КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Практика применения разнородных СЗИ в ГИС по итогам 2023 года

Кожемяка Егор

ДИРЕКТОР
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

Нормативная база требований

Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Указ распространяется на следующие органы (организации):

- федеральные органы исполнительной власти
- высшие исполнительные органы государственной власти субъектов РФ
- государственные фонды
- государственные корпорации (компании)
- и иные организации, созданные на основании федеральных законов

ГИС попадает под действие данного указа

Органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства с 1 января 2025 г.

Реализация требований

Для вновь создаваемых объектов информатизации

Вновь создаваемые объекты информатизации реализуются на базе отечественных ОС (сертифицированных или не сертифицированных)

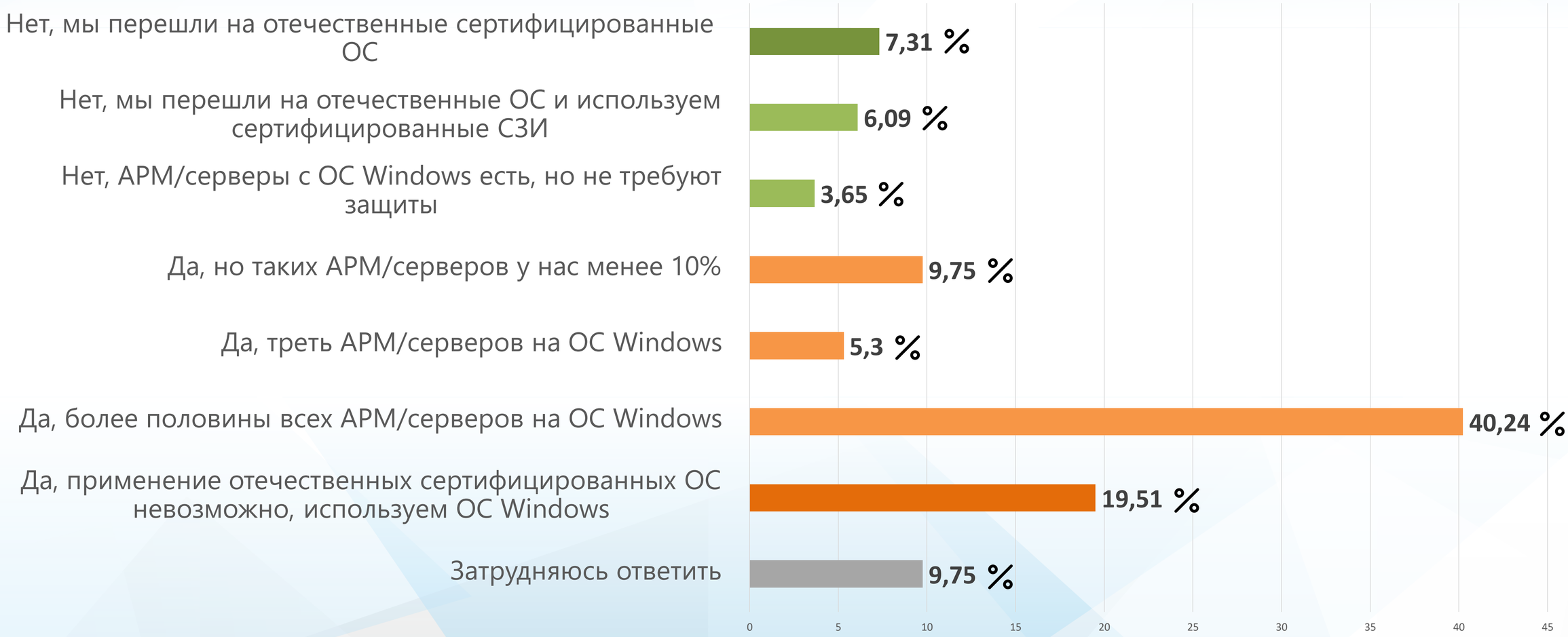
Для ранее созданных объектов информатизации

Какова реальная картина импортозамещения сейчас на объектах информатизации, которые уже имеют аттестат соответствия?

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Исследование ЦЗИ «Конфидент»

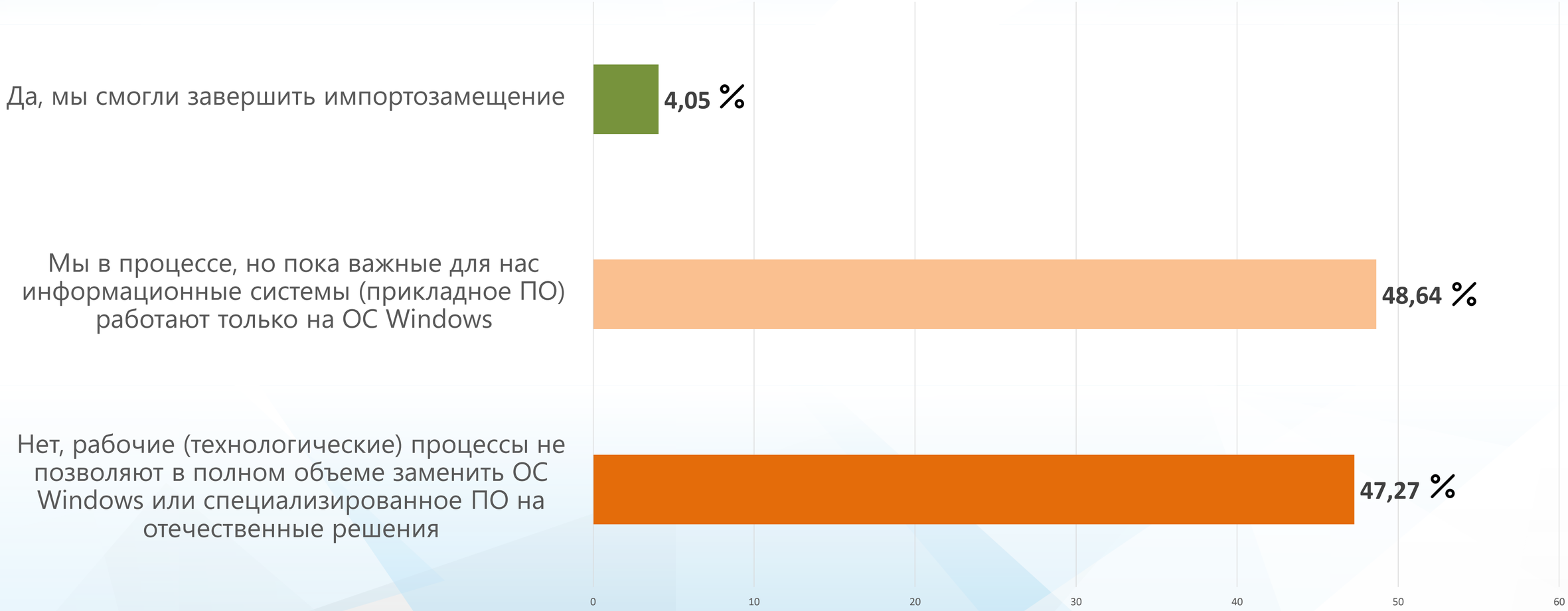
Существует ли **потребность в защите АРМ/серверов с ОС Windows** на ваших объектах информатизации?



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Исследование ЦЗИ «Конфидент»

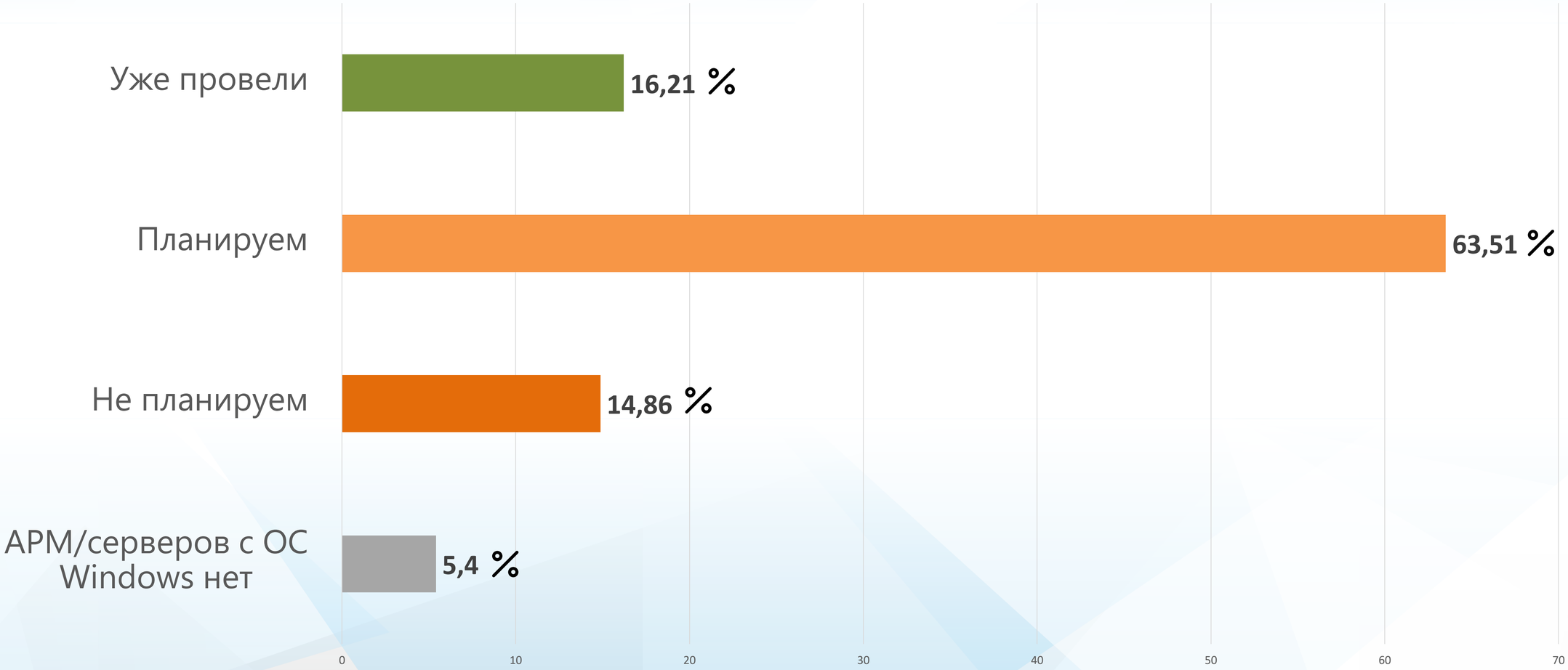
Удалось ли вам **перевести ИТ-инфраструктуру** (ОС, прикладное ПО, информационные системы) только на отечественные решения?



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Исследование ЦЗИ «Конфидент»

Планируете ли вы проводить обновление СЗИ на АРМ/серверах с ОС Windows?



Результаты исследования и «конфликт» обновления

Исходя из результатов исследования понятно, что ранее созданные объекты информатизации:

- все еще испытывают потребность в защите АРМ/серверов с ОС Windows – 74%
- в ближайшее время планируют обновления СЗИ на АРМ/серверах с ОС Windows – 63%
- не смогли завершить импортозамещение полностью – 96%

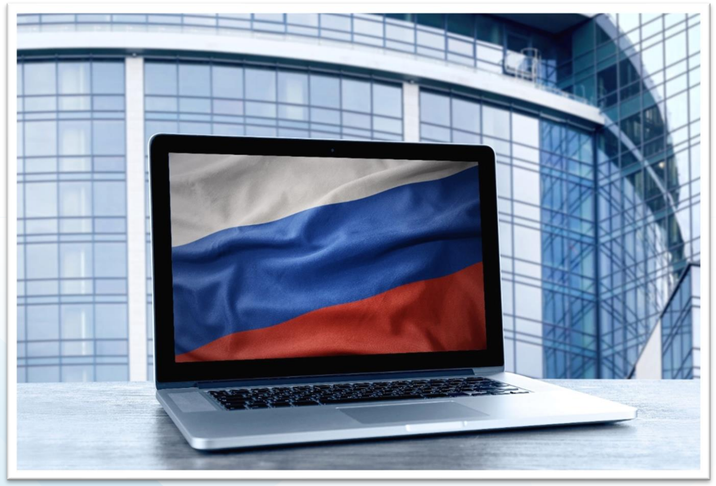
VS

Результаты исследования и «конфликт» обновления

Однако для вендоров сейчас невыгодно выпускать обновления СЗИ для ОС Windows:

- рынок СЗИ для отечественных ОС является наиболее перспективным и стратегически важным
- процесс обновления СЗИ для ОС Windows стал технологически сложнее для вендора
- рынок СЗИ для ОС Windows в перспективе – исчезающий рынок

VS



Решение ЦЗИ «Конфидент»

Необходимо продолжить выпуск обновлений СЗИ, пока сохраняются объекты информатизации, не завершившие процессы импортозамещения полностью

- ЦЗИ «Конфидент» **получил Решение ФСТЭК России** на продление сертификата для СЗИ НСД Dallas Lock 8.0-С
- Процесс импортозамещения **занимает время**, и в это время защита объектов информатизации не должна снижаться
- В продуктовой линейке СЗИ для ОС Windows будут **обновлены инструменты защиты** в соответствии с актуальными угрозами и потребностями пользователей

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Защита от атак типа ransomware

Один из трендов 2022-2023

- **Методы атак:** направлены на шифрование данных с последующим требованием выкупа. Преобладали фишинговые кампании и эксплуатация известных уязвимостей.
- **Цели:** в основном индивидуальные пользователи и малый бизнес, хотя были и крупные атаки на корпорации.
- **Масштабы использования:** чаще всего ограничивались определенными географическими регионами или отраслями.

2018

2019

2020

2021

2022

2023

2024

Методы атак: стали более изощренными, включая методы самораспространения по сети, использование уязвимостей «нулевого дня», механизмы для автономного распространения внутри сетей жертв.

Цели: государственные организации, КИИ. Атаки стали более целенаправленными и стратегически планируемыми.

Масштабы использования: стали глобальными, с поддержкой крупных группировок. Атаки стали чаще применяться «как услуга» (Ransomware as a Service, RaaS).

СОВ
v.803

Разработан **собственный эвристический механизм защиты** от вирусов-шифровальщиков, который включает:

- детектор вредоносной активности
- детектор подозрительных файловых операций
- подсистему принятия решений
- подсистему реагирования

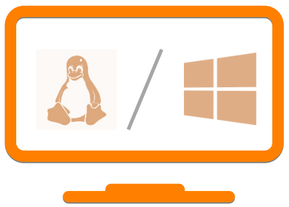
Планы развития СОВ:

- будет добавлен транзакционный механизм
- будет добавлен механизм динамического теневого копирования
- будет расширен перечень распознаваемых индикаторов
- отчет о работе станет удобнее и покажет, как развивалась атака

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Защита и централизованное управление в гетерогенной среде

Гетерогенные среды характеризуются разнообразием операционных систем, платформ и приложений, требуют комплексного и гибкого подхода к безопасности, который Dallas Lock успешно реализует, предлагая централизованное управление и гарантируя высокий уровень защиты в комплексе.



СДЗ Dallas Lock

СДЗ Dallas Lock

СДЗ Dallas Lock

Агент ЕЦУ

СЗИ Dallas Lock 8.0

НСД МЭ СОВ СКН

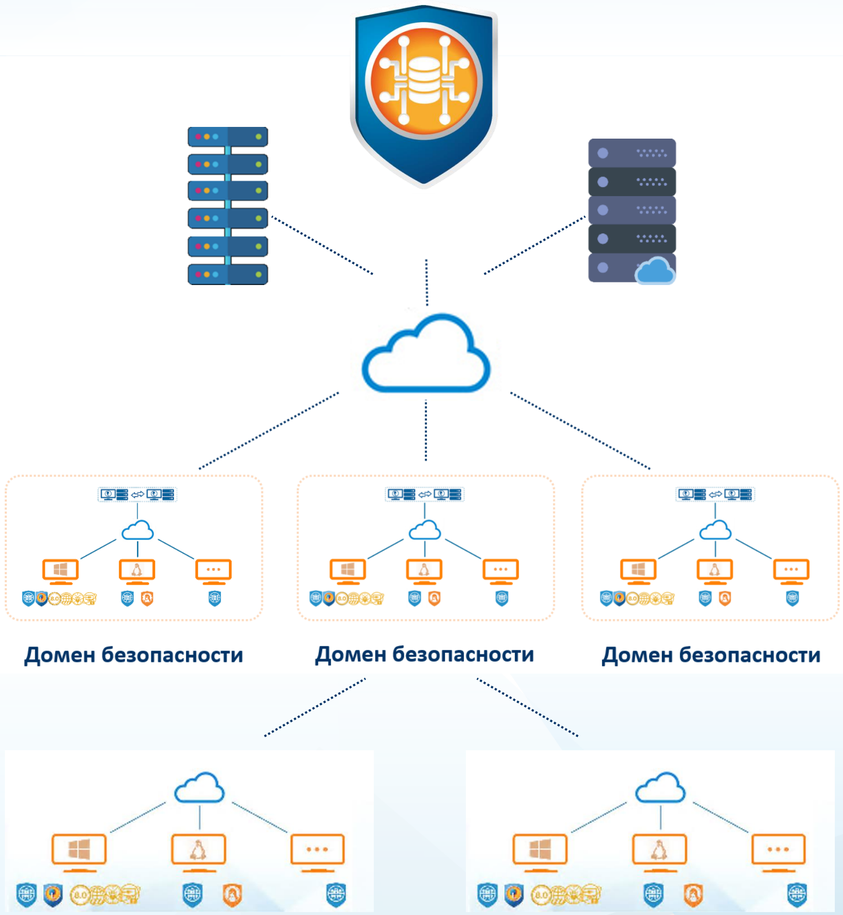
Dallas Lock Linux

МЭ СКН

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Защита и централизованное управление в гетерогенной среде

Единый центр управления Dallas Lock



Построение отказоустойчивых доменов безопасности

Защита сложных гетерогенных сетевых инфраструктур

Низкая стоимость владения

\+

универсальная лицензия на СЗИ

- Единый центр управления работает в том числе на российских ОС
- Иерархическая структура доменов безопасности
- Контроль состояния (целостности) активного сетевого оборудования
- Работа за NAT
- Построение отказоустойчивых кластеров из отдельных приложений ЕЦУ позволяет реализовать управление сложными гетерогенными инфраструктурами с количеством защищаемых объектов более 50 000 шт.

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Спасибо за внимание!

Кожемяка Егор

ДИРЕКТОР
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU