КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Тренды развития сертифицированных средств защиты информации в современных реалиях

Егор Кожемяка

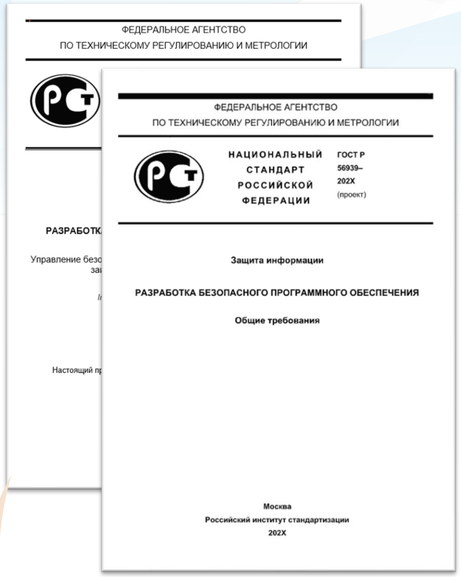
ДИРЕКТОР
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

ФСТЭК России. Новые требования безопасности. Новые решения на рынке


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939–202X (проект)

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Москва
Российский институт стандартизации
202X

1 Требования по безопасности информации к средствам обнаружения и реагирования уровня узла

2 Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети

3 Обновление Приказа ФСТЭК России от 11 февраля 2013 г. № 17

Производители СЗИ создают новые решения

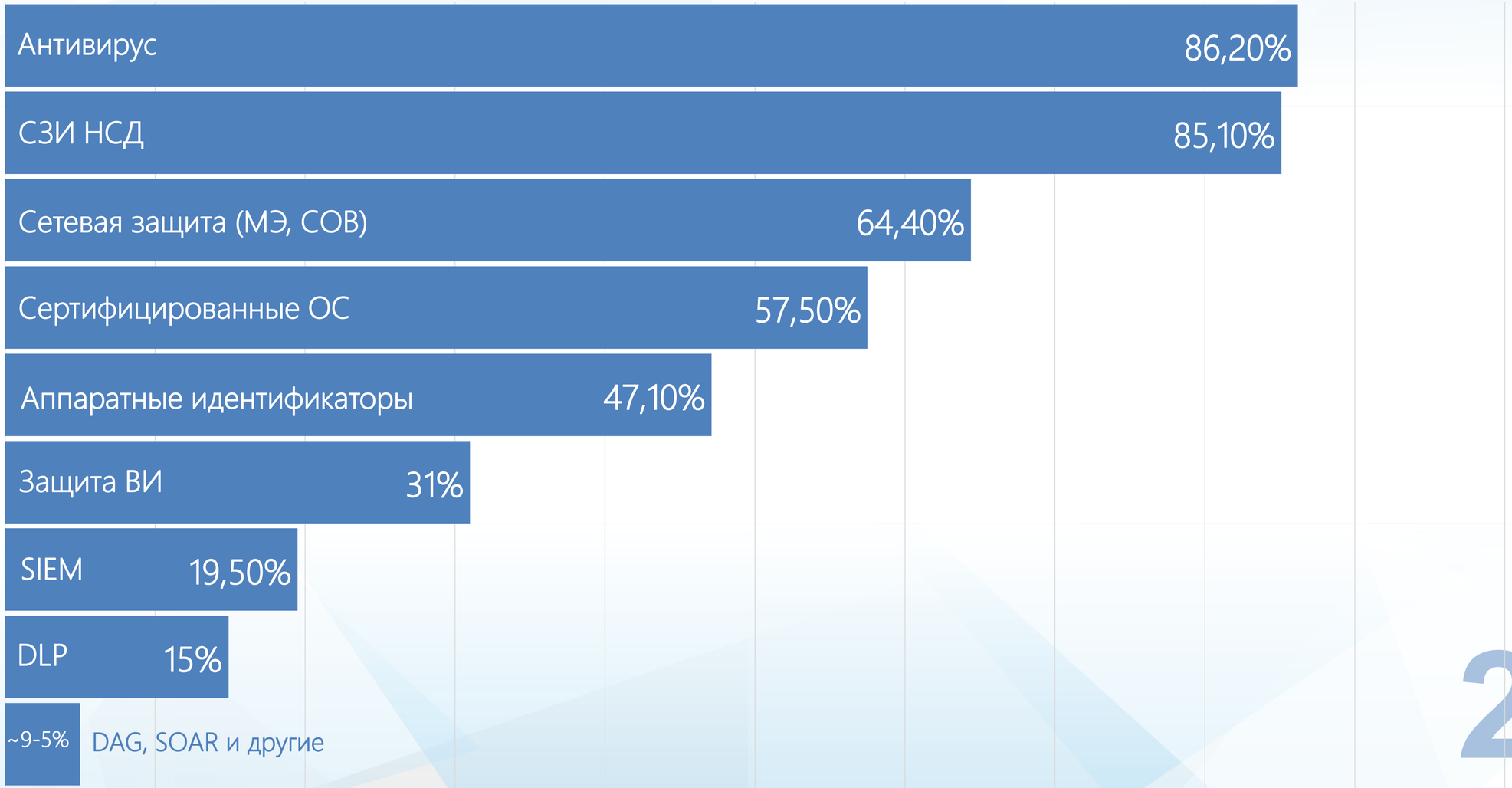
Развивают защиту конечных точек, усиливая обнаружение угроз, связанных с внедрением ВПО, а также обеспечивают оперативное реагирование, нейтрализацию и централизованное расследование таких инцидентов

Расширение возможностей продуктовой линейки

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

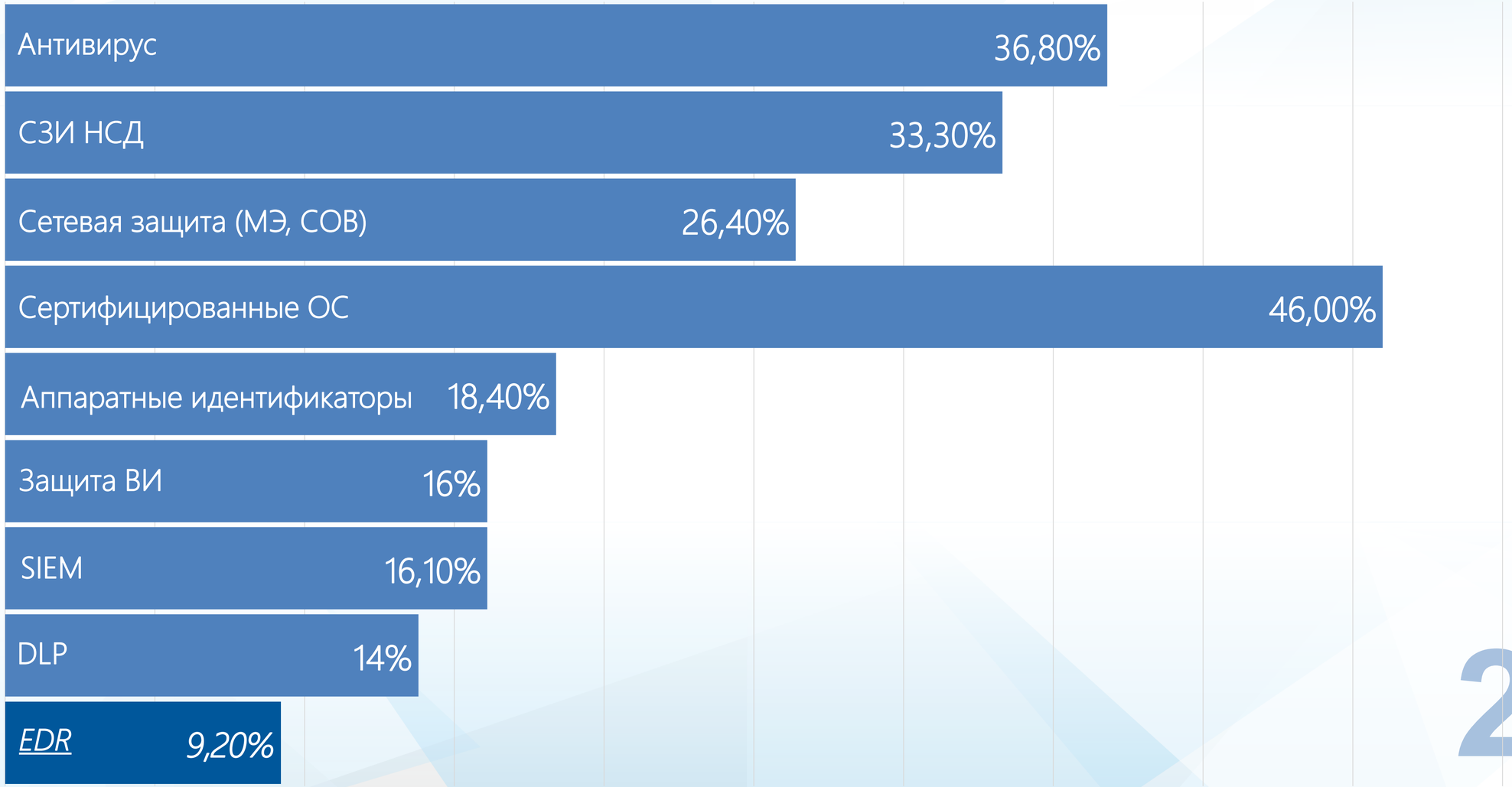
Какие средства защиты информации используются в вашей организации?



2025

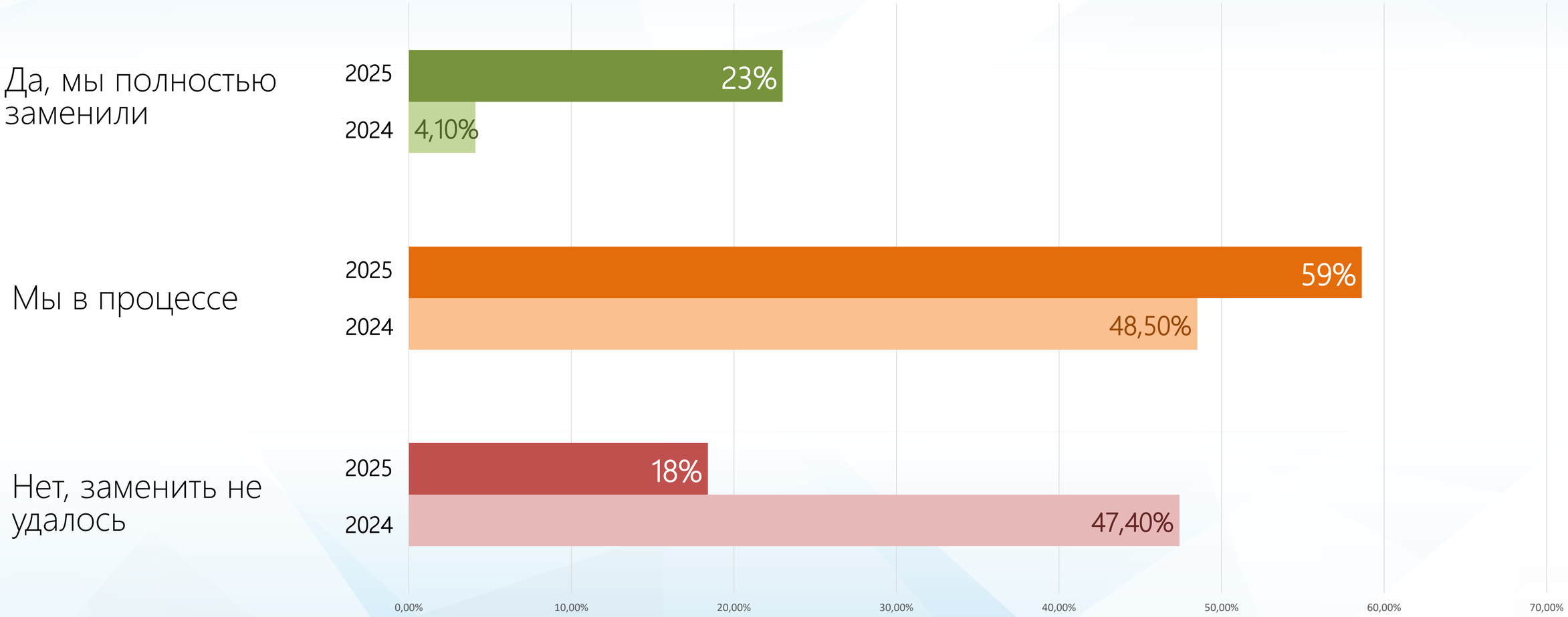
КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Какие средства защиты информации вы планируете внедрить в этом году?

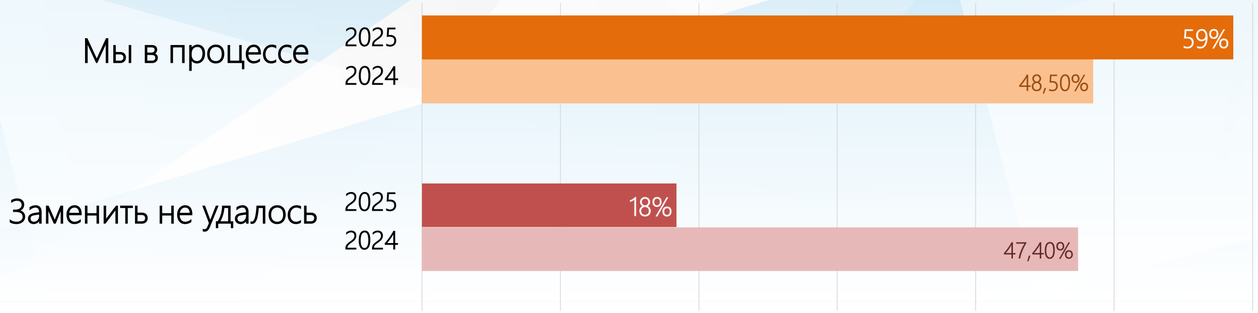


2025

Смогли ли вы заменить иностранные решения и сервисы на отечественные?



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ



ЦЗИ «Конфидент» продолжает выпуск обновлений СЗИ, пока сохраняются объекты информатизации, не завершившие процессы импортозамещения полностью

Процесс импортозамещения занимает время, и в это время защита объектов информатизации не должна снижаться.

В продуктовой линейке СЗИ для ОС Linux и Windows будут обновлены инструменты защиты в соответствии с актуальными угрозами и потребностями пользователей

ЕЦУ Dallas Lock

Поддержка российских ОС

ASTRALINUX® common edition · РЕДОС · base alt · ROSA · ASTRA LINUX

Централизованное управление

Управление сетевым оборудованием

- Сканирование сети для обнаружения устройств
- Контроль изменений конфигурации
- Сбор событий по протоколу Syslog

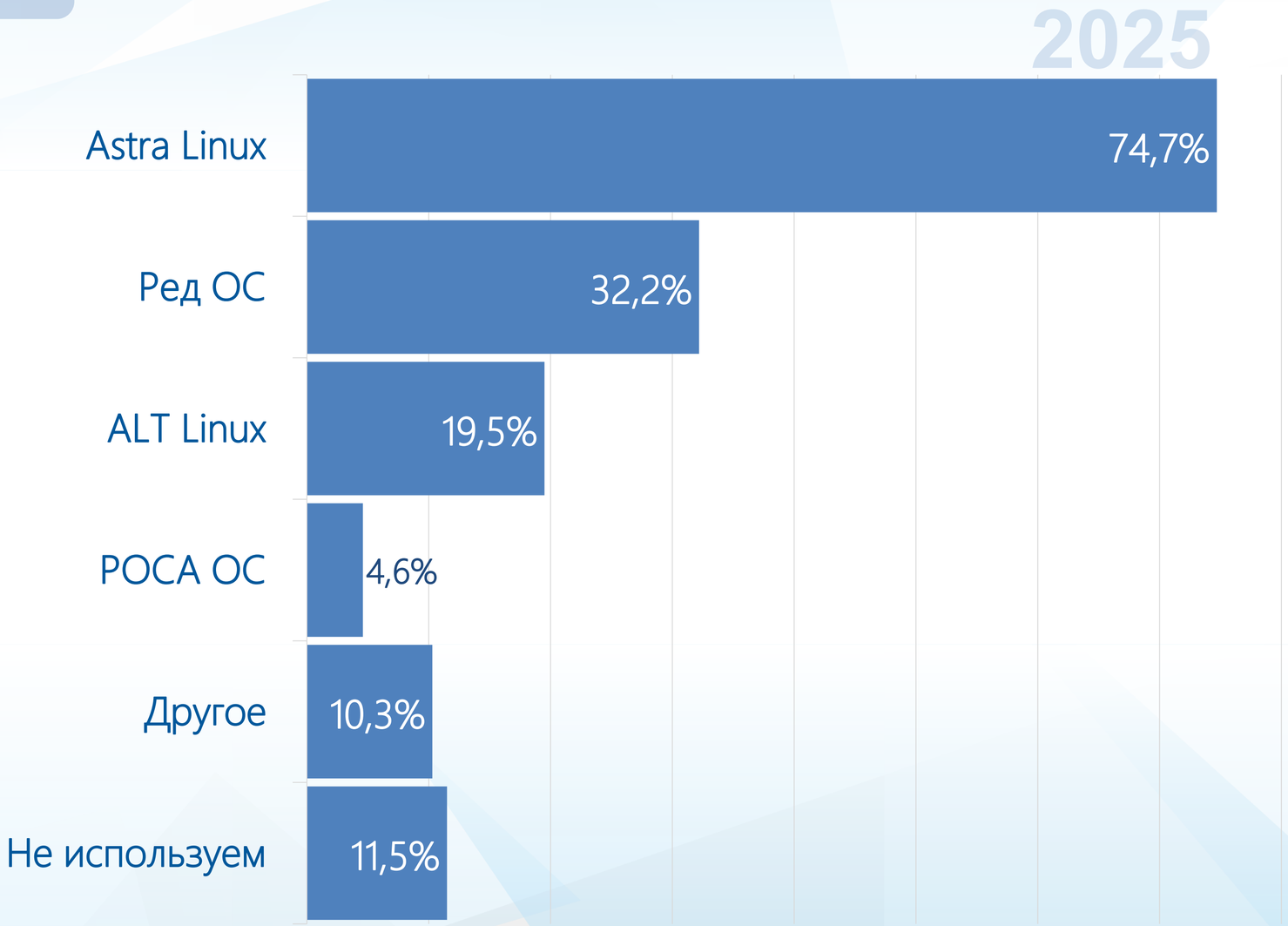
Интеграция со сторонними продуктами

РЕДАДМ · ALD Pro · FreeIPA · SIEM

ПОДРОБНАЯ ИНФОРМАЦИЯ
ДЕМОВЕРСИИ, БАЗА ЗНАНИЙ, НОВОСТИ
WWW.DALLASLOCK.RU

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Какие отечественные ОС вы используете?



Сертификат ФСТЭК России

Включен в единый реестр российского ПО

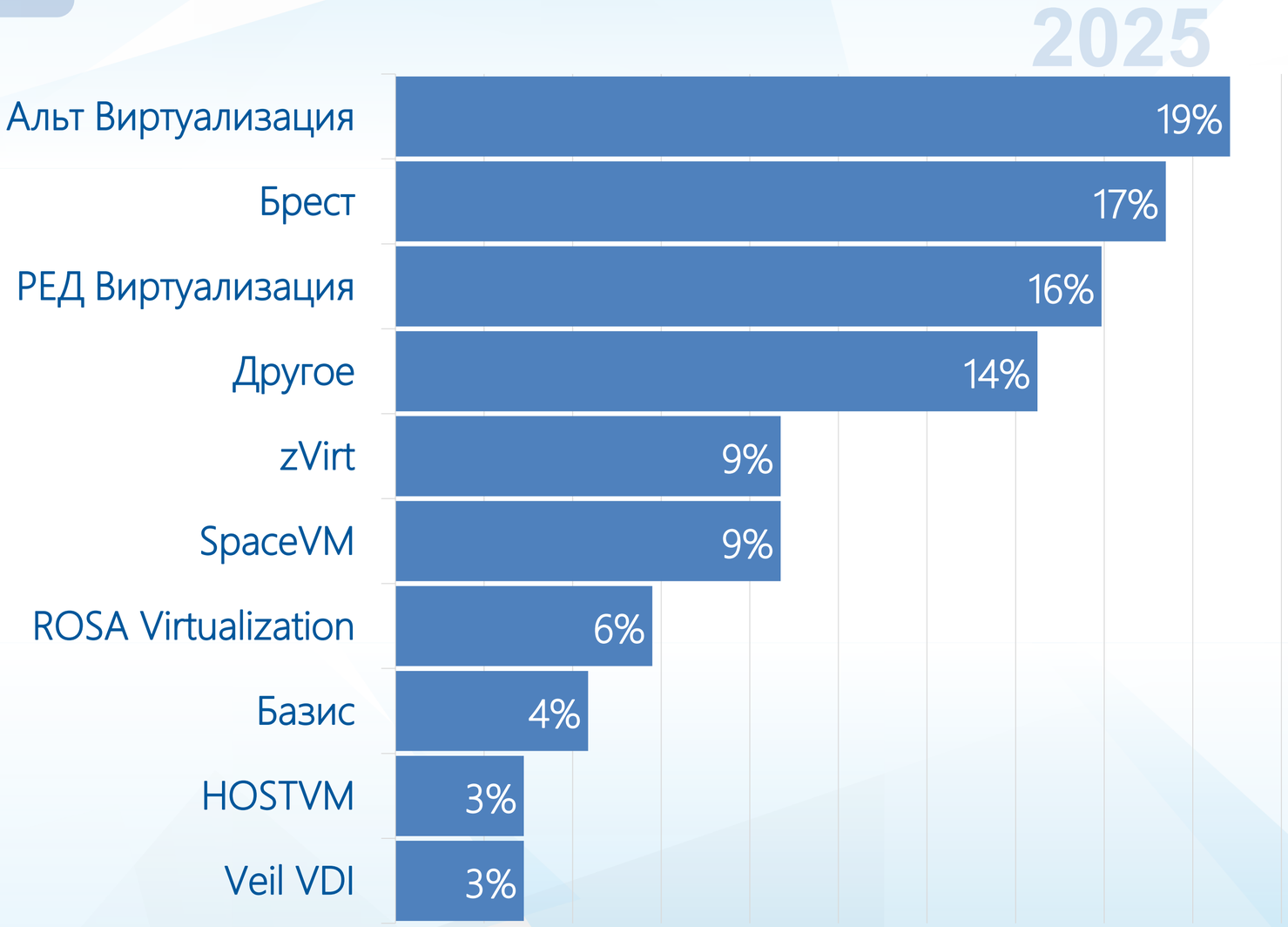
сертификат МЭ ИТ.МЭ.В4.ПЗ

сертификат СОВ уровня узла ИТ.СОВ.У4.ПЗ

сертификат СКН уровня подключения ИТ.СКН.П4.ПЗ

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Какие отечественные платформы виртуализации вы используете?



Сертификат ФСТЭК России

Включен в единый реестр российского ПО

сертификат МЭ ИТ.МЭ.Б4.ПЗ

Отечественные платформы виртуализации

vmware®

KVM

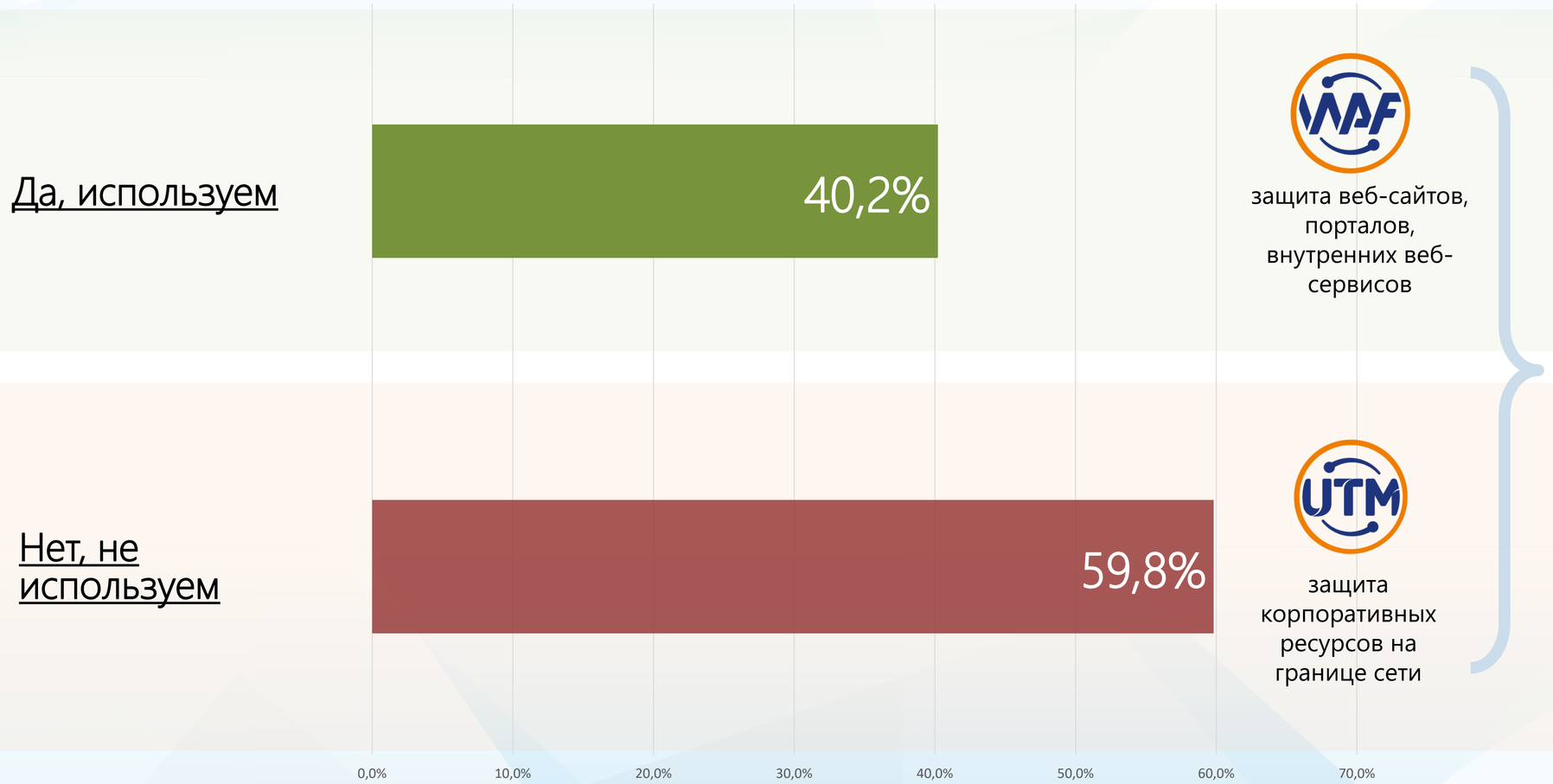
Управление полностью реализовано на отечественных решениях

Все параметры СЗИ ВИ можно легко настраивать через веб-консоль

ПОДРОБНАЯ ИНФОРМАЦИЯ
ДЕМОВЕРСИИ, БАЗА ЗНАНИЙ, НОВОСТИ
WWW.DALLASLOCK.RU

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Используете ли вы веб-приложения или сайты, которым требуется защита?



WAF

защита веб-сайтов, порталов, внутренних веб-сервисов

UTM

защита корпоративных ресурсов на границе сети

Шлюз безопасности WAF Dallas Lock

- **OWASP TOP 10**
- **Инспекция SSL/TLS**
- **GEO IP-фильтр**
- **Защита от DoS/DDoS**

Сертификат ФСТЭК России

Включен в единый реестр российского ПО

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Используется ли в вашей организации средство доверенной загрузки?

СДЗ платы расширения

PCI Express
для стандартных ПК и серверов

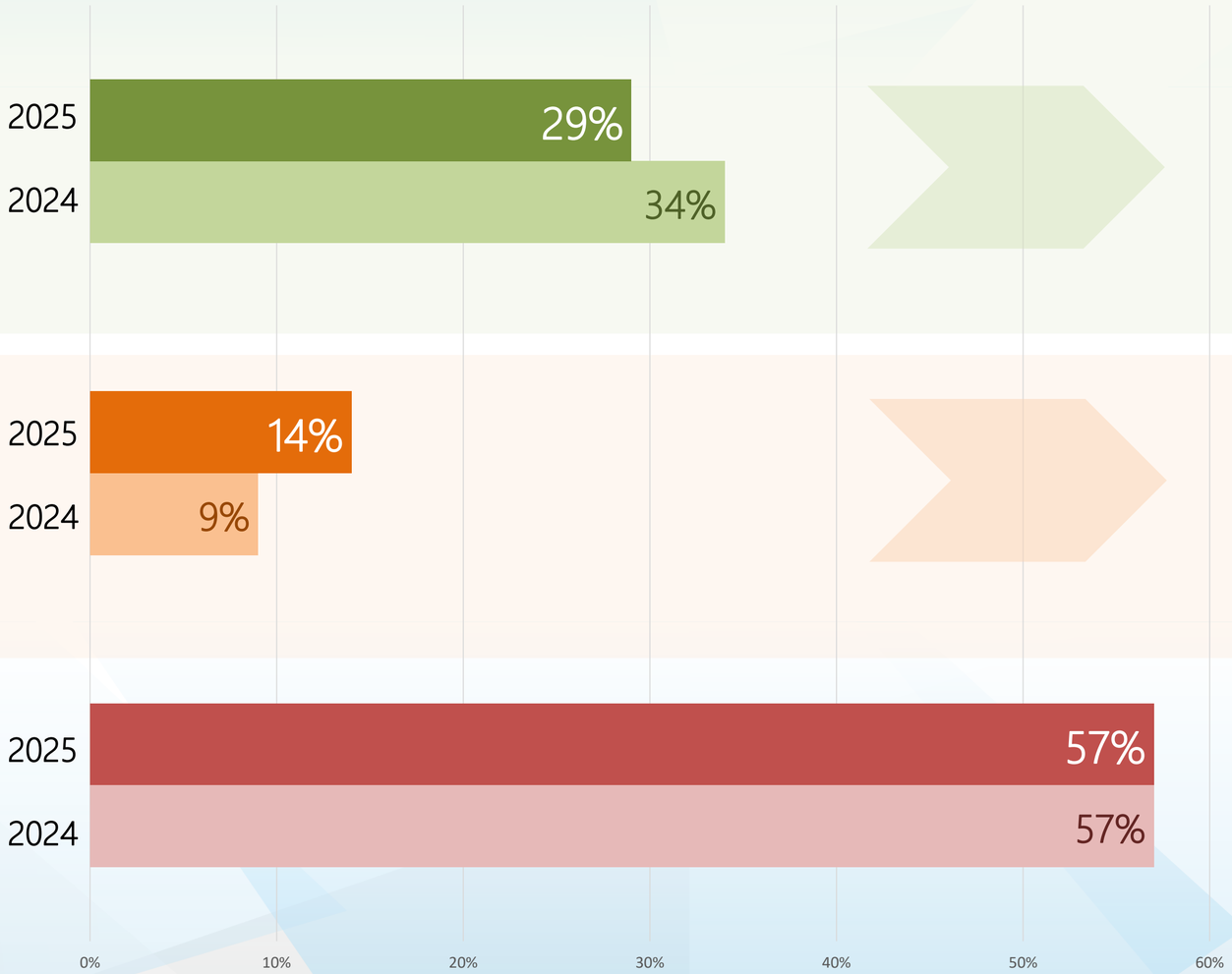
mini PCI Express
компактное решение для встраиваемых систем

M.2
для ультратонких устройств и ноутбуков

СДЗ уровня BIOS

Если использование СДЗ ПР невозможно, отличной альтернативой станет СДЗ уровня BIOS. Это также позволит сохранить высокий уровень безопасности

Не используется



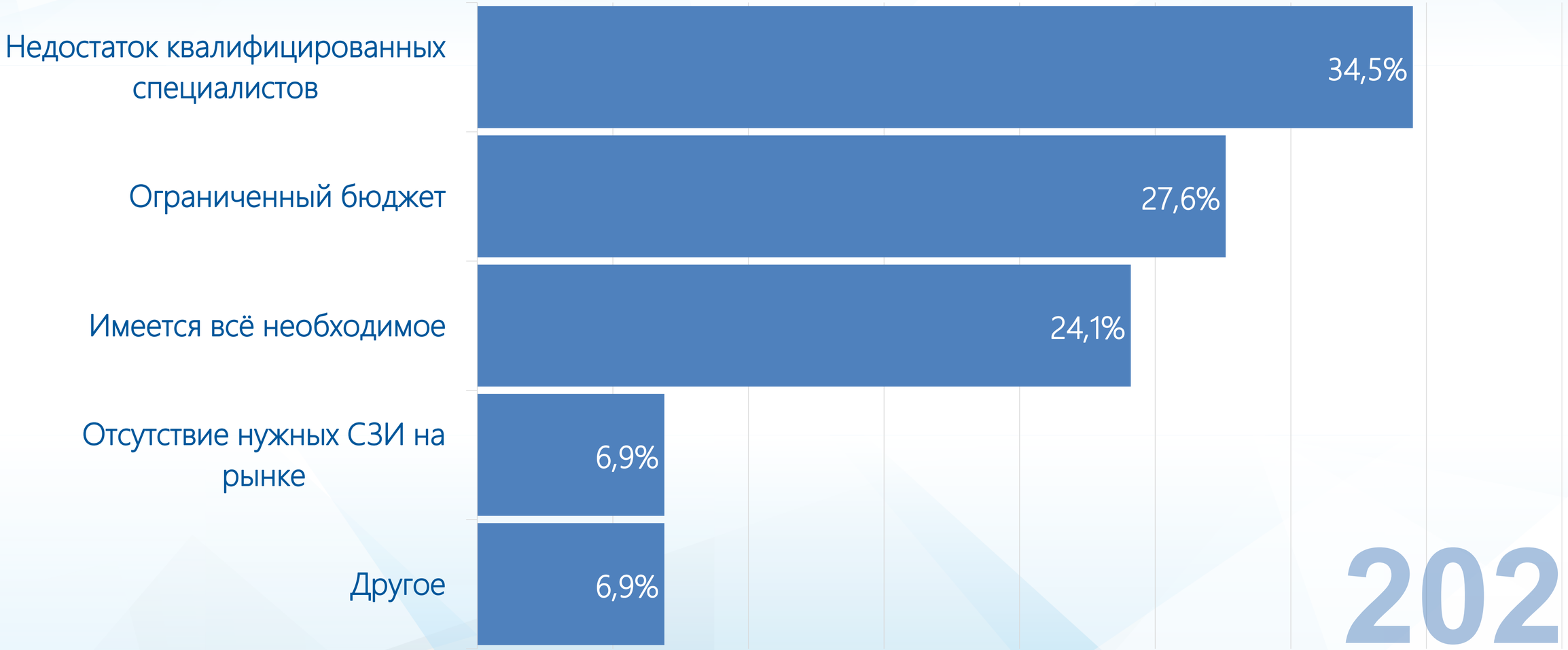
Сертификат ФСТЭК России

Сертификат МО России

Включен в единый реестр российского ПО

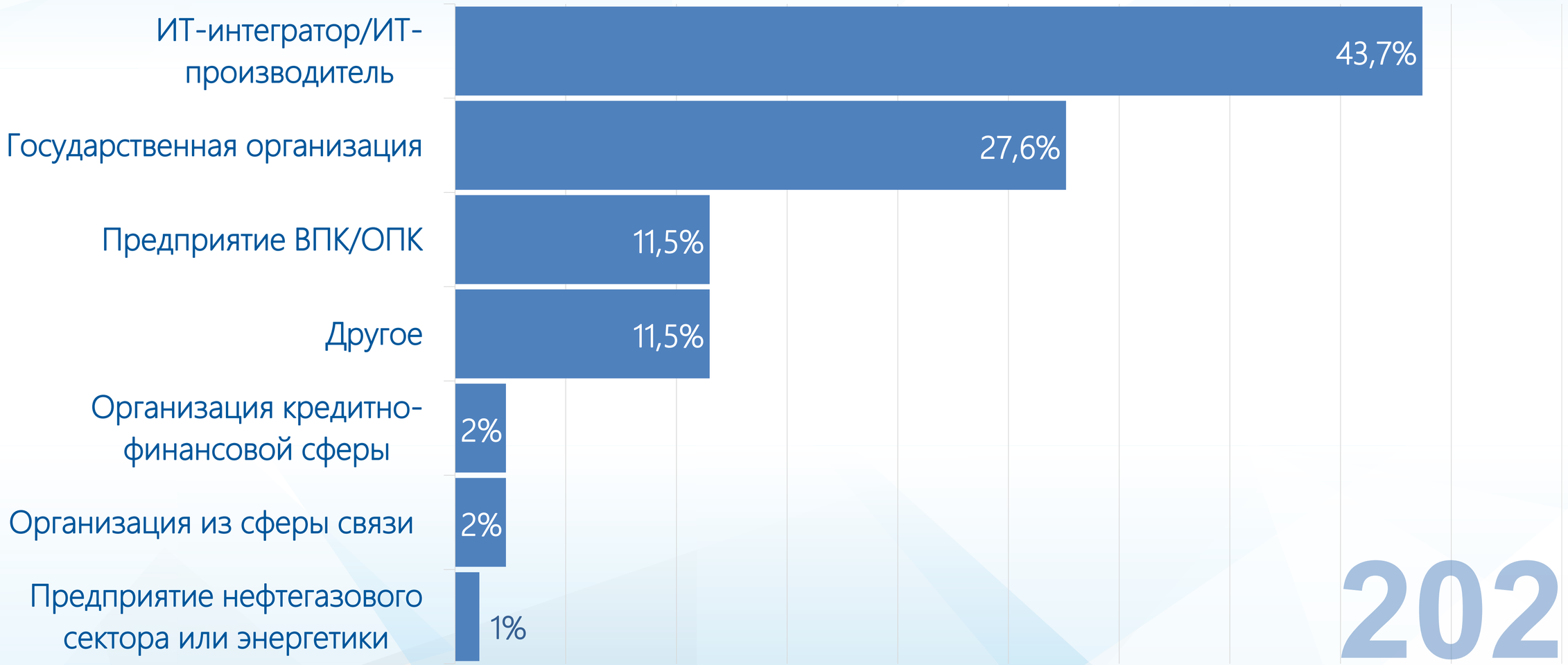
КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Какие основные факторы мешают успешной работе вашего отдела информационной безопасности?



2025

Какую организацию вы представляете?



2025

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

ИМПОРТОЗАМЕЩЕНИЕ ПРОДОЛЖАЕТСЯ

- Доля компаний, полностью заменивших иностранные решения, значительно выросла - с 4,1% до 23%
- К концу 2025 можно ожидать дальнейшее увеличение, поскольку большая часть участников опроса уже находится на этом пути

ВАЖНЫЙ ЭТАП ПЕРЕХОДА

Поддержка обновлений для средств защиты информации на иностранных ОС остаётся актуальной. Это критически важно для:

- стабильности и снижения рисков для организаций, которые ещё не завершили переход
- обеспечения непрерывности работы критически важных систем

РАЗВИТИЕ EDR. ОСОБОЕ ВНИМАНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

- Рост кибератак привел к тому, что ФСТЭК России вводит новые требования к EDR-системам. Это эволюция защиты конечных точек - от СОВ, МЭ и САВЗ к EDR
- Вендоры активно развивают такие решения, а данные опросов показывают, что пользователи осознают их необходимость и ожидают внедрения EDR
- Высокий спрос на решения NGFW и WAF. Более 40% организаций используют веб-приложения и сайты, что подтверждает актуальность WAF-решений для защиты веб-ресурсов от угроз OWASP Top 10, DDoS и других атак

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Приглашаем в наш телеграм-канал!

Егор Кожемяка

ДИРЕКТОР
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU