softline ОБЛАКО

Строим надежный фундамент для ваших данных:
ISOC и защита данных по 152-ФЗ

Роман Зацепин

Менеджер продукта облачных сервисов безопасности Софтлайн Облако

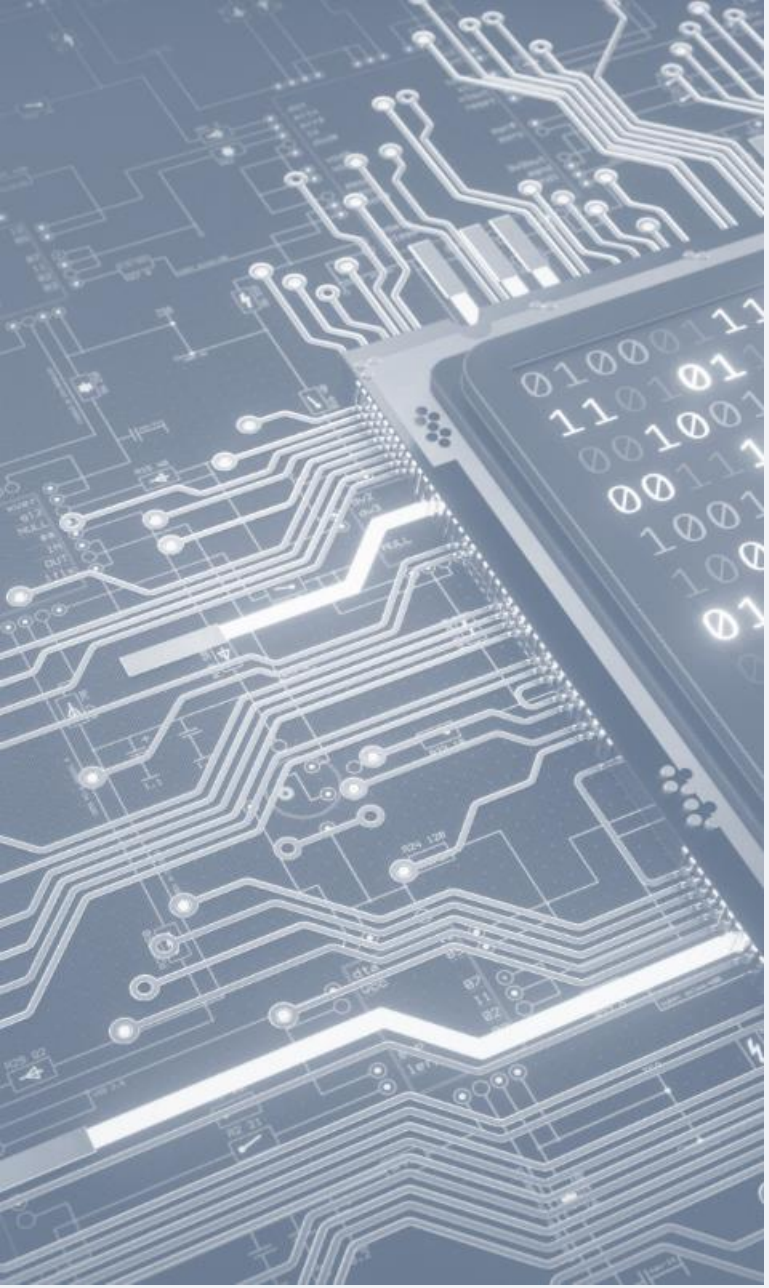
ISOC – Security Operation Center от Infosecurity, ГК Softline

ISOC - сервис круглосуточного мониторинга, выявления и предотвращения киберугроз. Доступен в вариантах стандартного SOC и SOC Mini для гипервизора облака Softline.

Центр предназначен для мониторинга, обнаружения, анализа и реагирования на киберинциденты в информационных системах организации.

Security Operation Center концептуально состоит **из трёх составляющих:**

1. **Люди** – ИБ и ИТ специалисты Infosecurity
2. **Программное обеспечение и технологии** – SIEM и IRP/SOAR-системы
3. **Процессы и регламенты** – выстроенные системы оповещения и реагирования



Чем поможет ISOC

ЗАДАЧИ, КОТОРЫЕ РЕШАЕТ SOC:

- Снижение рисков ИБ
- Сокращение величины ущерба от инцидентов ИБ
- Выполнение требований регуляторов
- Повышение уровня зрелости ИБ компании
- Снижение нагрузки на ИБ и ИТ персонал

ПРОБЛЕМЫ В ЧАСТИ ИБ:

- Недостаточная эффективность превентивных средств защиты из СЗИ - нет единого видения инцидента ИБ
- Отсутствие регламентированных и отлаженных процессов реагирования
- Недостаточная численность и квалификация внутренней команды
- Размытые зоны ответственности между ИТ и ИБ
- Большой поток ложных срабатываний

ISOC 2026

- 50+ экспертов в команде
- 10+ лет экспертизы и опыта
- Мониторинг и реагирование **24x7**
- Расследование сложных инцидентов
- Собственный Threat intelligence
- Гибкий SLA и условия оплаты
- 100+ поддерживаемых источников
- **500+** собственных сценариев детектирования
- **30+** сценариев автоматического реагирования
- Гарантированная доступность платформы **99%**
- Стоимость владения **в ~4 раза** ниже in-house SOC

Как работает ISOC

События с источников клиента

Автоматический Мониторинг

Создание заявки
и email/tg оповещения

Реагирование

(первичный анализ и верификация)

Первичный анализ
и обработка инцидента

Верификация,
оповещение, базовые
рекомендации

Подключение
эксперта к онлайн-
анализу

Подробный анализ
и обработка инцидента

Реагирование

(плейбуки для типовых
инцидентов)

Консультационное реагирование – рекомендации по контрмерам для самостоятельного применения Заказчиком

Реагирование

(сложные инциденты ИБ,
не по плейбукам)

Расширенная поддержка, консультации, сопровождение специалистов заказчика по применению выдаваемых рекомендаций.

Состав базового сервиса

ВИЗУАЛИЗАЦИЯ И ОТЧЕТНОСТЬ

- Web-интерфейс SIEM
- Web-интерфейс IRP
- Чат-бот в telegram
- Чат по реагированию
- Регулярные встречи с командой
- Стандартный набор отчетов/дашбордов

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

- Типовой регламент реагирования на инциденты
- Частичная автоверификация + авторекомендации
- Консультационное реагирование на инциденты
- Стандартная схема коммуникации
- Расследование инцидентов в объеме событий в SIEM
- Реагирование L3 (сложные инциденты, не по плейбукам)

АВТОМАТИЧЕСКИЙ МОНИТОРИНГ И ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ ИБ

- Стандартная облачная архитектура
- Канал VPN AES 256
- Базовый набор источников
- Базовый набор правил корреляции
- Обогащение IoC из платных подписок
- Хранение событий – 3 мес.

Необходимый и достаточный функционал для управления инцидентами

Дополнительные опции сервиса

ВИЗУАЛИЗАЦИЯ И ОТЧЕТНОСТЬ

- Доработка базовых отчетов/дашбордов
- Разработка кастомных отчетов/дашбордов
- Подготовка нестандартных отчетов (в т.ч. аналитических)
- Дополнительные регулярные встречи с командой SOC
- Передача информации в НКЦКИ/ФинЦЕРТ

РАССЛЕДОВАНИЯ И РАСШИРЕННАЯ АНАЛИТИКА

- Расследование инцидентов
- Аналитика и экспертные консультации
- Проактивный поиск угроз

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

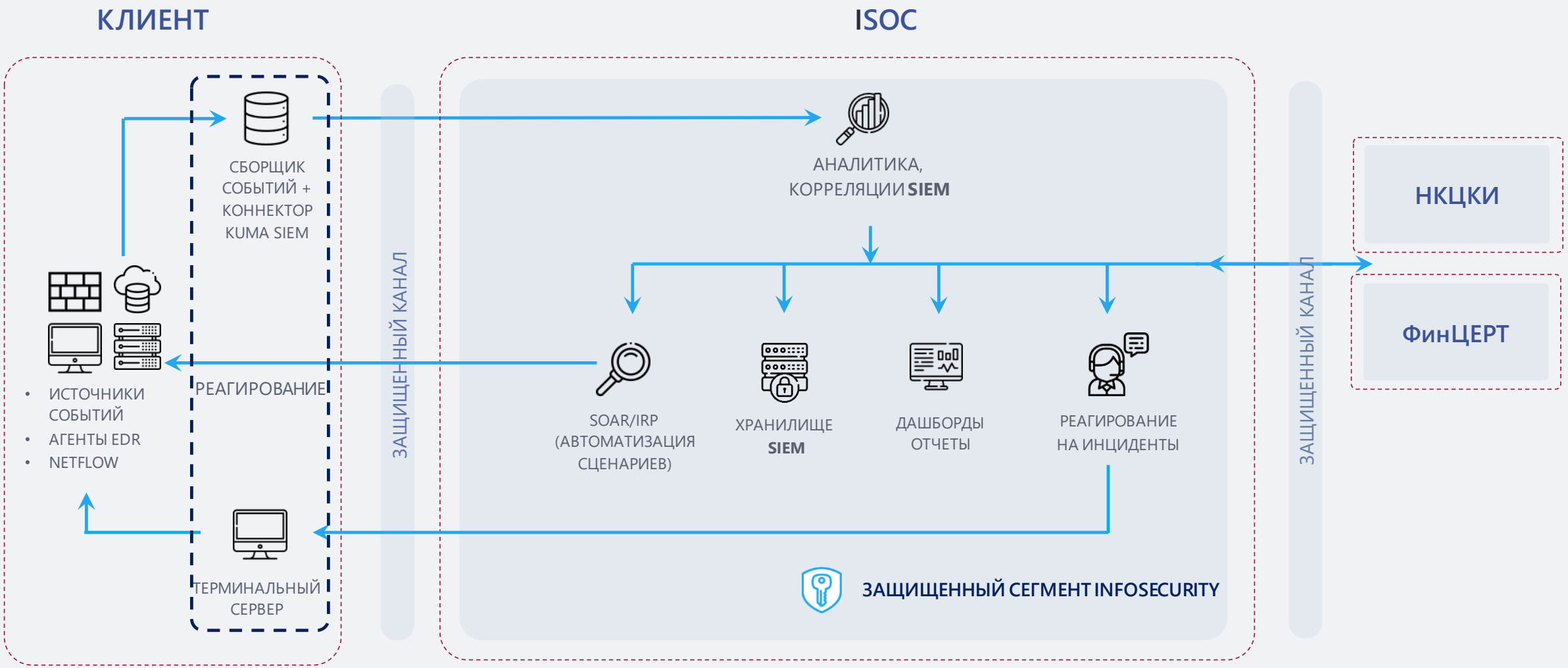
- Кастомизация плейбуков
- Применение контрмер силами аналитиков SOC
- Подключение сценариев автоматического реагирования
- Разработка кастомных сценариев автоматического реагирования
- Интеграции с системами клиента (ITSM, почта, CMDB и тд)

АВТОМАТИЧЕСКИЙ МОНИТОРИНГ И ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ ИБ

- Подключение *дополнительных типовых* источников
- Подключение *дополнительных нетиповых* источников
- Настройка источников силами инженеров ИС
- Канал ГОСТ СКЗИ
- Расширенный мониторинг с помощью KEDR MSSP
- Разработка кастомных правил корреляции
- Расширенный срок хранения событий

Расширенные возможности для решения дополнительных задач

ISOC – архитектура SOC as a Service



Интерфейсы сервиса ISOC

Автоматические оповещения (telegram/e-mail) о выявленных подозрениях на инциденты ИБ

Телефонные звонки ответственным лицам при верификации особо критичных подозрений на инциденты ИБ

Личный кабинет для просмотра событий ИБ, алертов, инцидентов, этапов обработки инцидента ИБ (в т.ч. детали и рекомендации)

Интеграция с ITSM системами клиента, автоматическое реагирование на инциденты ИБ

Рекомендации по самостоятельному разрешению инцидента ИБ и минимизации последствий – по согласованным каналам связи

Регулярные статистические отчеты по событиям ИБ, детальные отчеты по каждому инциденту ИБ и его разрешению

Автоматизация реагирования на инциденты ИБ

Единое окно контроля за циклом управления и реагирования на инциденты ИБ

Сокращение времени реагирования на типовые инциденты ИБ (снижение MTTR до 20 раз!)

Упрощение процессов и автоматизация рутинных задач

Интеграция с прочими сервисами на уровне плейбуков (в т.ч. Security Awareness)

Соответствие требованиям

INFOSECURITY:

- Лицензия ФСТЭК России на деятельность по ТЗКИ
- Лицензия ФСБ России на работу с СКЗИ
- Соглашение о взаимодействии с НКЦКИ
- Соглашение о взаимодействии с ФинЦЕРТ

ISOC 3.0:

- IRP/SOAR сертифицирована ФСТЭК по 4 УД
- SIEM сертифицирована ФСТЭК по 4 УД

Команда SOC

50+ экспертов в команде мониторинга и реагирования на инциденты ИБ

Опыт работы в ИБ – от 2 лет

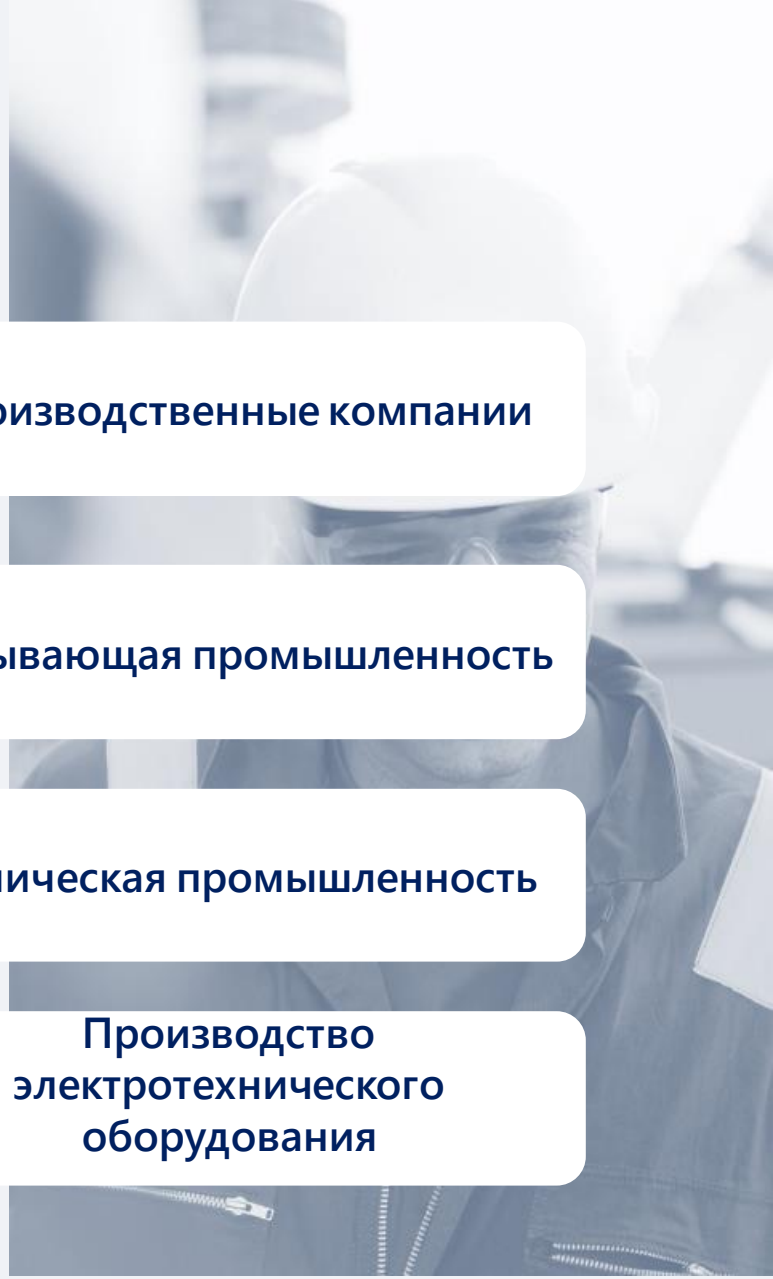
Более 80% сотрудников с профильным образованием по ИБ и международными сертификатами

Регулярные совместные учения с командой пентеста

С ISOC взаимодействуют **100+ специалистов** по различным направлениям ИБ и ИТ

Клиенты ISOC

- Международные компании
- Дочерние общества крупных холдингов
- Производственные компании
- Банки и Финансы
- Страхование
- Добывающая промышленность
- Retail & FMCG
- Информационные технологии
- Химическая промышленность
- Производство автомобилей
- Девелопмент и строительство
- Производство электротехнического оборудования



Страхование рисков ИБ в составе SOC Infosecurity

Покрытие затрат на восстановление после инцидента через партнерскую программу страхования

Компенсация затрат

на расследование, локализацию, предоставление «чистой инфраструктуры», СЗИ, восстановление критичных систем и данных, консультации

Минимизация простоя

Экстренное восстановление для скорейшего возвращения бизнеса к работе

Возможность расширения страховки

Формирование индивидуальных предложений по полному покрытию рисков ИБ на выгодных условиях для клиентов SOC

Экспертиза из «единого окна»

Предоставим специалистов с компетенциями по различным направлениям ИБ и ИТ в рамках договора на SOC

Роман Зацепин

Менеджер продукта облачных сервисов безопасности Софтлайн Облако

Roman.Zatsepin@softline.com

cloud.softline.ru

OXYGEN
DATA CENTERS & CLOUDS

Александр Будкин, ИТ-директор OXYGEN

Как работать с ПДн и КИИ

Работа с персональными данными регулируется 152-ФЗ

Категория	Характеристика	Примеры
Общедоступные	Данные, доступные неограниченному кругу лиц. Обрабатываются без согласия, если источник опубликован самим субъектом.	ФИО, должность, рабочий телефон (в справочниках)
Специальные	Наиболее чувствительные. Обработка запрещена кроме случаев, предусмотренных законом.	Раса, национальность, политические взгляды, религия, здоровье, интимная жизнь
Биометрические	Физиологические особенности для идентификации личности. Требуют отдельного согласия на обработку.	Фото, отпечатки пальцев, запись голоса, радужка глаза
Иные	Все остальные данные, не вошедшие в предыдущие категории. Обрабатываются в общем порядке с согласия субъекта.	Адрес проживания, номер телефона, email, место работы, доходы, номер автомобиля

Отраслевая специфика ПДн

- **РИТЕЙЛ И E-COM**

Чаще всего работает с ПДн: ФИО, адрес доставки, телефон, email. Часто есть программа лояльности (история покупок, предпочтения).

- **ФИНТЕХ**

Чаще всего работает с ПДн: паспорт, СНИЛС, ИНН, данные карт, история транзакций. Требования регулятора здесь максимально строгие (ГОСТ Р 57580.1-2017).

- **ПРОМЫШЛЕННОСТЬ**

Чаще всего работает с ПДн сотрудников (кадровый учет, зарплатные проекты), данные пропускной системы.
Реже — данные контрагентов-физлиц.

OXYGEN
DATA CENTERS & CLOUDS

ПЕРСДАННЫЕ – это новая реальность

Их приходится обрабатывать в любой компании

От типа персональных данных и их количества зависит уровень защищенности компании

Тип ИСПДн	Категория субъектов	Количество субъектов	1 тип угроз	2 тип угроз	3 тип угроз
Специальные	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее 100 000	УЗ 1	УЗ 2	УЗ 3
Биометрические	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее 100 000	УЗ 1	УЗ 2	УЗ 3
Иные	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 1	УЗ 3	УЗ 4
		Менее 100 000	УЗ 1	УЗ 3	УЗ 4
Общедоступные	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 2	УЗ 3	УЗ 4
		Менее 100 000	УЗ 2	УЗ 3	УЗ 4

Три типа угроз

Угрозы 1-го типа:

недекларированные возможности в системном ПО (ОС, драйверы, BIOS).

Угрозы 2-го типа:

недекларированные возможности в прикладном ПО (офисные программы, 1С, корпоративные системы).

Угрозы 3-го типа:

недекларированные возможности отсутствуют.

Кто определяет, какому УЗ нужно соответствовать?

УЗ определяет Оператор ПДн (то есть вы сами) на основании модели угроз.

МОДЕЛЬ УГРОЗ > оценивает актуальные кибератаки, наличие инсайдеров и типы уязвимостей.

Формула:

Тип ПДн + Кол-во субъектов + Модель угроз (и типы угроз) = Уровень Защищенности

Как именно защищать ПДн?

№ пп	Содержание мер по обеспечению безопасности ПДН	Всего	УЗ-4	УЗ-3	УЗ-2	УЗ-1
I	Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	6	5	5	6	6
II	Управление доступом субъектов доступа к объектам доступа (УПД)	17	10	12	13	13
III	Ограничение программной среды (ОПС)	4	0	0	1	2
IV	Защита машинных носителей персональных данных (ЗНИ)	8	0	1	3	3
V	Регистрация событий безопасности (РСБ)	7	4	4	5	5
VI	Антивирусная защита (АВЗ)	2	2	2	2	2
VII	Обнаружение вторжений (СОВ)	2	0	0	2	2
VIII	Контроль (анализ) защищенности персональных данных (АНЗ)	5	1	4	5	5
IX	Обеспечение целостности информационной системы и персональных данных (ОЦЛ)	8	0	0	2	2
X	Обеспечение доступности персональных данных (ОДТ)	5	0	0	2	3
XI	Защита среды виртуализации (ЗСВ)	10	2	5	8	8
XII	Защита технических средств (ЗТС)	5	2	2	2	2
XII	Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	20	1	2	5	6
XIV	Выявление инцидентов и реагирование на них (ИНЦ)	6	0	0	6	6
XV	Управление конфигурацией информационной системы и СЗПДн (УКФ)	4	0	4	4	4
Итого		**109**	**27**	**41**	**66**	**69**

Законодательство предписывает конкретный набор мер для УЗ-1, 2, 3, 4 (Приказ ФСТЭК №21).

OXYGEN
DATA CENTERS & CLOUDS

Например, вы определили, что попадаете под требования УЗ-1

Можно построить инфраструктуру самим? Можно, но...

Матрица распределения ответственности

Инфраструктура оператора	Инфраструктура как услуга	Платформа как услуга	Программное обеспечение как услуга
Приложения	Приложения	Приложения	Приложения
Данные	Данные	Данные	Данные
Среда выполнения	Среда выполнения	Среда выполнения	Среда выполнения
Связующее программное обеспечение	Связующее программное обеспечение	Связующее программное обеспечение	Связующее программное обеспечение
Операционная система	Операционная система	Операционная система	Операционная система
Платформа виртуализации	Платформа виртуализации	Платформа виртуализации	Платформа виртуализации
Аппаратная платформа	Аппаратная платформа	Аппаратная платформа	Аппаратная платформа
Система хранения данных	Система хранения данных	Система хранения данных	Система хранения данных
Сетевая инфраструктура	Сетевая инфраструктура	Сетевая инфраструктура	Сетевая инфраструктура
Оператор		Поставщик услуг	

На инфраструктурном уровне защиту обеспечивает поставщик услуг

Облачный кластер для 152-ФЗ от OXYGEN

Обеспечиваем максимальную защиту инфраструктуры для размещения ГИС и ИСПДн по классу защищенности **К1 / УЗ1.**

Идентификация и аутентификация субъектов доступа и объектов доступа.

Управление доступом субъектов доступа к объектам доступа.

Ограничение программной среды.

Защита машинных носителей информации.

Регистрация событий безопасности.

Антивирусная защита.

Обнаружение (предотвращение) вторжений.

Контроль (анализ) защищенности информации.

Целостность информационной системы и информации.

Доступность информации.

Защита среды виртуализации.

Защита технических средств.

Облако 152-ФЗ от OXYGEN

Полностью безопасное облако, которое соответствует требованиям федерального закона «О персональных данных»

Максимальный уровень защиты данных

Размещение ГИС и ИСПДн (К1 / У31).

Универсальность в подходах и решениях

Базовые СЗИ + дополнительные средства ИБ.

Управление облачной инфраструктурой

Через межсетевые экраны и криптографические средства в соответствии приказом ФСТЭК РФ № 21 и приказом ФСБ РФ № 378.

Инфраструктура на базе собственного ЦОД TIER III

Уровень ответственности SLA: 99.5 - 99.9%.

Подходит для хранения:

разных типов ИСПДн, включая специальные, биометрические, общедоступные и иные данные сотрудников и несотрудников в количестве более 100 000 субъектов.

Применимость:

- №152-ФЗ: любая организация, обрабатывающая ПДн

Кейс

КРУПНАЯ ОРГАНИЗАЦИЯ В СФЕРЕ СТРАХОВАНИЯ

Гибридная инфраструктура с защищенным облаком 152-ФЗ и частной инсталляцией S3

ПРОБЛЕМАТИКА:

Клиент столкнулся с частыми сбоями и долгой техподдержкой у предыдущего провайдера. Требовалась миграция в защищенное облако для ПДн и надежная связность между разными объектами инфраструктуры.

ЧТО БЫЛО СДЕЛАНО:

- ✓ Миграция в облако 152-ФЗ
- ✓ Защищенное S3-хранилище в соответствии со 152-ФЗ
- ✓ Бэкап всей инфраструктуры
- ✓ Сетевая связность: облако + ресурсы клиента + colocation в ЦОД

РЕШЕНИЕ:

Отказоустойчивая гибридная инфраструктура с физическими и облачными ресурсами в защищенном контуре по требованиям 152-ФЗ и бэкапами.

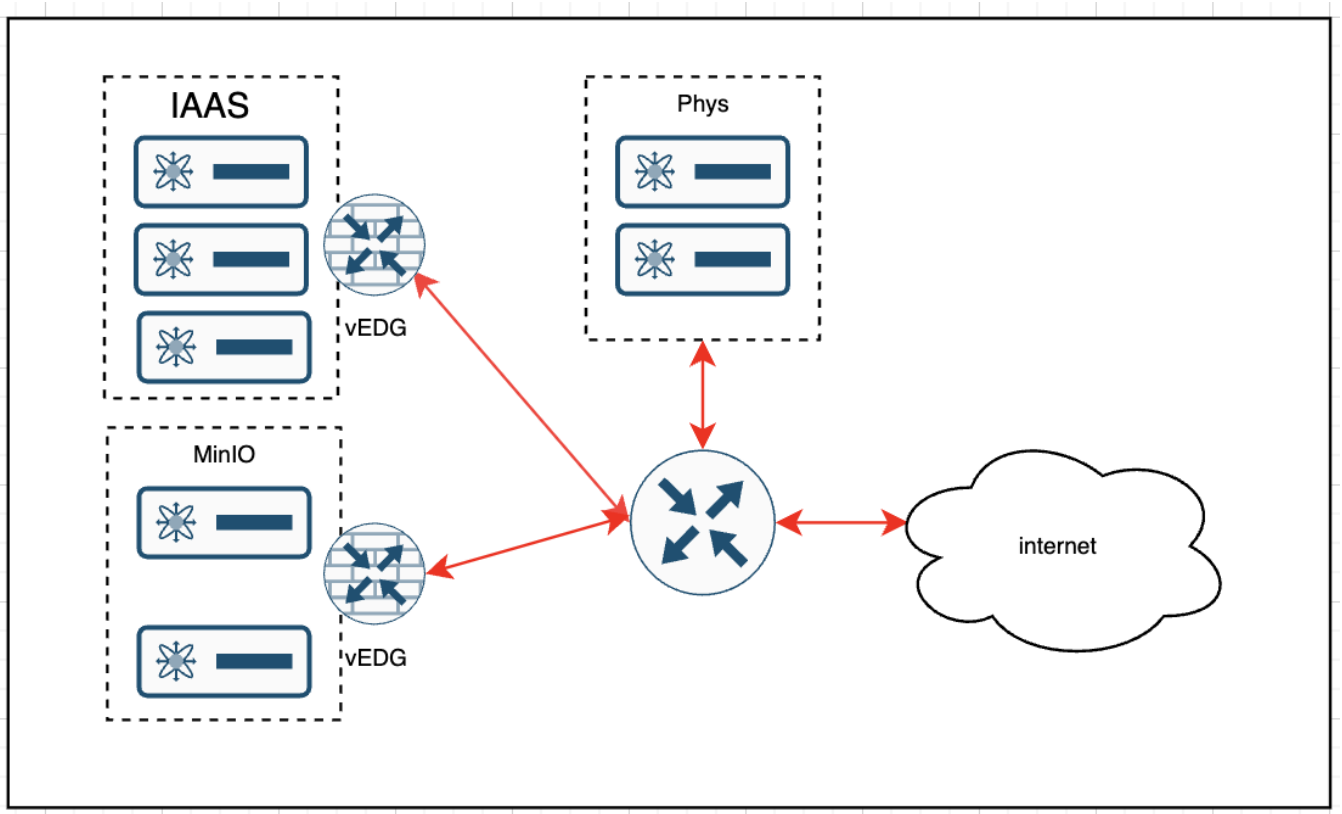
РЕЗУЛЬТАТ:

Клиент полностью закрыл требования 152-ФЗ к обработке ПДн, исключил сбои и утрату критических данных, получил постоянно доступную инфраструктуру.

Кейс

КРУПНАЯ ОРГАНИЗАЦИЯ В СФЕРЕ СТРАХОВАНИЯ

Гибридная инфраструктура
с защищенным облаком 152-ФЗ
и частной инсталляцией S3



Кейс

ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ

Защищенное облако 152-ФЗ для высоконагруженной российской системы ЭДО

ПРОБЛЕМАТИКА:

Клиент хотел оптимизировать ИТ-бюджет, при этом получить стабильный и качественный сервис обслуживания ИТ-инфраструктуры. Главный вызов миграции — «тяжелая» система ЭДО: 5000 активных пользователей и 150 Тб данных.

ЧТО БЫЛО СДЕЛАНО:

- ✓ Провели двухэтапную миграцию: сначала тестовый переезд (убедились, что все ВМ стартуют и успешно работают), затем перевезли продуктивный контур.
- ✓ Настроили кластер под повышенные нагрузки, чтобы 5000 пользователей не «положили» систему.

РЕШЕНИЕ:

Защищенное облако 152-ФЗ для российской системы ЭДО.

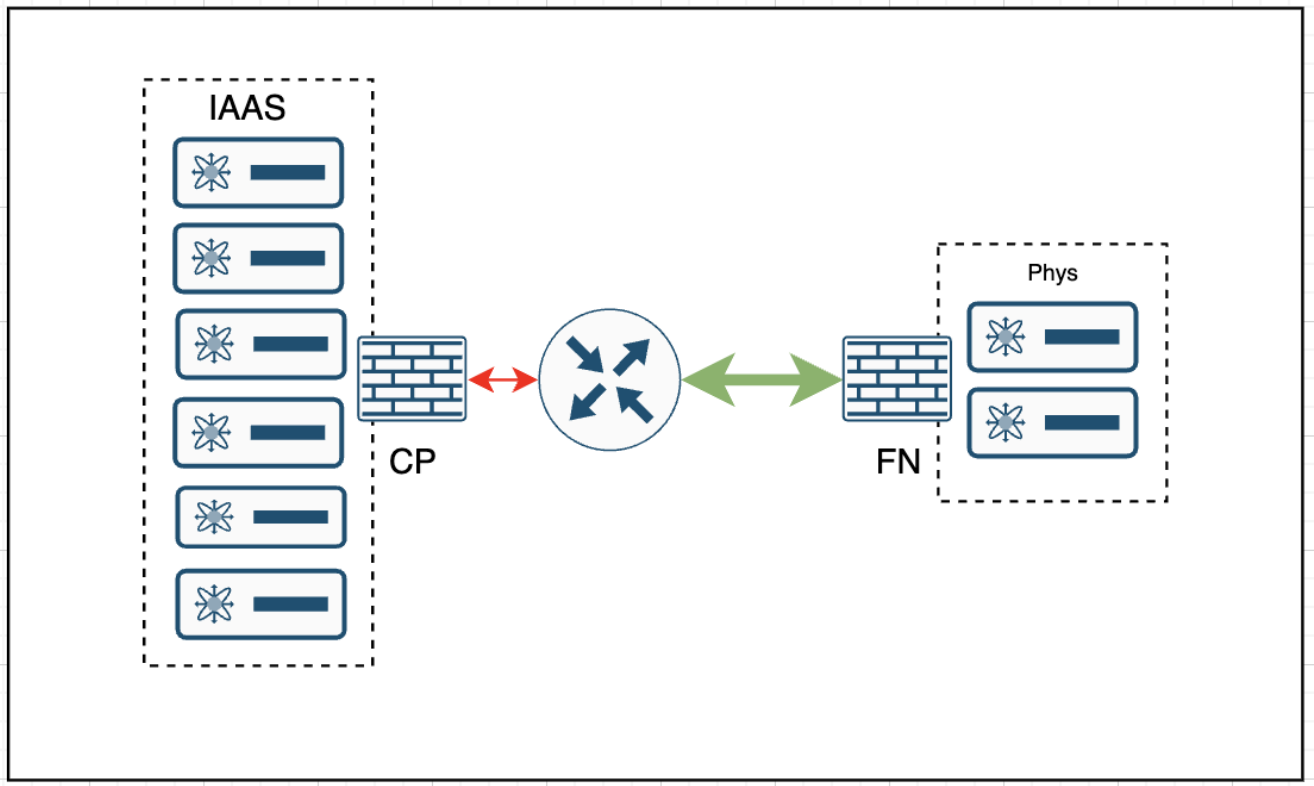
РЕЗУЛЬТАТ:

Полгода стабильной работы системы без тормозов и сбоев. Облачный консалтинг OXYGEN по FinOps помог сократить затраты на облачную инфраструктуру.

Кейс

ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ

Защищенное облако 152-ФЗ для высоконагруженной российской системы ЭДО



Кейс

АВИАКОМПАНИЯ

Защищенное облако 152-ФЗ

ПРОБЛЕМАТИКА:

Клиент пересмотрел ИТ-стратегию на горизонте 5 лет. Ключевая задача — создать современную инфраструктуру, которая выдержит угрозы кибербезопасности и пройдет любой аудит регуляторов на соответствие 152-ФЗ.

ЧТО БЫЛО СДЕЛАНО:

- ✓ Проработали защищенное соединение узлов через ГОСТ-шифрование.
- ✓ Смоделировали сценарии переключения информационных потоков в случае инцидентов.
- ✓ Создали мультисервисную среду с модульной архитектурой — новые сервисы подключаются как готовые блоки, без переработки ядра.

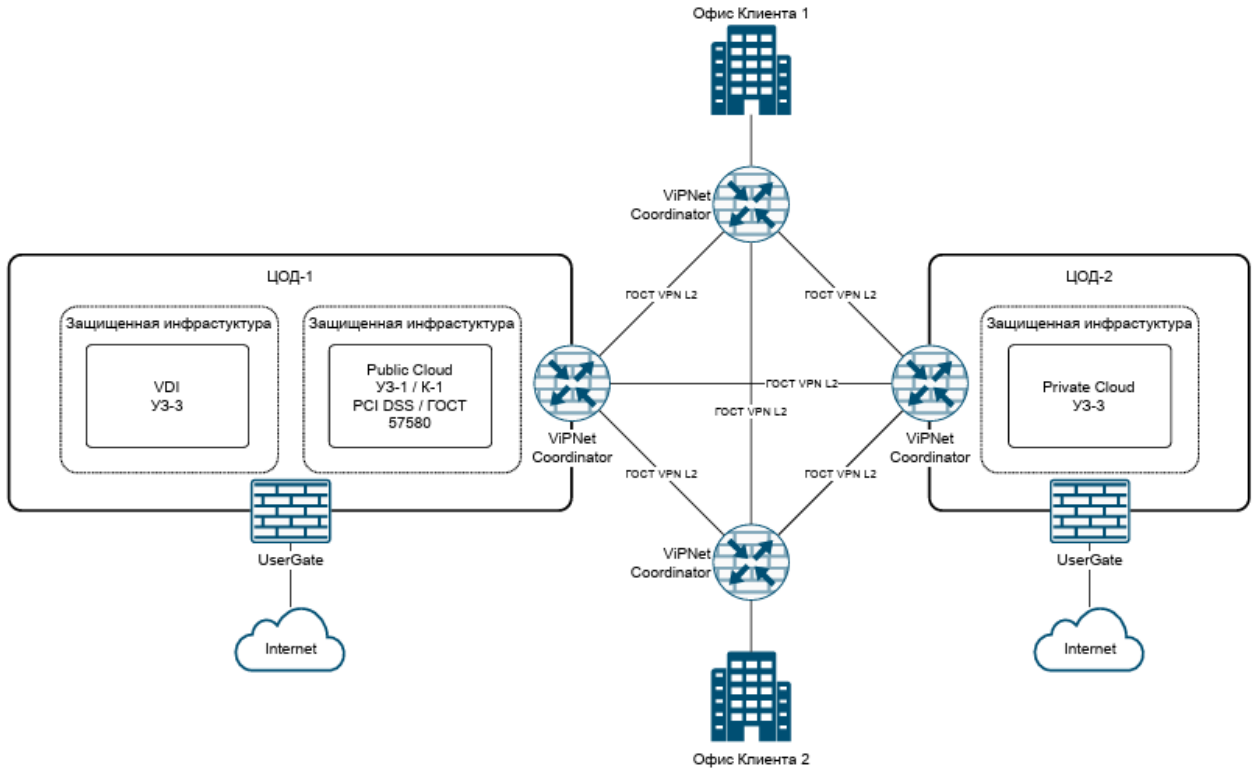
РЕШЕНИЕ:

Клиент получил гибридную георапределенную инфраструктуру, которая полностью соответствует требованиям 152-ФЗ. В защищенном облаке можно безопасно работать с персональными данными, резервные площадки в других городах обеспечивают защиту от сбоев, а мультисервисная архитектура дает фундамент для развития ИТ на годы вперед.

Кейс

АВИАКОМПАНИЯ

Защищенное облако 152-ФЗ



КИИ — это не только ПДн

Это критическая инфраструктура жизненно важных социальных сервисов в стране.

К КИИ помимо ПДн также относятся:

- Конструкторские разработки
- АСУ и ИТ-системы учета договоров, платежей и убытков страхования/перестрахования в банковской сфере
- CRM-системы в области оборонной промышленности
- Любая другая информация ограниченного доступа

ФСТЭК регулирует, относится ли система к КИИ.

Есть перечень типовых объектов КИИ в Распоряжении Правительства Российской Федерации от 26.02.2026 № 360-р.

КИИ и ЗО КИИ — в чем разница?

КИИ >

Критическая информационная инфраструктура

Это совокупность объектов и сетей, которые обеспечивают работу стратегических отраслей: энергетика, здравоохранение, транспорт, финансы, связь и другие. Попадает под действие №187-ФЗ.

ЗО КИИ >

Значимые объекты КИИ

Это конкретные объекты КИИ, которым присвоена категория значимости (1, 2 или 3) по результатам категорирования.

Кейс

ПРОЕКТНОЕ БЮРО

Инфраструктура VDI для НО КИИ

ПРОБЛЕМАТИКА:
Нужно было организовать защищенные рабочие места с графическими процессорами и выполнить требования по размещению НО КИИ — незначимого объекта критической информационной инфраструктуры.

ЧТО БЫЛО СДЕЛАНО:

- ✓ Развертывание платформы VMware Horizon с картами GPU NVIDIA a40.
- ✓ Внедрение подсистемы защиты информации.
- ✓ Проведение оценки эффективности принимаемых мер защиты.

РЕШЕНИЕ:

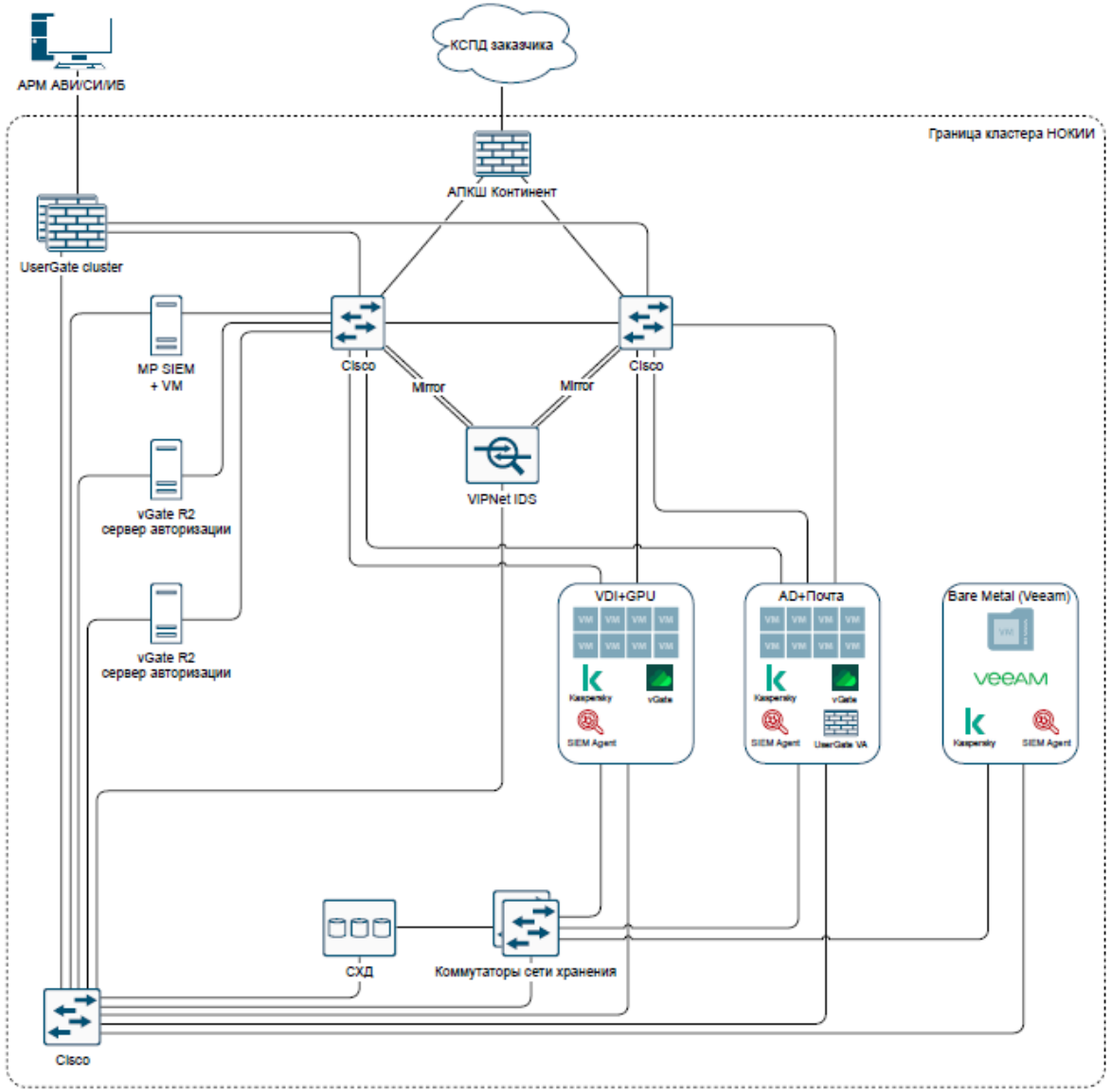
ПАК VDI на базе HORIZON в ЦОД OXYGEN в защищенном контуре ИБ по требованиям Приказа ФСТЭК РФ № 239.

РЕЗУЛЬТАТ:
Клиент успешно открыл новый офис с рабочими местами проектировщиков и обеспечил работу с важными данными под особым контролем со стороны ИБ.

Кейс

ПРОЕКТНОЕ БЮРО

Инфраструктура VDI для НО КИИ



Кейс

ЕЩЕ ОДНО ПРОЕКТНОЕ БЮРО

Реализация отечественного VDI с GPU с соблюдением требований к КИИ

ПРОБЛЕМАТИКА:

Дать технологам мощный инструмент для проектирования и вычислений — и при этом максимально защитить рабочие места на двух площадках и обеспечить защиту с учетом требований к КИИ.

ЧТО БЫЛО СДЕЛАНО:

- ✓ Отдельный кластер внутри защищенного контура.
- ✓ Интеграция с инфраструктурой клиента.
- ✓ Шифрование трафика, выделенный канал.

РЕШЕНИЕ:

Импортозамещенное облако с VDI и GPU-мощностями. Особенность проекта — его георасределенная архитектура.

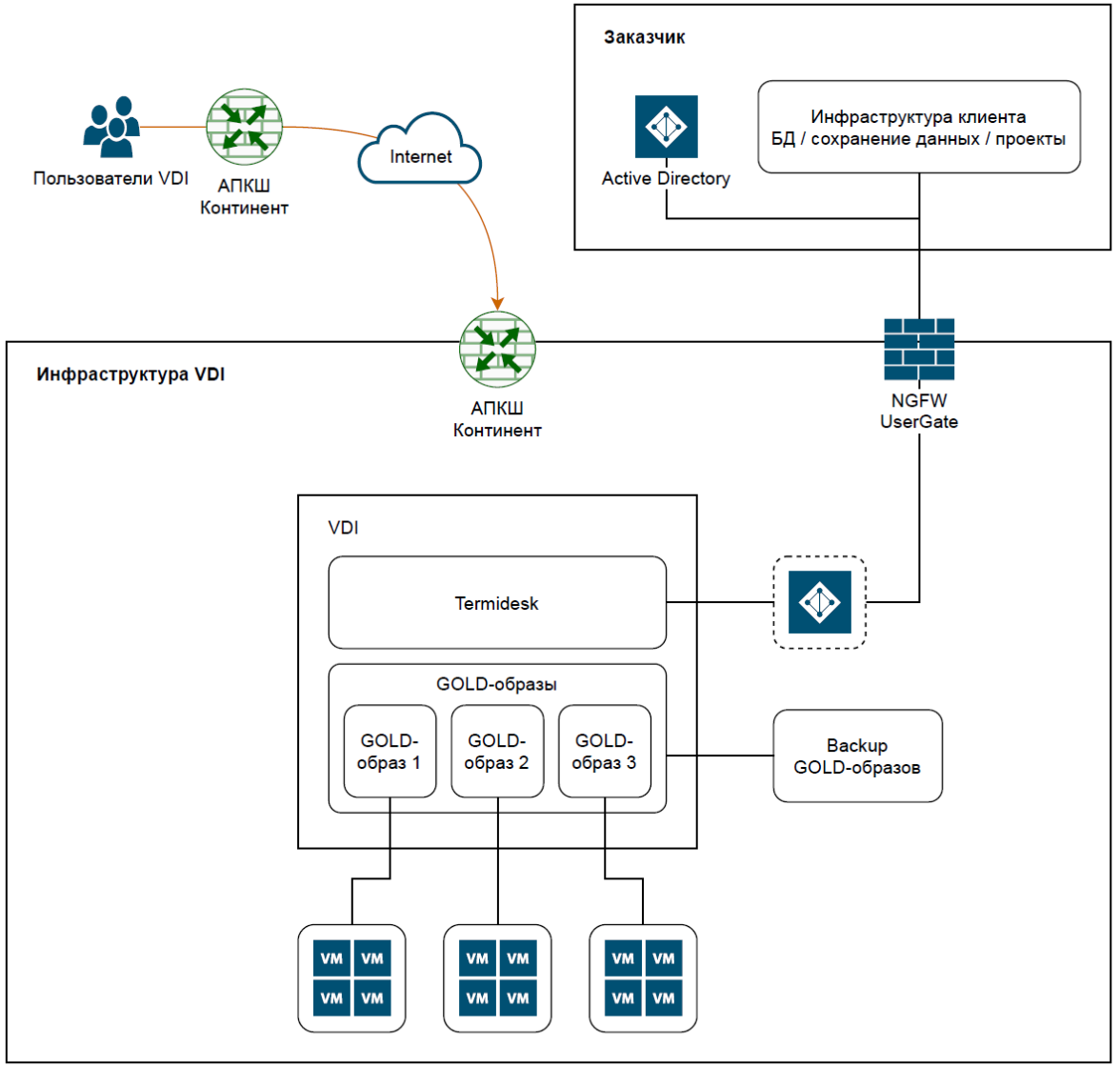
РЕЗУЛЬТАТ:

Технология прошла проверку расстоянием. Данные хранятся в защищенном ЦОДе. Пользователи эффективно работают на удалении 1500 км.

Кейс

ЕЩЕ ОДНО ПРОЕКТНОЕ БЮРО

Реализация отечественного VDI с GPU с соблюдением требований к КИИ



OXYGEN
DATA CENTERS & CLOUDS

КЛАСТЕР ЗО КИИ READY

Импортонезависимое частное облако по 187-ФЗ. Готово к работе

#частное облако

#импортозамещение

Взять в тест

Кластер ЗО КИИ Ready от OXYGEN

подходит для размещения:

ИТ-решений уровня Business Critical

Персональных данных, коммерческой тайны

Высоконагруженных систем

Государственных информационных систем

Полностью отечественный стек для ваших задач

🖥️ **Вычислительная мощность**	**480** vCPU
💾 **Оперативная память**	**4 ТБ** vRAM
⚡ **Производительное хранилище**	**36 ТБ** SSD
🔒 **Защищенный бэкап**	**70 ТБ** (СРК)
🔌 **Сеть**	**10 Гбит/с** (Eltex)

ELTEX ГРАВИТОН RuBackup БРЕСТ СИЛА

Типовой набор средств защиты для ЗО КИИ

- **ПАК ViPNet Coordinator** — шифрование и VPN между объектами
- **ПАК NGFW UserGate** — блокировка атак на уровне приложений
- **MaxPatrol + SIEM** — сбор событий + приоритизация угроз
- **Kaspersky+EDR** — защита ПК + запись для расследований
- **PAM** — контроль админов и привилегированных пользователей
- **MFA** — двухфакторная авторизация (закрывает 80% атак на пароли)

Спасибо за внимание

web: oxygen.cloud
TG: @oxygen_dc

Email: info@o2xygen.ru
Телефон: +7 495 935 72 00

Роман Зацепин

Менеджер продукта облачных сервисов безопасности Софтлайн Облако

Roman.Zatsepin@softline.com

cloud.softline.ru

Инфраструктура. Надёжная. Защищённая.

softline ОБЛАКО