Безопасность после импортозамещения: какие риски создаёт переход на отечественный стек

CNews Forum 2026, секция "Импортозамещение", 12 ноября 2026 года

Николай Лобанов

Независимый эксперт по информационной безопасности и защите КИИ

О чём доклад

Импортозамещение не убирает риски, а меняет их состав

1. Где при переходе появляются новые слабые места
2. Что меняют акты 2026 года для КИИ, государственных систем и поставщиков ПО
3. Что ИТ-директору сделать сейчас, не дожидаясь требований

Откуда опыт

С 2021 по 2024 год отвечал за техническую политику замены серверного парка и перевода систем на отечественные операционные системы в центральном депозитарии финансового рынка. Это инфраструктура, которую нельзя остановить на время переезда.

В 2026 году подаю замечания к проектам актов ФСТЭК России и Минцифры России на regulation.gov.ru.

Практика

Пять слабых мест перехода

1	**Повторное тестирование прикладного слоя**	После смены ОС, СУБД или виртуализации заново проверяется всё, что на них работает, включая настройки защиты
2	**Зрелость поддержки нового вендора**	Опыта поддержки именно вашей конфигурации и нагрузки у него может быть мало
3	**Скорость выпуска обновлений безопасности**	Сколько дней проходит от публикации уязвимости до исправления у вендора и до установки у вас
4	**Зависимость от единственного поставщика**	Если на весь контур одна платформа, её ошибка или уход вендора затрагивает все системы сразу
5	**Технический долг ускоренной миграции**	Временные решения и отложенные настройки защиты остаются после переезда

Практика

Что с этим делать

1 Тестирование	Повторные испытания и пересмотр настроек защиты после каждой смены платформы
2 Поддержка	Сроки реакции поддержки и устранения уязвимостей в договоре
3 Обновления	Счёт дней от бюллетеня вендора до установки исправления у себя
4 Один поставщик	Карта зависимостей и сценарий на случай отказа платформы
5 Долг миграции	Реестр временных решений с ответственным и сроком закрытия

Что уже принято

Акт	О чём	Вступает в силу
ПП РФ от 18.08.2026 № 1024	Как государственные системы используют облачные техсредства, программы и базы данных	**с 01.09.2026**
Приказ Минцифры России от 31.07.2026 № 702	Требования о защите информации при предоставлении вычислительной мощности операторам государственных и муниципальных систем	**с 01.03.2027**
Приказ ФСТЭК России от 16.07.2026 № 220	Значимые объекты КИИ: показатель защищённости Кзи не реже раза в 6 месяцев, показатель уровня зрелости Узи не реже раза в 3 года; субъект КИИ требует Узи от подрядчика до доступа	**с 01.03.2027**
Приказ ФСТЭК России от 08.05.2026 № 137	Государственные системы, Требования № 117: показатель уровня зрелости Пзи стал Узи; с 01.03.2027 его считает подрядчик до доступа и не реже раза в 2 года	**с 01.09.2026; п. 32 с 01.03.2027**

Реквизиты сверены по официальному опубликованию, publication.pravo.gov.ru, 26.10.2026

Что ещё в проектах

Доверенные ПАК

Действует ПП № 1912 о переходе субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов на значимых объектах.

Проект Минпромторга 160786: с 1 января 2030 года недоверенные ПАК на значимых объектах не допускаются, кроме четырёх случаев и при условии мер защиты по решениям ФСБ России и ФСТЭК России. На 26.10.2026 не принят.

Доверенное ПО

Проект Минцифры 171820, требования к информационной безопасности доверенного ПО:

- нет неустранённых (необработанных) уязвимостей из банка данных угроз ФСТЭК, устранение в порядке и сроки ФСТЭК
- обновления только с разрешения пользователя, в том числе через лицензионное соглашение, и не через средства за пределами России или их копии
- перечень компонентов по запросу пользователя

Мои замечания к проекту поданы 14.10.2026.

Если проект примут, устранение уязвимостей станет условием включения ПО в перечень доверенного. Установить исправление у себя по-прежнему придётся вам.

Два вопроса из моих замечаний

1 Облако для государственных систем, проект 170797

Я предложил записать в требованиях к платформе показатели доступности и время восстановления, содержание услуги резервного копирования и информирование потребителя.

Минцифры ответило, что разрыва ответственности нет и требования ФСТЭК к восстановлению, резервному копированию и взаимодействию с ГосСОПКА оператор может исполнять силами поставщика. Предложение частично учтено, доработанного текста нет.

На мой взгляд, отвечает оператор, а средства исполнения у поставщика. Без показателей в требованиях к платформе оператору нечего с него спросить.

2 Уязвимости доверенного ПО, проект 171820

Что такое необработанная уязвимость, проект не определяет, а сроки устранения отсылает к порядку ФСТЭК, не называя акта.

Я предложил определить термин и назвать акт.

Вывод на обсуждение

Считать критическую инфраструктуру защищённой рано

Пока DNS, внешний хостинг и облачные сервисы без доступа к значимому объекту остаются вне требований к его защите

- С 01.03.2027 по приказу № 220 подрядчик с доступом к значимому объекту, в том числе для обработки и хранения информации, считает Узи до получения доступа
- Если при переходе системы переехали в облако или к подрядчику, обязанности по защите значимого объекта остались у вас
- ПП № 1024 об облачных ресурсах касается государственных систем, приказ № 702 о вычислительной мощности также муниципальных

Что сделать сейчас, не дожидаясь требований

1. Провести инвентаризацию внешних зависимостей: облака, DNS, хостинг, каналы, площадки подрядчиков
2. Записать в договор с провайдером уведомление об инцидентах, сроки устранения уязвимостей и условия выхода
3. Подготовить сценарий работы при недоступности внешнего сервиса
4. Запросить у поставщика ПО перечень компонентов и срок исправления уязвимостей
5. Завести реестр временных решений миграции с ответственным и сроком

Спасибо. Вопросы

Николай Лобанов

Независимый эксперт по информационной безопасности и защите КИИ

Сайт	**nikolay-lobanov.ru**
Канал "На стадии обсуждения"	**t.me/na_stadii, max.ru/channel_na_stadii**
Почта	**nlobanov-25@ranepa.ru**

Замечания к проектам 171820 и 170797 пришлю по запросу.