



Актуальные вопросы повышения качества проектов и продуктов по ИБ Из опыта разработчика СЗИ

ЕГОР КОЖЕМЯКА

ДИРЕКТОР ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU



Тысячи проектов ежегодно
реализуются в России
с использованием
продуктов Dallas Lock

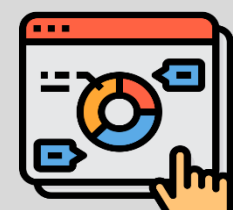


Основные потребности заказчиков:

- Внедрение самых современных компьютерных технологий
- Надёжность функционирования информационных систем
- Выполнение требований по защите информации и импортозамещению

Особенности крупных проектов:

- Десятки тысяч АРМ (закупка новых, модернизация)
- Импортозамещение
- В регионах/ведомствах, где сегодня есть бюджеты на цифровизацию



Прикладное ПО



Средства защиты информации

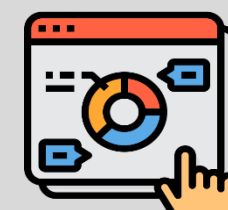


Операционная система



Оборудование

Физическая
инфраструктура



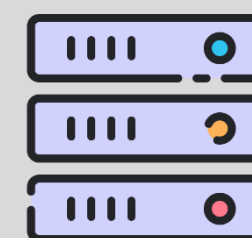
Виртуальные машины, прочее ПО



Средства защиты среды виртуализации



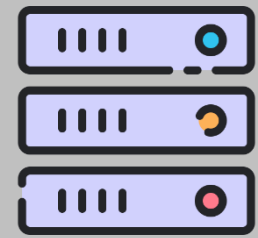
Система виртуализации



Оборудование

Виртуализованная
инфраструктура

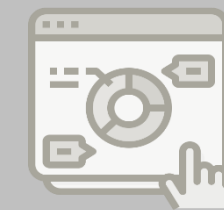
Закупка
оборудования



Установка
ОС/ВИ



Установка
прикладного ПО



Установка
СЗИ



Особенности закупки оборудования:

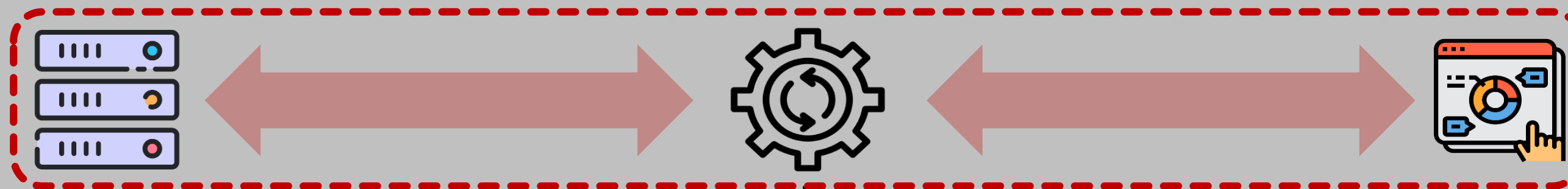
- *лучше сразу купить самое новое надёжное и производительное, так как в следующий раз бюджета может и не быть*
- *«кризис полупроводников»: с 2020 года наблюдается существенная задержка в поставках аппаратных средств, а также повышение стоимости на серверное, сетевое оборудование и прочие аппаратные решения*

Закупка
оборудования

Установка
ОС/ВИ

Установка
прикладного ПО

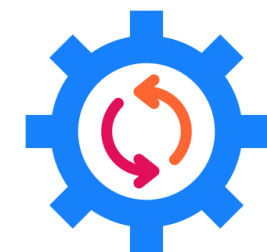
Установка
СЗИ



ОС/ВИ'



ОС/ВИ''



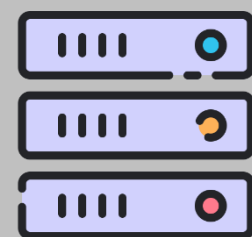
ОС/ВИ'''



**Обеспечение совместимости
требует времени:**

- процессор и видеокарта не поддерживаются ядром ОС/ВИ
- принтеры не печатают
- прикладной софт не работает

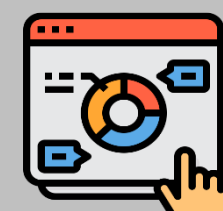
Закупка
оборудования



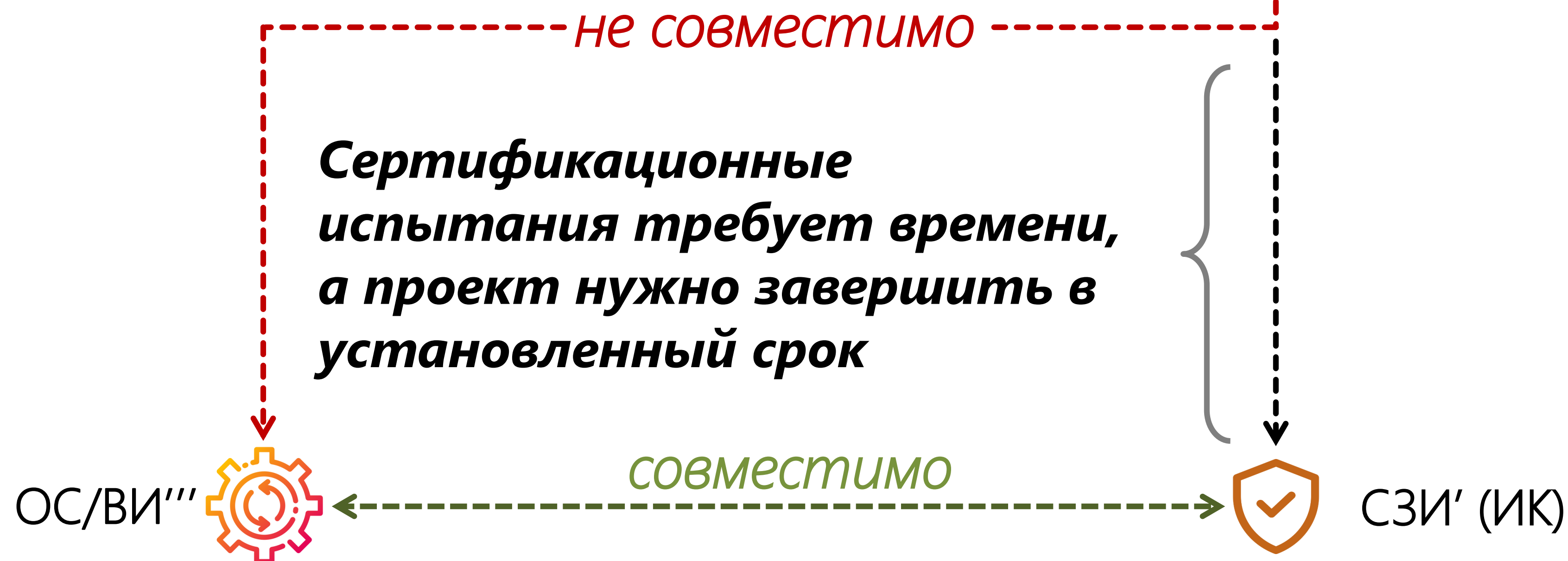
Установка
ОС/ВИ

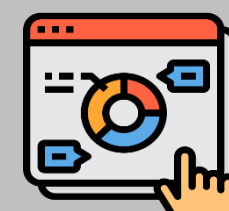
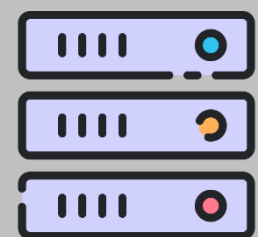


Установка
прикладного ПО



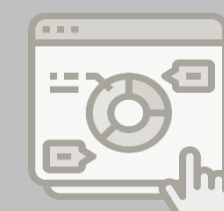
Установка
СЗИ





В результате тратится много времени, денег и прочих ресурсов для достижения результата. Создаётся впечатление, что продукты некачественные, интегратор работает непрофессионально, а заказчик впустую тратит деньги.

Практический кейс в процессе эксплуатации



Обновление ОС/ВИ

Необходимо устранить уязвимость, но СЗИ (включая централизованное управление) выйдет из строя из-за несовместимости с обновлением

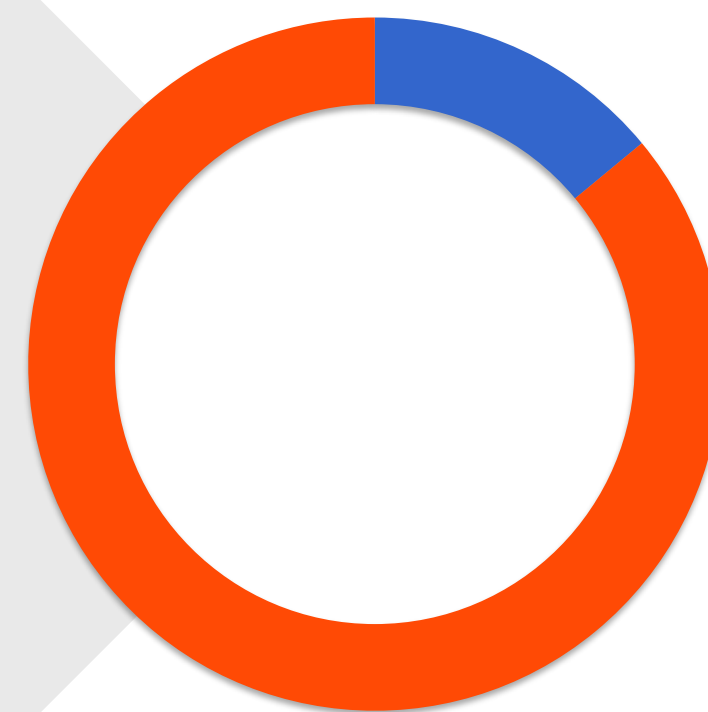
Работоспособность СЗИ

Необходимо сохранить работоспособность СЗИ (включая централизованное управление), но в ОС/ВИ останется незакрытая уязвимость





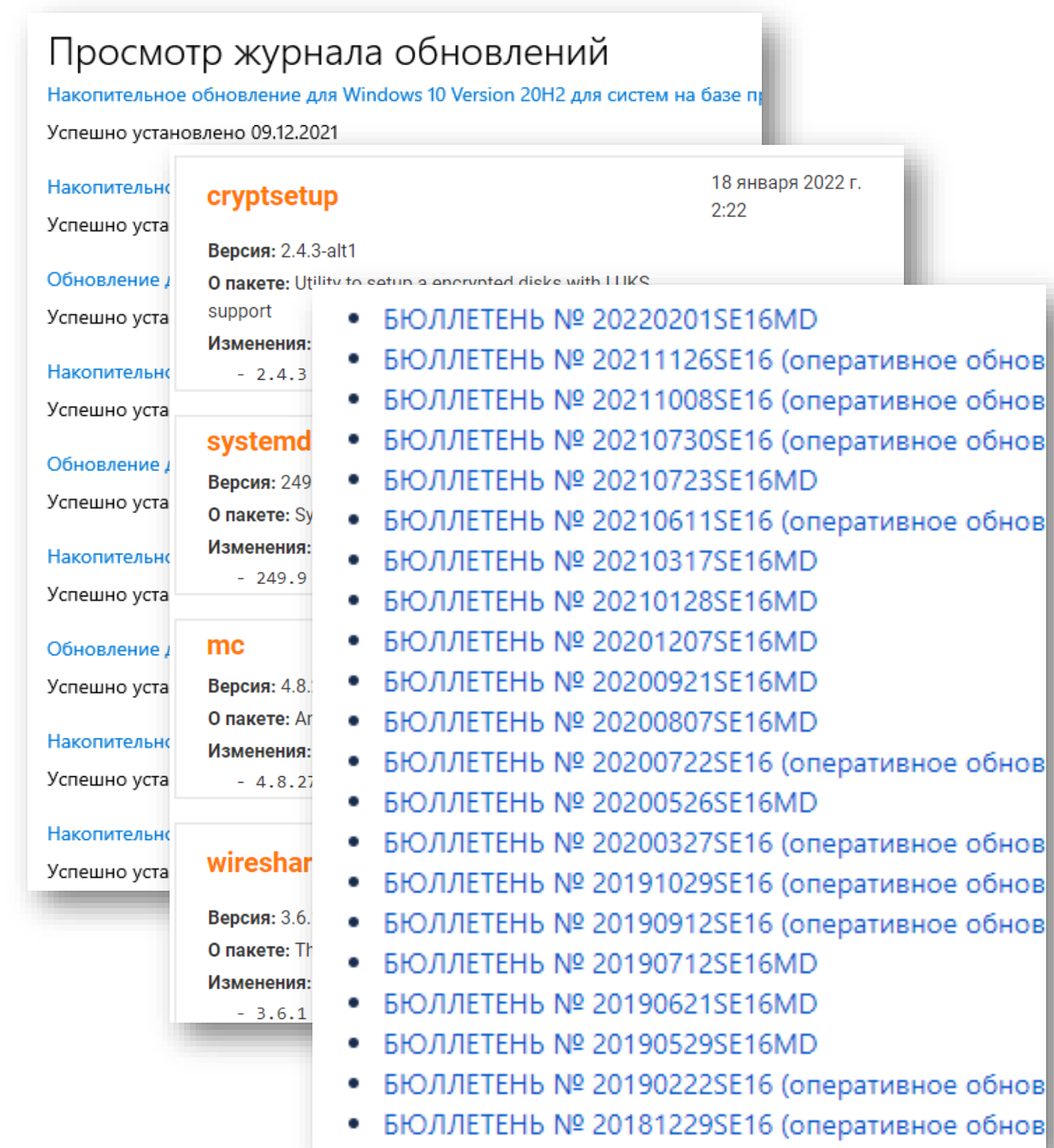
14% обновляют ОС/ВИ
86% не обновляют ОС/ВИ



*Результаты опроса
ключевых партнёров
ЦЗИ «Конфидент»*

Как часто выпускаются обновления среды исполнения?

- Microsoft Windows обновляет функции 2 раза в год, а обновления по безопасности выпускаются более 20 раз за год.
- Astra Linux получает кумулятивные бюллетени по безопасности примерно 6 раз в год.
- Alt Linux, РЕД ОС, РОСА ОС получают десятки обновлений пакетов в год.



Результаты опроса ключевых партнёров ЦЗИ «Конфидент» об источниках проблем в проектах:

13%

Сложности выполнения новых требований по моделированию угроз и аттестации информационных систем

21%

Сложности импортозамещения: совместимость ОС/ВИ с оборудованием и ПО, управление СЗИ, защита отечественных платформ виртуализации

36%

Несовместимость СЗИ с ОС/ВИ, длительная процедура сертификации СЗИ для сокращения отставания СЗИ от обновлений среды исполнения

22%

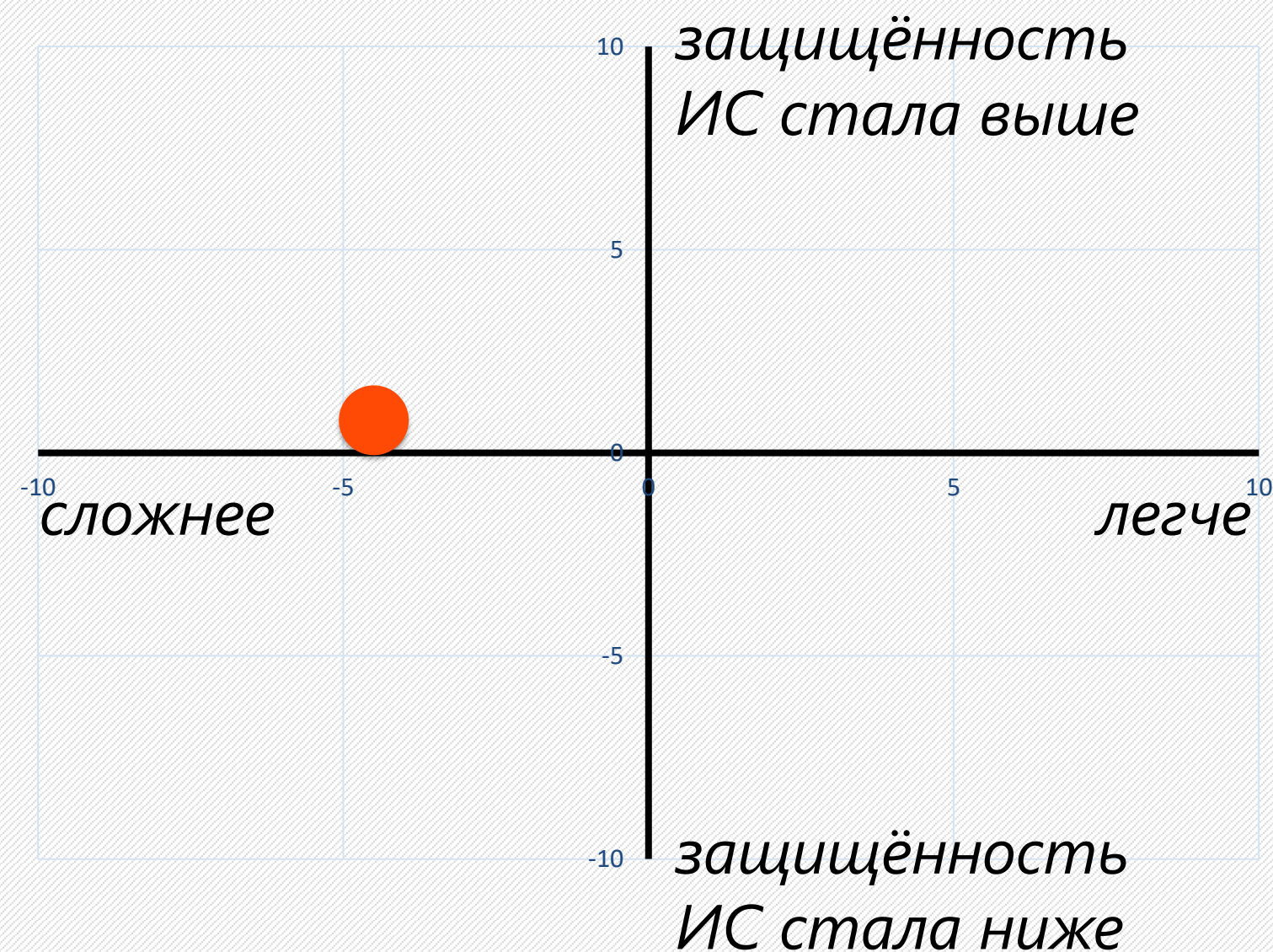
Кадровые проблемы. Нехватка квалифицированных специалистов, «утечка мозгов» в крупные госкорпорации и ИТ-гиганты

8%

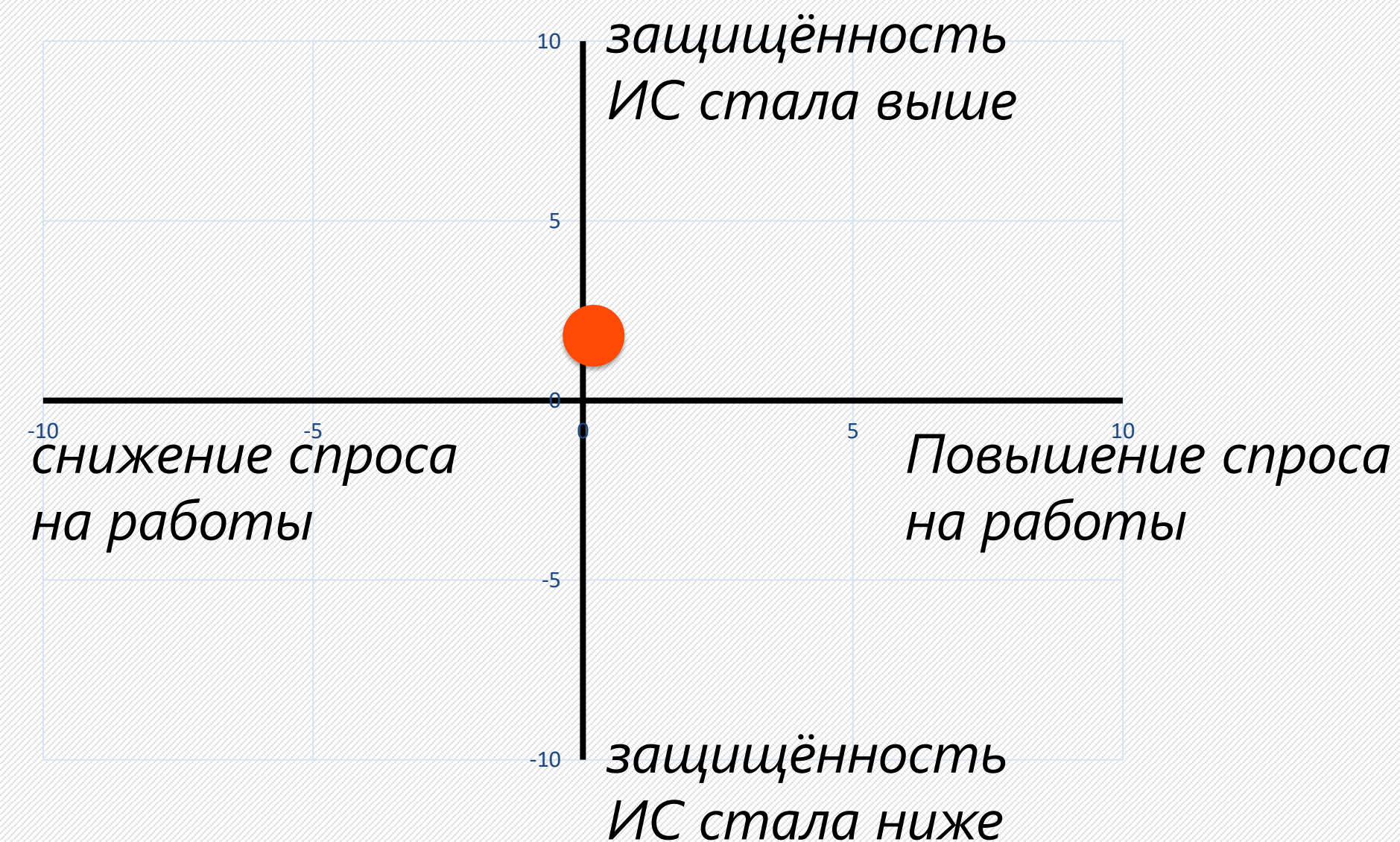
Другое: нехватка финансов, желание заказчиков обходиться только орг. мерами, непонимание ИБ руководством, кризис полупроводников

Результаты опроса ключевых партнёров ЦЗИ «Конфидент»:

Как вы оцениваете применение на практике новой Методики оценки угроз безопасности информации ФСТЭК России?



Новый порядок аттестации объектов информатизации согласно Приказу ФСТЭК России №77 от 29.04.2021 г.

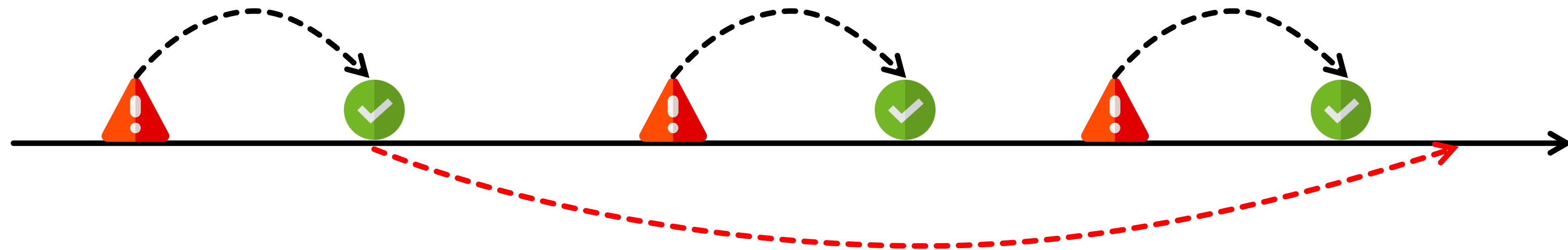


ЧТО МЫ ДЕЛАЕМ:

1. Инвестиции в разработку, оптимизация методологии.
2. Активное применение и развитие подходов к безопасной разработке ПО.
3. Автоматизация тестирования: unit-тестирование, автоматическое тестирование сборок в разных средах исполнения, автоматизация ручных тестов.
4. Сотрудничество с разработчиками отечественных ОС и платформ виртуализации.
5. Привлечение сторонних организаций для независимого тестирования.

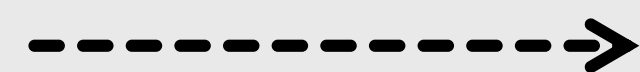
ЧТО МЫ ПРЕДЛАГАЕМ:

Устранение уязвимостей в ОС/ВИ: быстрый выпуск обновлений по понятной процедуре



Устранение несовместимости с ОС/ВИ в накладных сертифицированных решениях через процедуру ИК

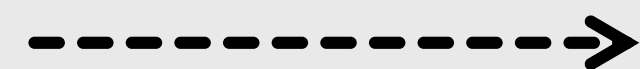
В СЗИ обнаружена уязвимость



Формальная процедура устранения уязвимости



Изменение среды исполнения СЗИ



Предлагаем внести изменения в нормативную базу



ЧТО МЫ ПРЕДЛАГАЕМ:

1

Предлагаем уточнить порядок сертификационных испытаний при изменении среды исполнения: внести изменения в Положение о системе сертификации средств защиты информации, а также разработать соответствующие рекомендации.

73. В случае внесения в сертифицированное средство защиты информации изменений, связанных **с устранением уязвимостей** (недекларированных возможностей) средства защиты информации или **обновлением баз данных**, необходимых для реализации функций безопасности средства защиты информации, заявитель информирует потребителей о необходимости обновления средства защиты информации и доводит до потребителей обновления средства защиты информации до проведения испытаний, предусмотренных пунктами 71 и 72 настоящего Положения.

Добавить:

или **изменением среды исполнения** средства защиты информации

2

Предлагаем на основе информации, содержащейся в формулярах на изделия, вносить информацию о совместимости в Государственный реестр сертифицированных СЗИ.



Спасибо за внимание!

ЕГОР КОЖЕМЯКА

**ДИРЕКТОР ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»**

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

www.dallaslock.ru