ОБЕСПЕЧЕНИЕ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАВРОПОЛЬСКОГО КРАЯ

Заместитель директора
государственного казеного учреждения
“Краевой центр информационных технологий”

Алексей Александрович Писаренко

Железноводск, 2026

ИМПОРТОЗАМЕЩЕНИЕ

Замена зарубежного сетевого оборудования на отечественные аналоги

>500

Заявок по вопросам функционирования отечественной операционной системы

~780

Инструктажей пользователей по работе с отечественным ПО

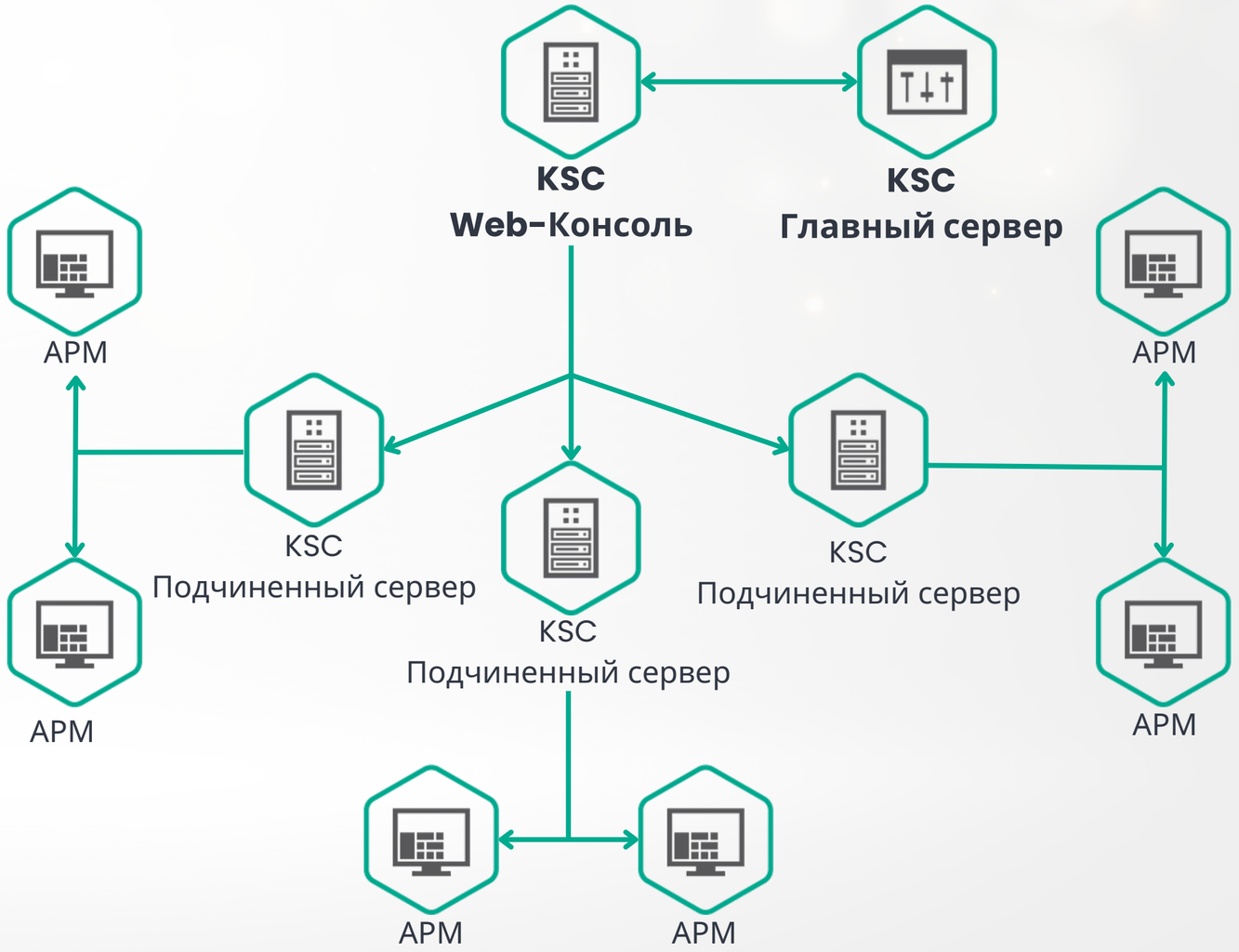
РЕДОС P7 офис

7.3 ➤ 8.1

Обновление операционной системы “РЕД ОС” с миграцией данных и учетных записей

МЕРОПРИЯТИЯ 2025

1. Перевод серверов СЗИ на отечественные средства виртуализации и серверные ОС
2. ViPNet SafePoint и ViPNet EndPoint Protection на рабочие места во всех ОГВ и подведомственных учреждениях
3. Древовидная структура управления серверами Kaspersky Security Center



ЦЕНТР **МОНИТОРИНГА**

Обработано **4 378 818 142** события ИБ

Заблокировано **416 761** потенциально опасных IP адреса

Отражено более **1900** атак

МЕРОПРИЯТИЯ 2025

4 **BUGBOUNTY** для портала госуслуг СК и портала “Электронные журналы и дневники”

5 Сектор обеспечения ИБ успешно прошел **4** проверки регуляторов

6 Заключено соглашение на сопровождение межведомственного центра бухгалтерского обслуживания

LOW

Проблемы безопасности с минимальным практическим воздействием. Самая низкая выплата

MEDIUM

Уязвимость с ограниченным воздействием. Часто требует специфичных условий или даёт доступ к не самой чувствительной информации.

HIGH

Серьёзная уязвимость, которая обходит ключевые, важнейшие механизмы защиты и является прямой угрозой конфиденциальности или целостности данных.

CRITICAL

Самый серьёзный уровень. Уязвимости такого типа — прямая угроза бизнесу и безопасности данных.

КАТЕГОРИИ CTF

WEB

Анализ и эксплуатация уязвимостей веб-приложений. Поиск уязвимостей: SQL-инъекции, XSS или обход аутентификации

FORENSIC

Нахождение скрытых данных в файлах, восстанавление удалённых данные или анализировать сетевые дампы.

CRYPTO

Расшифровка или взлом зашифрованных данных.

REVERSE

Анализ программного обеспечения с целью понять его внутреннюю структуру, алгоритмы и логику работы.

OSINT

Сбора, анализа и интерпретации информации, которая находится в открытом доступе

МЕРОПРИЯТИЯ 2025

7

Пилотный запуск Phishman. Рассылка фишинговых писем для выявления уязвимых мест. Лекции по кибергигиене

8

Анализ веб-ресурсов органов исполнительной власти: сбор cookie, наличие SSL сертификатов, политика сбора данных

9

Собрана команда CTF для участия в киберучениях. Обсуждение создания собственной платформы для проведения соревнований ИБ

2026

ЗАПЛАНИРОВАНО

Технологическая независимость и повышение уровня защищенности

ЦОД	EPP и SF	8.1
Доведены средства на модернизацию центра обработки данных на отечественных компонентах	Обновление серверов и агентов до новой версии. Подключние к центру мониторинга	Перевод АРМ на отечественную ОС РЕД ОС 8.1

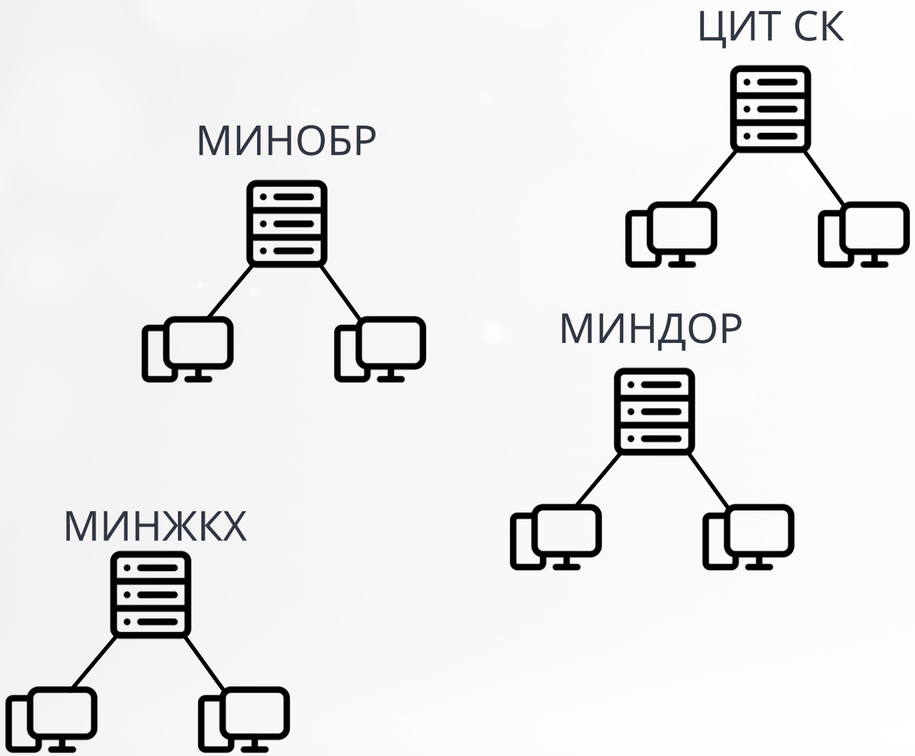
ЕДИНАЯ ДОМЕННАЯ СТРУКТУРА

Главный контроллер домена

Контроллер домена

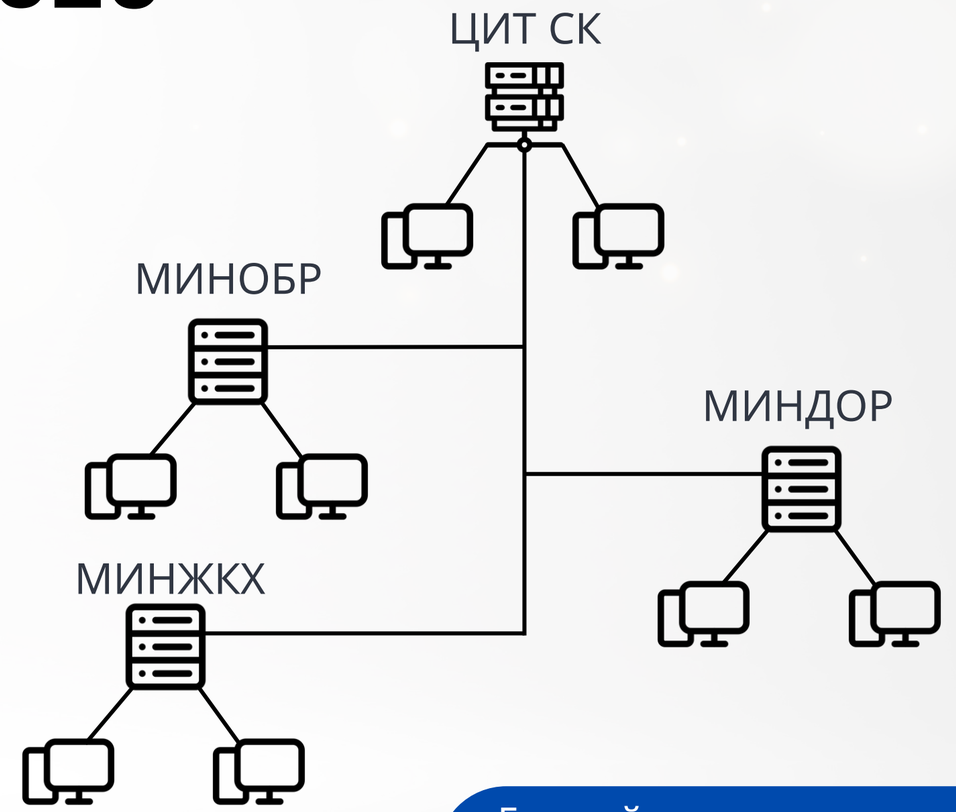
АРМ

2025



В каждом ОГВ свой контроллер домена, нет централизованного управления

2026



Единый домен позволит оперативно внедрять обновления ПО, закрывать уязвимости ИБ

ЦЕНТРАЛИЗОВАННАЯ **ЗАКУПКА**

Закупка, проводимая каждый год для стабильной и безопасной работы органов государственной власти и их подведомственных организаций

Средства антивирусной защиты

Средства анализа защищенности

XSpider

Сканер-ВС
анализ защищенности

БЛАГОДАРЮ ЗА ВНИМАНИЕ

aa.pisarenko@cit-sk.ru

Железноводск, 2026