Методология формирования доверенной информационной среды Союзного государства в условиях технологической зависимости

Исаев Владислав Олегович, к.т.н.

Блинков Юрий Владимирович

Оперативно-аналитический центр при Президенте Республики Беларусь

Актуальность проблемы

КЛЮЧЕВЫЕ ВЫЗОВЫ

Технологическая независимость
и информационная безопасность приобретают решающее значение.

Рост сложности
информационных систем и их зависимость от внешних поставщиков.

Необходим контроль
над критически значимыми технологиями, от которых зависит устойчивость системы.

Особая актуальность
для интеграции информационных систем Беларуси и России.

Цель работы

Формирование нового методологического подхода к оценке доверенности информационной среды

Учет технологической зависимости

Рассматривать зависимость от зарубежных поставщиков как самостоятельный, обособленный класс рисков, а не просто как одну из уязвимостей.

Создание согласованных критериев

Разработать критерии оценки, которые можно использовать в правовых системах обоих государств без необходимости полной унификации национальных законов.

Нормативно-правовая база: Республика Беларусь

1

Концепция цифрового развития до 2030 года

Заложила основы цифрового суверенитета.

2

Указ Президента № 40 «О кибербезопасности»

Определяет архитектуру кибербезопасности и принцип непрерывного мониторинга.

3

Указ Президента № 196 (под координацией ОАЦ)

Отвечает за категорирование критически важных объектов информатизации.

4

Закон «Об информации, информатизации и защите информации»

Прописывает базовые правила работы с данными.

Нормативно-правовая база: Российская Федерация

1

Федеральный закон № 187-ФЗ «О безопасности КИИ»

Определяет обязанности субъектов критической информационной инфраструктуры.

2

Система ГосСОПКА

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3

Приказ ФСТЭК России № 117

Устанавливает требования по защите информации в государственных информационных системах (ИС).

4

ГОСТ Р 56939-2024 «Разработка безопасного ПО»

Регламентирует этапы безопасной разработки программного обеспечения.

Общая основа: Гармонизация и стандарты

Глубинная гармонизация

Правовые конструкции в Беларуси и России имеют схожее функциональное назначение. Понятия «критически важный объект информатизации» (РБ) и «значимый объект КИИ» (РФ) преследуют одну цель — выделить системы, сбой в которых нанесет ущерб национальным интересам.

Опора на стандарты

Методология полностью базируется на действующих в обоих государствах стандартах менеджмента рисков: сериях СТБ ISO/IEC 27001, 27002, 27005 в Беларуси и аналогичных стандартах ГОСТ Р ИСО/МЭК в России.

Что такое «доверенная информационная среда»?

Мы предлагаем определить её как совокупность всех компонентов — от «железа» до организационных процедур, — где мы можем гарантировать и подтверждать выполнение требований безопасности на протяжении всего жизненного цикла.

Важный тезис: доверенность не равна происхождению продукта.

Контролируемость

Прозрачность и управляемость всего жизненного цикла компонента.

Прозрачность

Понимание всех технологических зависимостей компонента.

Проверяемость

Возможность верифицировать заявленные свойства и функции.

Целостность

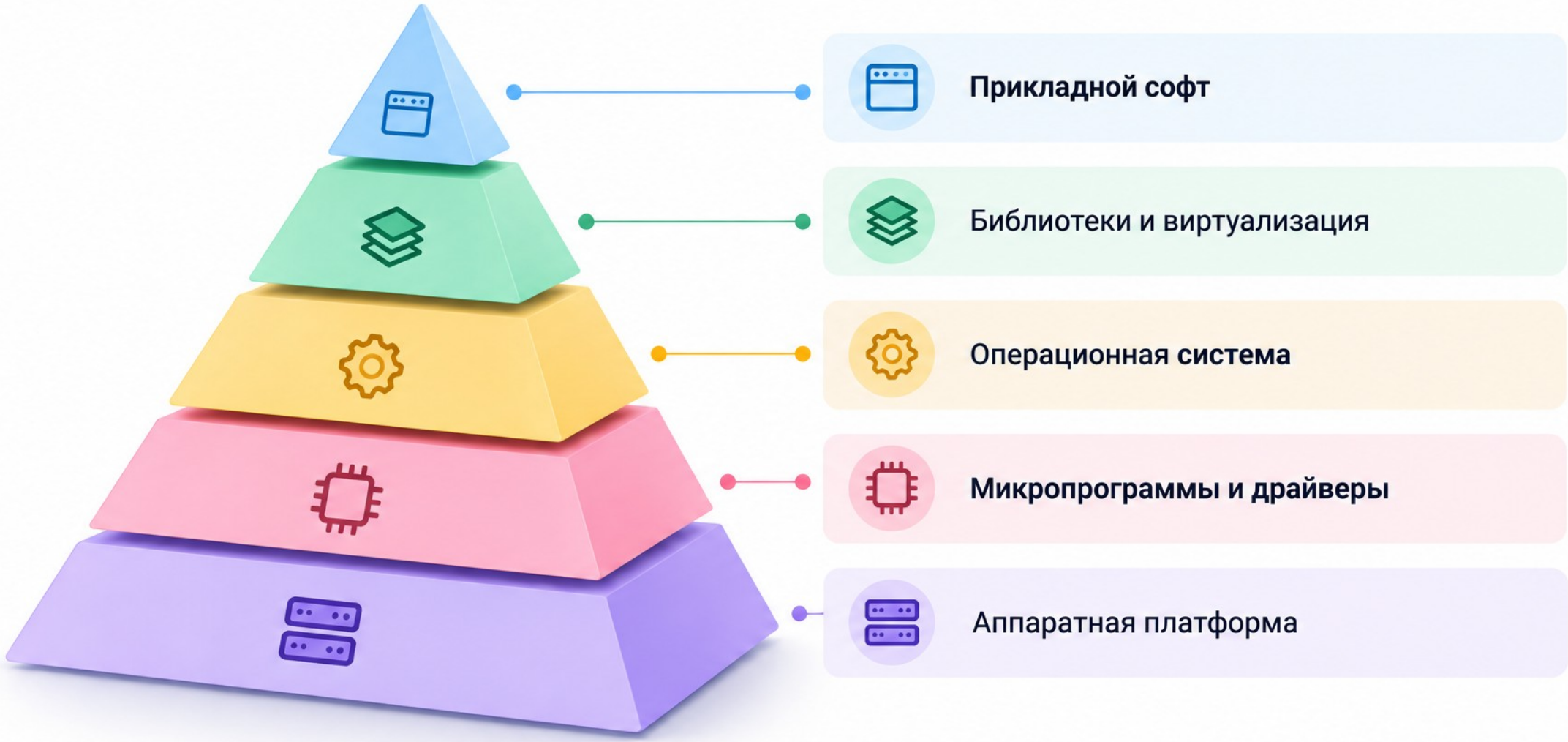
Гарантия неизменности компонента от разработки до эксплуатации.

Восстанавливаемость

Способность системы к восстановлению после сбоя или атаки.

Архитектура зависимостей и риски

Современная информационная система — это «слоеный пирог». Из-за тесных технологических связей компрометация любого низкоуровневого элемента каскадом обрушивает безопасность всего, что находится выше.



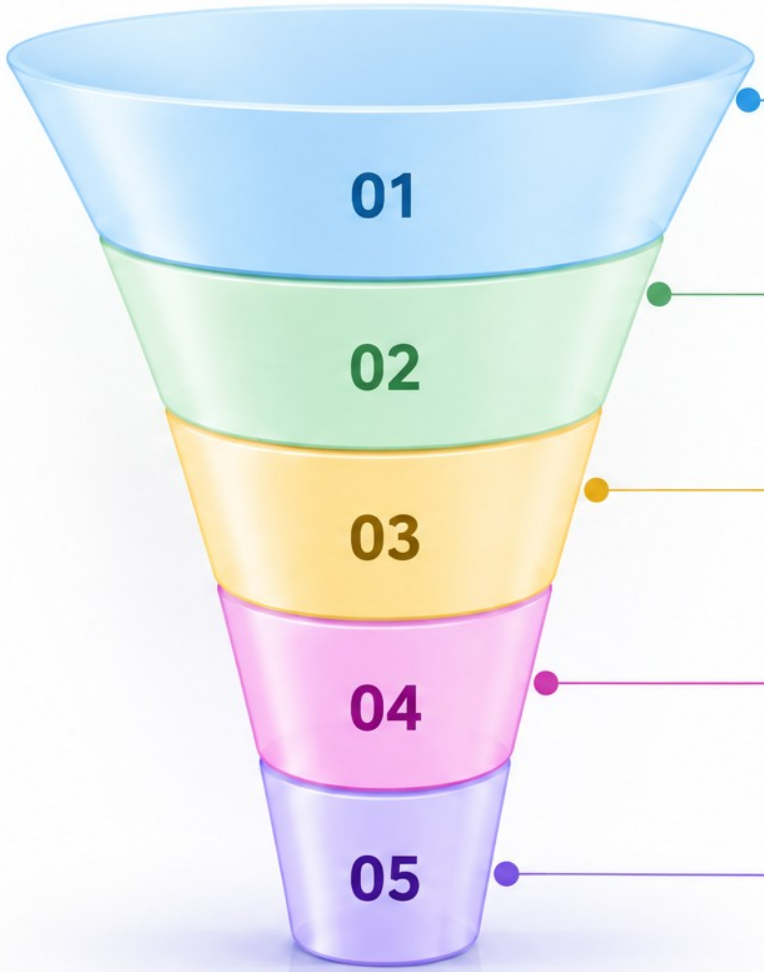
Технологическая зависимость как самостоятельный фактор риска

Мы призываем рассматривать технологическую зависимость как самостоятельный фактор риска, который шире привычной триады «угроза — уязвимость».

Если компонент критичен для работы, но его невозможно оперативно заменить или проверить, риск максимален, даже если в нем нет известных уязвимостей.

Смысл импортозамещения — не в механической замене софта «один в один», а в ликвидации неконтролируемых единых точек отказа.

Методология оценки: 5 последовательных шагов



01 Инвентаризация компонентов и их связей

02 Оценка критичности компонентов

03 Оценка уровня технологической зависимости

04 Расчет доверенности для каждого компонента

05 Расчет интегрального показателя доверенности всей среды

Математическая модель: Оценка компонента и среды

Доверенность компонента (Ti)

$$Ti = w_1C_i + w_2V_i + w_3I_i + w_4R_i - w_5D_i$$

C — Контролируемость

V — Проверяемость

I — Целостность

R — Восстанавливаемость

D — Технологическая зависимость (штраф)

w — Весовые коэффициенты

Доверенность среды (Tсреды)

$$T_{среды} = 0, \text{ если } \exists i \in K_{крит}: (X_i < X_{min}) \vee (D_i > D_{max});$$

$$\text{иначе } T_{среды} = \sum \alpha_i T_i.$$

Ключевое нововведение

Логическая функция-отсекатель. Если хотя бы один критический компонент проваливается ниже порога, интегральная оценка всей среды падает до нуля. Это исключает маскировку «дыры» в важном элементе за счет высоких показателей второстепенных программ.

Пример расчета на гипотетической системе

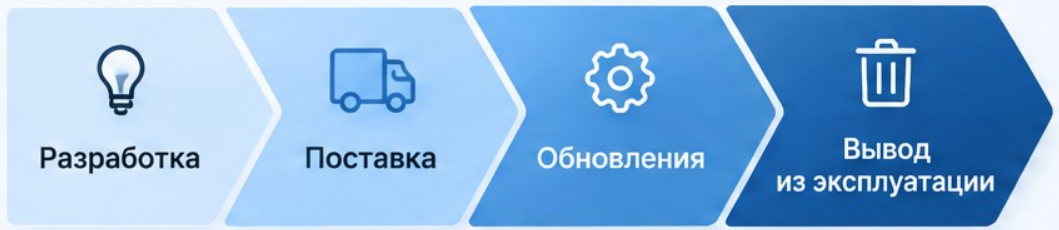
Пороговые значения: **Xmin = 0.5, Dmax = 0.6**. В примере параметр целостности (Ii) для ОС упал до 0.3, что ниже порога. Традиционный метод усреднения скрыл бы проблему, но наша модель за счет функции-отсекателя мгновенно маркирует всю среду как неприемлемую.

Компонент	Критичность	C_i	V_i	I_i	R_i	D_i	T_i	Статус
1. Ядро СУБД	Критический	0.8	0.7	0.9	0.8	0.2	0.74	Норма
2. ОС	Критический	0.6	0.5	0.3	0.7	0.1	0.50	Крит. провал (I_2 < Xmin)
3. Веб-интерфейс	Некритический	0.7	0.6	0.8	0.7	0.8	0.46	Норма

Контроль цепочек поставок и непрерывность

Контроль жизненного цикла

Доверенность нельзя оценить один раз при покупке. Продукт должен контролироваться на всех этапах: от разработки и безопасной поставки до обновлений и вывода из эксплуатации. Показатель проверяемости увязан с требованиями к стадиям разработки ПО (ГОСТ Р 56939-2024).



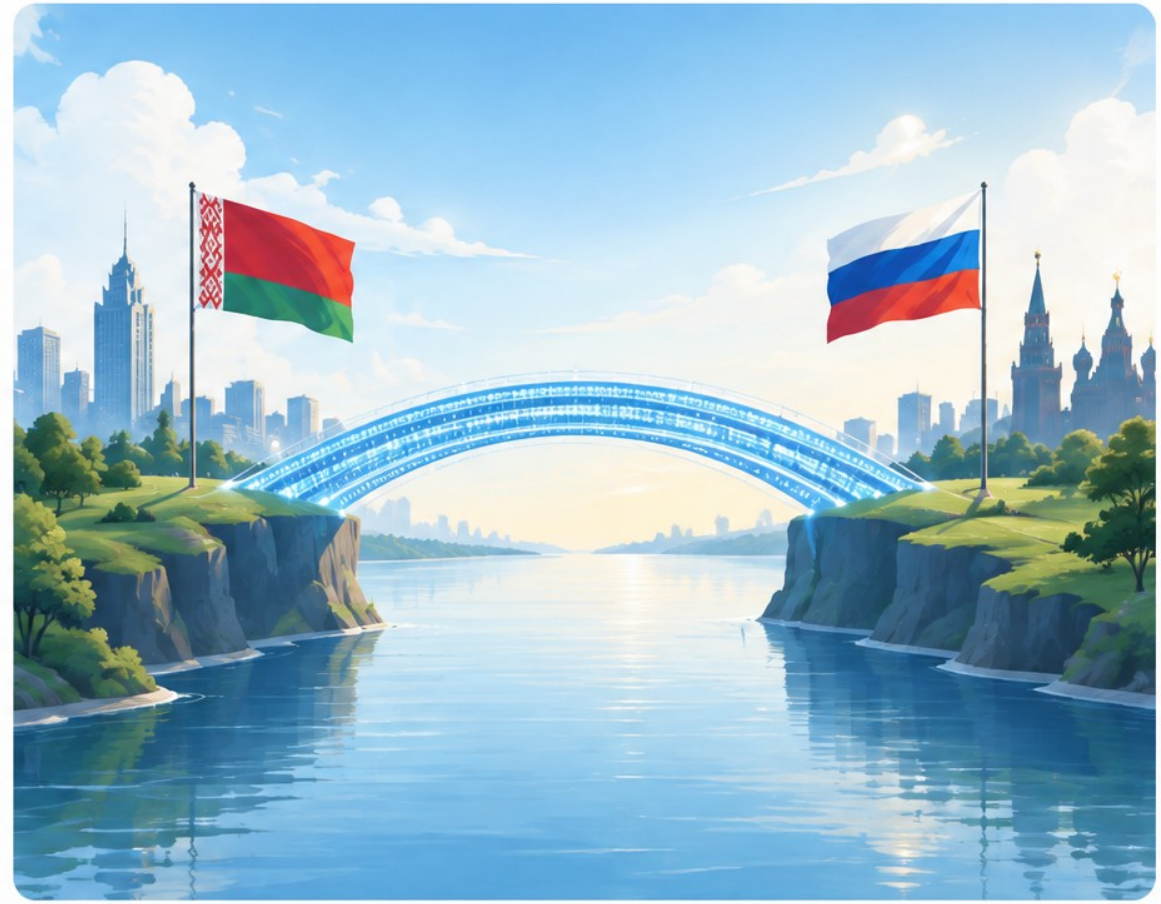
Принцип непрерывности

Информационная система динамична: выходят патчи, меняются конфигурации. Аттестация, пройденная год назад, не гарантирует безопасность сегодня. Доверенность переходит в новое качество — киберустойчивость системы.

Перспективы гармонизации в Союзном государстве

Стратегические шаги

1. Сформировать единое совместимое методологическое пространство.
2. Согласовать общий понятийный аппарат и пороговые критерии.
3. Взаимно признавать и сопоставлять результаты оценок ИС в совместных проектах.
4. Создать реестр критических технологических зависимостей и динамических карт рисков.



Заключение: Основные результаты

01

Смена парадигмы

Переход от защиты локальных ресурсов к комплексному управлению свойствами всей технологической экосистемы. Технологическая зависимость введена как самостоятельный фактор риска.

02

Исключение компенсационного эффекта

Использование логической функции-отсекателя доказало свою эффективность, исключая маскировку критических недостатков.

03

Динамический контроль

Доказано, что доверенность является не статической, а динамической характеристикой, требующей непрерывного подтверждения.

Разработанный аппарат может послужить **основой для концепции** следующей научно-технической программы Союзного государства в области комплексной защиты информации.