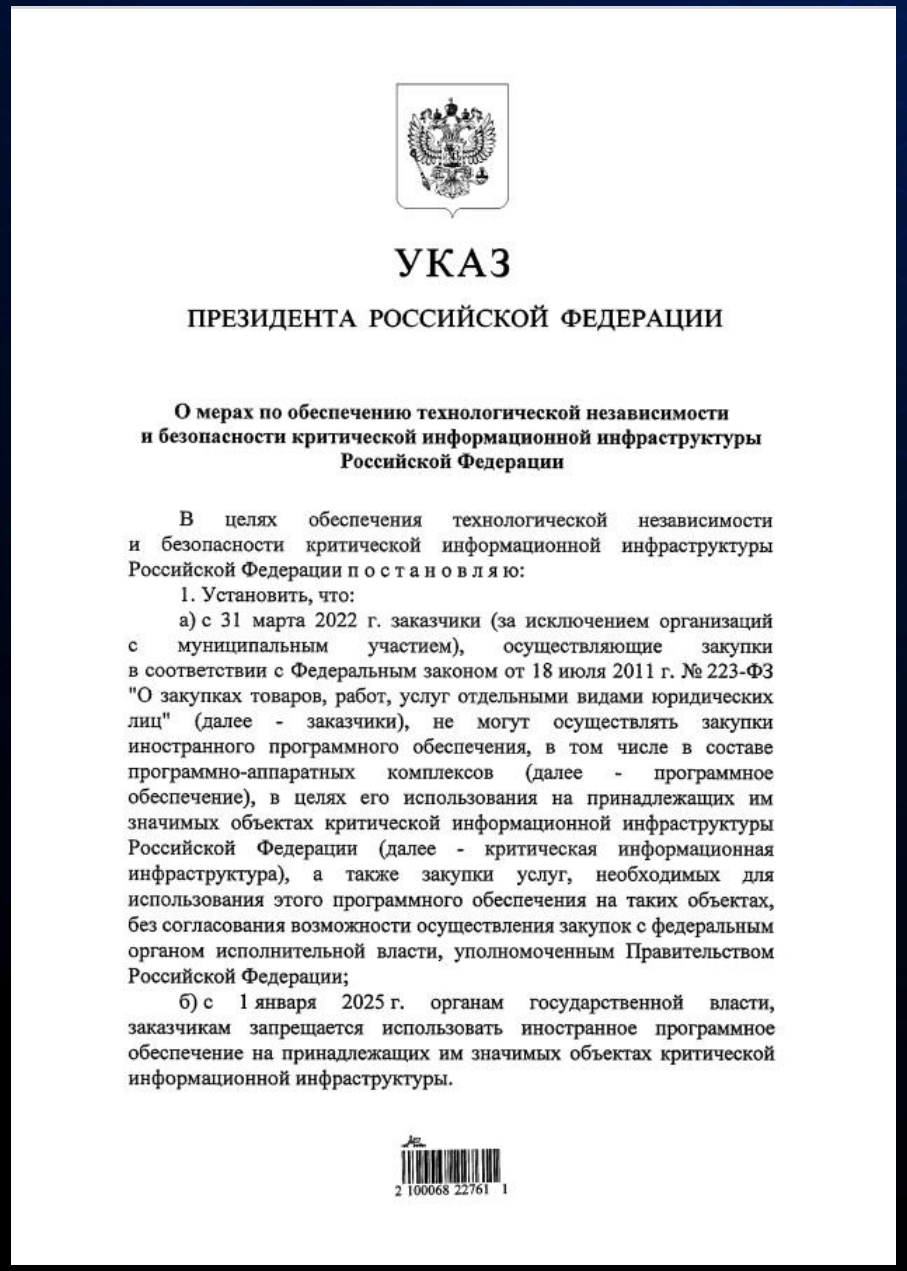
4812393

1. Создать Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий, к полномочиям которого относятся:

а) оценка мер по импортозамещению в сфере информационно-коммуникационных технологий, предусматривающая выполнение следующих работ;

б) осуществление методологического сопровождения разработки стратегий цифровой трансформации акционерных обществ с государственным участием и мониторинга их реализации, предусматривающее выполнение следующих работ.

Запрет на использование иностранного ПО
Указ президента РФ от 30.03.2022 г. №166



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации п о с т а н о в л я ю:

1. Установить, что:

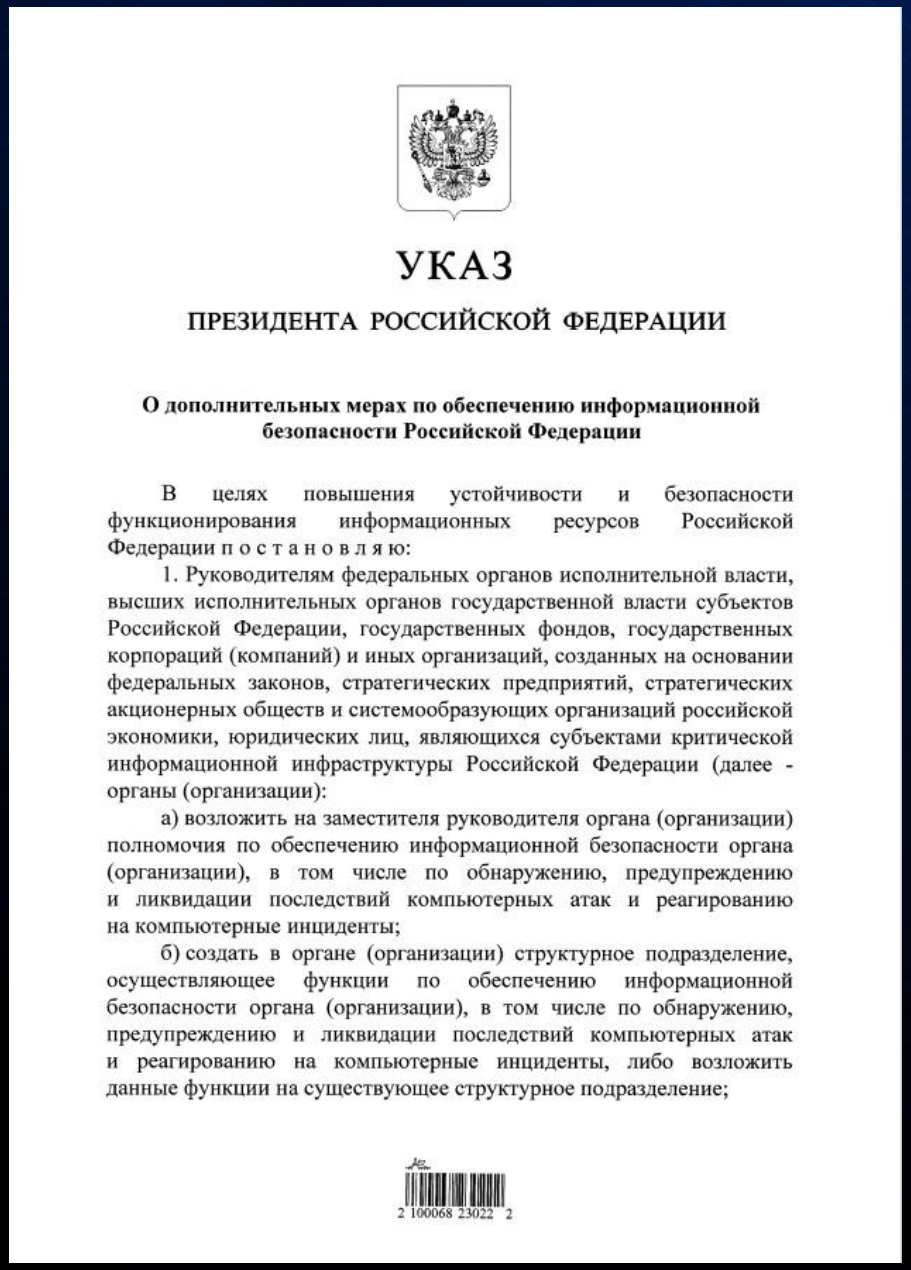
а) с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее - заказчики), не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов (далее - программное обеспечение), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

2 100068 22761 1

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

Запрет на использование средств защиты информации
Указ Президента РФ от 01.05.2022 г. №250



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации п о с т а н о в л я ю:

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

2 100068 23022 2

6 Установить, что с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхож-д е н и я к о т о р ы х я в л я ю т с я и н о с т р а н н ы е государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо п р о и з в о д и т е л я м и к о т о р ы х я в л я ю т с я организации, находящиеся под юрисдикцией таких иностр а н н ы х г о с у д а р с т в, п р я м о и л и к о с в е н н о подконтрольные им либо аффилированные с ними.

Индустриальные Центры компетенций по развитию технологических решений (ЦКР)

16 отраслевых комитетов (машиностроение, самолетостроение, металлургия, электроника и микроэлектроника, связь, образование, транспорт, экология и т.д.)
Основная задача – курирование ИЦК, определение приоритетных направлений, видов, классов замещения ПО и формирования технических заданий для вендеров на разработку конкретных продуктов под потребности Российской промышленности

35 индустриальных Центров компетенции
Бюджет – 37,1 млрд. руб.

Основная задача – обеспечить переход на отечественные технические решения.
В состав ИЦК входят представители отраслевых предприятий, эксперты и вендоры.

Импортозамещение ПО в автоматизации проектирования на базе ИЦК «Беспилотные авиационные системы»

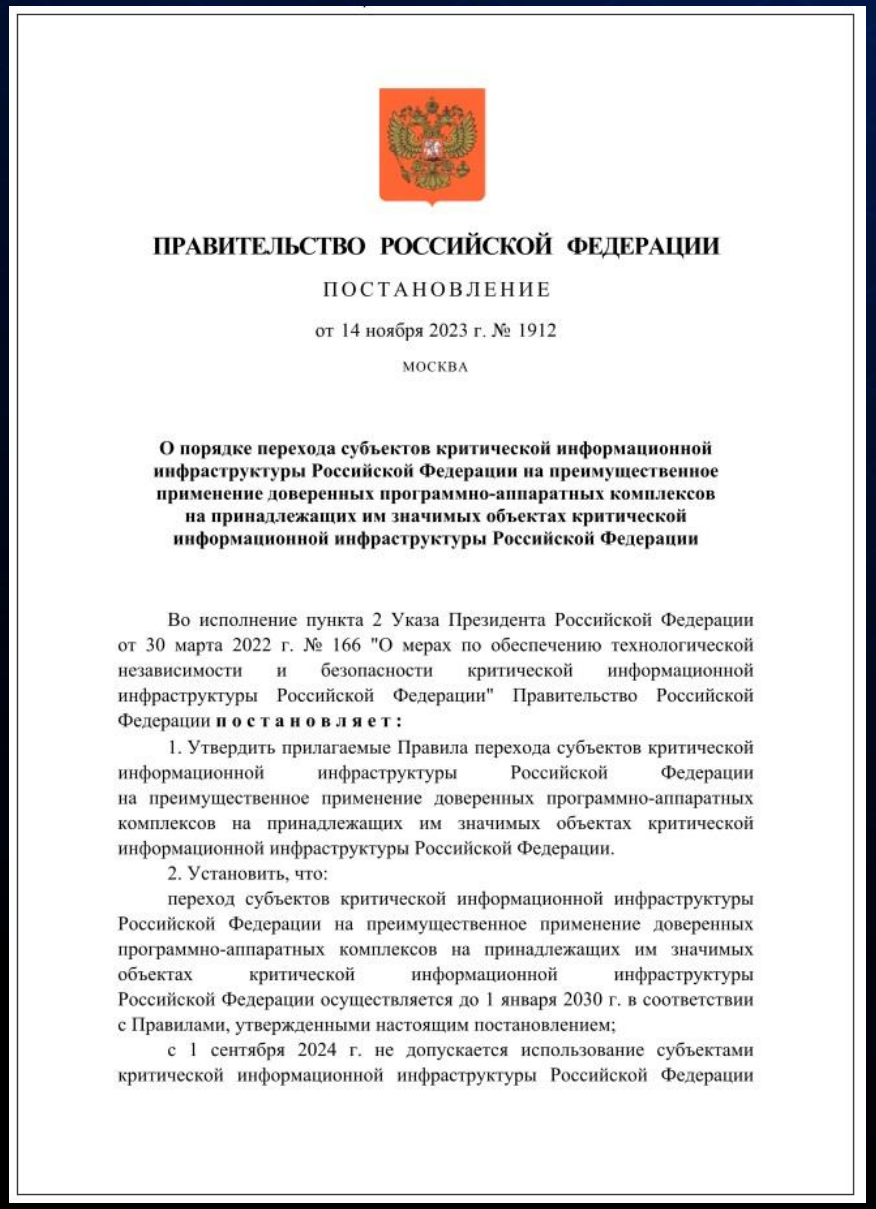
Разработка электронного макета изделия	~~SIEMENS NX~~	T-FLEX CAD, КОМПАС-3D	
Разработка текстовых документов	~~Word~~ ~~Writer~~ ~~Excel~~	МойОфис, Р7-ОФИС	
Управление инженерными данными (PDM)	~~Teamcenter~~	T-FLEX PLM, ЛОЦМАН:PLM, Search	
Разработка чертежей	~~SIEMENS NX~~	T-FLEX CAD 2D+, КОМПАС-График, NANOCAD	
Разработка ЭД ИЭТР	~~Corona3D~~	TG Builder, Seamatica, POWERGUIDE	
Проектирование электросхем	~~E3.series~~	САПР МАКС, dBricks, ElectriCS Pro Авиация	
Проектирование систем управления	~~MATLAB & SIMULINK~~	SimInTech Simulation in technic	
Проектирование Изделий из ПКМ	~~FIBERSIM~~	НЕТ	
Управление требованиями	~~Teamcenter~~	T-FLEX PLM	
Гидрогазо-динамика	~~ANSYS~~ ~~Fine™/Turbo~~	ЛОГОС, FlowVision	
Расчеты на прочность	~~MSC Nastran~~ ~~ANSYS~~ ~~Femap~~	ЛОГОС, T-FLEX Анализ, WinMachine, ИСПА	
Расчет ударов и столкновений	~~LS DYNA~~	НЕТ	
Анализ надежности	~~ANSYS medini analyze~~	Asonika, ПК АРБИТР	
Электромагнитная совместимость	~~ANSYS~~	Asonika	
Аэроупругость	~~MSC Nastran~~	АРГОН (ЦАГИ), IMAD	
1D Проектирование и 3D профилирование турбомашин	~~Concepts NREC EXPERTS IN TURBOMACHINERY~~	TRD Turbo Research & Design	
Оптимизация	FLYPOINT PARAMETRICA	pSeven	
Портал эксплуатанта	OperKit		
Система управления базой данных	~~ORACLE~~ ~~Microsoft SQL Server~~	ЛИНТЕР, POSTGRES PRO, РЕД БАЗА ДАННЫХ	
Операционная система	~~Windows~~	ASTRA LINUX, alt linux, РЕДОС, Циркон	

Импортозамещение ПО. Результаты тестирования отечественного ПО

Обледенение и СКВ	FlowVision	ПО закуплено	
Оптимизация	FLYPOINT PARAMETRICA	ПО закуплено	pSeven — ПО закуплено
Разработка ЭД ИЭТР	TG Builder	ПО закуплено	
Расчет аэроупругости	АРГОН (ЦАГИ) IMAD	ПО закуплено	
Проектирование электросхем	САПР МАКС	ПО закуплено	
Проектирование печатных плат	DeltaDesign	Идет закупка	
Аэродинамика, предварительные расчеты	CADFlo	Тестирование завершено, планируется закупка	
Расчет ударов и столкновений	ЛОГОС	ПО в наличии	
Проектирование Изделий из ПКМ	НЕТ, ждем модуля Компас 3D		
1D Проектирование и 3D профилирование турбомашин	TRD Turbo Research & Design	Тестирование неуспешное	

Управление требованиями	DEVPROM ALM	T-FLEX PLM	Идет тестирование
Аэродинамика точная	FlowVision	Идет тестирование	
Разработка электронного макета изделия	Тестирование неуспешное: КОМПАС-3D	Идет тестирование: T-FLEX CAD	
Управление инженерными данными (PDM)	T-FLEX PLM	Идет тестирование	
Разработка чертежей	T-FLEX CAD	Идет тестирование	
Проектирование систем управления	Тестирование неуспешное: ATLAS Visual Engineering	Планируется тестирование: ENGEE, МДС	
Анализ надежности	Планируется тестирование: Программный комплекс «Надежность»		
Электромагнитная совместимость	НЕТ, ждем модуля ЛОГОС		
Расчеты на прочность	FIDESYS	Тестирование неуспешное	
Расчеты на прочность	ЛОГОС	Тестирование неуспешное	

О порядке перехода субъектов КИИ РФ на преимущественное применение доверенных ПАК на ЗО КИИ РФ с 01.01.2030 г.



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 14 ноября 2023 г. № 1912

МОСКВА

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

Во исполнение пункта 2 Указа Президента Российской Федерации от 30 марта 2022 г. № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые Правила перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации.

2. Установить, что:

переход субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации осуществляется до 1 января 2030 г. в соответствии с Правилами, утвержденными настоящим постановлением;

с 1 сентября 2024 г. не допускается использование субъектами критической информационной инфраструктуры Российской Федерации

2. Установить, что:

- переход субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации осуществляется до 1 января 2030 г. в соответствии с Правилами, утвержденными настоящим постановлением;

- с 1 сентября 2024 г. не допускается использование субъектами критической информационной инфраструктуры Российской Федерации на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации программно-аппаратных комплексов, приобретенных субъектами критической информационной инфраструктуры Российской Федерации с 1 сентября 2024 г. и не являющихся доверенными программно-аппаратными комплексами, за исключением случаев отсутствия произведенных в Российской Федерации доверенных программно-аппаратных комплексов, являющихся аналогами приобретенных субъектами критической информационной инфраструктуры Российской Федерации программно-аппаратных комплексов.

Проблемные вопросы по импортозамещения ПО

Не весь программный продукт Российского производства работает под отечественные операционные системы

Отсутствие достаточного количества профессиональных кадров по информационной безопасности на предприятиях, отвечающих за ЗО КИИ

Слабая компетенция у некоторых заместителей генерального директора (руководителя службы безопасности) в вопросах информационной безопасности, курирующих ЗО КИИ

Не достаточное финансирование на некоторых предприятиях направления ЗО КИИ

Пути решения повышения защищённости критически важных объектов

1. Выполнение на предприятии ВПК требований

Указа Президента РФ от 30 марта 2022 г. №166 «О мерах по обеспечению технической независимости и безопасности критической информационно инфраструктуры РФ» (регулирует использования иностранного программного продукта)

Указа Президента РФ от 1 мая 2022 г. №250 «О дополнительных мерах по обеспечению информационной безопасности РФ» (распределяющее полномочия между государственными структурами по вопросам информационной безопасности и возлагающее полномочия на должностных лиц предприятия по вопросам информационной безопасности)

Постановления Правительства РФ от 15 июля 2022 г. №1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации)» (установление требований наличия профильного образования либо переподготовки по специальности «Информационная безопасность»)

Приказа ФСТЭК России от 21 декабря 2017 г. №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования»

Постановления Правительства РФ от 22 августа 2022 г. №1478 «Об утверждении требований к программному обеспечению…» (определены требования к ПО на значимых объектах КИИ, порядок закупки иностранного ПО и определены правила перехода на отечественное ПО)

2. Введение на предприятиях ВПК Профстандартов

«Специалист по технической защите информации», утвержденного приказом Минтрудсоцзащиты от 9 августа 2022 г. №474н

«Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Минтрудсоцзащиты от 14 сентября 2022 г. №536н

«Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтрудсоцзащиты от 14 сентября 2022 г. №525н

«Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтрудсоцзащиты от 14 сентября 2022 г. №533н

Разработка Российскими предприятиями программных продуктов, в том числе средств защиты информации (программных, аппаратно-программных) в соответствии с требованиями ФСТЭК России, ФСБ России и Минобороны России

Применение на предприятиях ВПК аппаратно-программных комплексов Российского производства и имеющих действующие сертификаты ФСТЭК России и ФСБ России

В соответствии с требованиями ст. 196 ТК РФ отправлять на подготовку или дополнительное профессиональное образование работников, ответственных за защиту информации, но не имеющих соответствующее профильное образование

В соответствии с требованиями Постановления Правительства РФ от 15 июня 2022 г. №1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации)…» на переподготовку по специальности «Информационная безопасность», если таковой у данного должностного лица не имеется

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 15 июля 2022 г. № 1272

МОСКВА

Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)

В соответствии с подпунктом "а" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые:

типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации);

типовое положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации).

Председатель Правительства Российской Федерации

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
5FDFEB8A4E9C5502C6806721EA4CAFFCDFC...
Поставщик: Федеральное казначейство
Правительство Российской Федерации
Действителен с 10.12.2021 по 10.03.2023

М.Мишустин

5724855 (1.10)

(организации) и подчиняется непосредственно руководителю органа (организации) либо должностному лицу, его замещающему.

4. Ответственное лицо входит в состав коллегиальных органов органа (организации).

5. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми государственными служащими, муниципальными служащими и работниками органа (организации).

II. Квалификационные требования к ответственному лицу

6. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), он должен пройти обучение по программе профессиональной переподготовки по направлению "Информационная безопасность".

7. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:

а) основные (в том числе производственные, бизнес и управленческие) процессы органа (организации) и специфика обеспечения информационной безопасности органа (организации);

б) влияние информационных технологий на деятельность органа (организации), в том числе:

роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования органа (организации);

зависимость основных процессов функционирования органа (организации) от информационных технологий;

в) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в органе (организации);

способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее - системы и сети), в том числе ограниченного доступа;

типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

5724855 (1.10)

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27002— 2012

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Свод норм и правил менеджмента информационной безопасности

ISO/IEC 27002:2005
Information technology — Security techniques — Code of practice for information security management (IDT)

Издание официальное

Москва
Стандартинформ
2014

Рекомендация по реализации

Насколько возможно и допустимо с практической точки зрения пакеты программ, поставляемые поставщиком, следует использовать без изменений. Там, где необходимо внести изменения в пакет программ, следует учитывать следующее:

a) риск в отношении встроенных мер и средств контроля и управления и процедур обеспечения целостности;

b) необходимость получения согласия поставщика;

c) возможность получения требуемых изменений от поставщика в качестве стандартной программы обновления;

d) возможные последствия в случае, если организация станет ответственной за будущее сопровождение программного обеспечения в результате внесенных изменений.

Если необходимо внесение изменений, то оригинальное программное обеспечение следует сохранить, а изменения вносить в четко определенную копию. Следует реализовывать процесс управления обновлением программного обеспечения, чтобы иметь уверенность в том, что для всего разрешенного программного обеспечения устанавливаются новейшие одобренные к применению патчи и обновления прикладных программ (см. 12.6). Все изменения необходимо полностью тестировать и документально оформлять таким образом, чтобы их можно было использовать повторно для будущих обновлений программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимой оценочной организацией.

12.5.4 Утечка информации

Мера и средство контроля и управления

Возможность утечки информации должна быть предотвращена.

Рекомендация по реализации

Для снижения риска утечки информации, например по причине использования и эксплуатации скрытых каналов, необходимо принимать во внимание следующее:

a) сканирование носителей исходящей информации и каналов связи на наличие скрытой информации;

b) маскирование и регулирование поведения систем и каналов связи для снижения вероятности того, что третья сторона сможет извлечь информацию из поведения систем и каналов связи;

c) использование систем и программного обеспечения, которые считаются максимально достоверными, например использование оцененных продуктов (см. ИСО/МЭК 15408);

d) регулярный мониторинг деятельности персонала и систем там, где это разрешено существующим законодательством или предписаниями;

e) мониторинг использования ресурсов в компьютерных системах.

Дополнительная информация

Скрытые каналы — это каналы, не предназначенные для передачи информационных потоков, но которые, тем не менее, могут существовать в системе или сети. Например манипулирование битами в пакетах протоколов связи может использоваться как скрытый метод передачи сигналов. Природа скрытых каналов такова, что предотвратить существование всех возможных скрытых каналов затруднительно или даже невозможно. Однако такие каналы часто используются «троянскими» программами (см. 10.4.1). Следовательно, принятие мер по защите от «троянских» программ снижает риск использования скрытых каналов.

Предотвращение неавторизованного доступа к сети (см. 11.4), а также политики и процедуры, препятствующие неправильному использованию информационных услуг персоналом (см. 15.1.5), способствуют защите от скрытых каналов.

12.5.5 Аутсорсинг разработки программного обеспечения

Мера и средство контроля и управления

Аутсорсинг разработки программного обеспечения должен быть под наблюдением и контролем организации.

Рекомендации по реализации

Благодарю за внимание!