

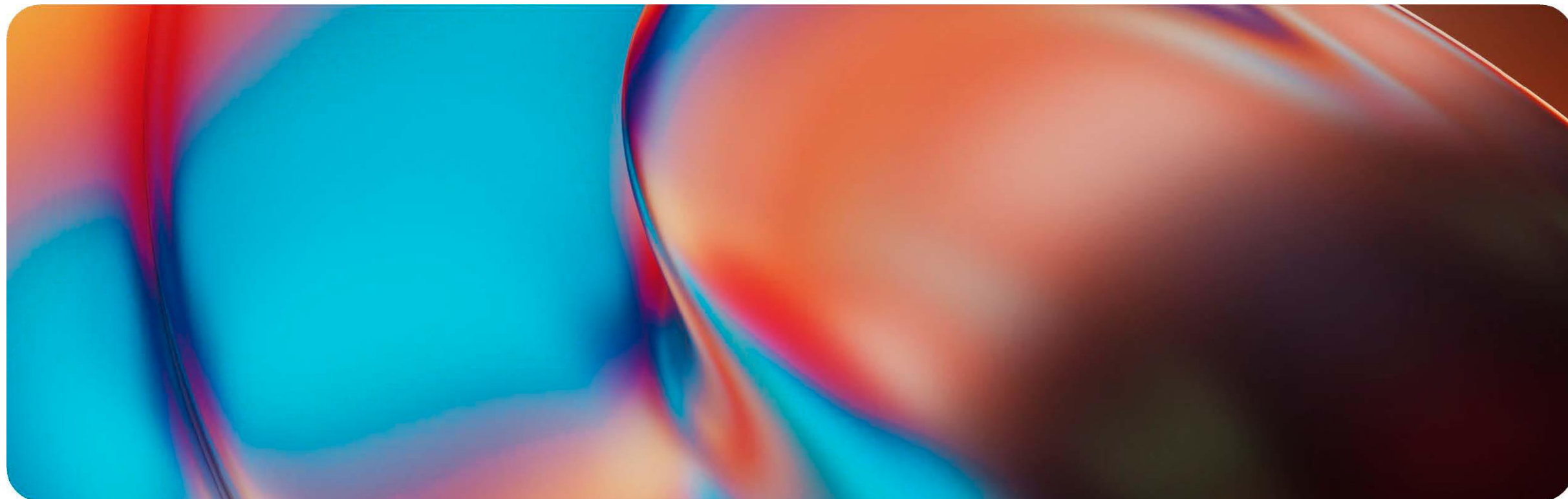


ПРОМЫШЛЕННЫЙ КЛАСТЕР
РЕСПУБЛИКИ ТАТАРСТАН

Ваша проблема

Наше решение

Перечень услуг



ЦИФРОВОЙ ФУНДАМЕНТ БИЗНЕСА





ОТРАСЛЕВОЙ КОММИТЕТ «ИННОВАЦИИ И ПРОИЗВОДИТЕЛЬНОСТЬ ТРУДА»



Руководитель отраслевого комитета
«Инновации и производительность труда»
Промышленный кластер РТ

МУЛЬКОВ
Дмитрий Сергеевич

ОСНОВНЫЕ ЗАДАЧИ ОТРАСЛЕВОГО КОМИТЕТА «ИННОВАЦИИ И ПРОИЗВОДИТЕЛЬНОСТЬ ТРУДА» ПРОМЫШЛЕННОГО КЛАСТЕРА РЕСПУБЛИКИ ТАТАРСТАН

- Развитие новых отечественных технологий и направлений.
- Развитие кооперации и создание инновационных продуктов.
- Привлечение федеральных субсидий и льготного финансирования.
- Развитие кооперации и создание инновационных продуктов.
- Повышение производительности труда, роботизация и автоматизация производственных процессов в промышленных предприятиях.
- Увеличение объемов внедрения ИТ- технологий на рынке Республики Татарстан.
- Выстраивание взаимодействия между организациями разных отраслей и органами законодательной и исполнительной власти.
- Просветительская деятельность.



ПРОМЫШЛЕННЫЙ КЛАСТЕР
РЕСПУБЛИКИ ТАТАРСТАН

О КОММИТЕТЕ

**В состав отраслевого комитета входит 60 участников
из 8 регионов Российской Федерации и 2 стран:**



Республика
Татарстан



Удмуртская
Республика



Ульяновская область



Самарская область



г. Москва



г. Санкт-Петербург



Свердловская область



Пермский край



Китай



Республика Беларусь



Министерство экономического
развития РФ



Министерство экономики РТ



ГАУ «Центр
энергоресурсоэффективных
технологий Республики Татарстан»



ЗАО «Инновационно-
производственный Технопарк
«Идея»



Полномочное представительство
Республики Татарстан в РФ
ООО «ФРИИ Инвест»



Академия Наук РТ



Постоянное представительство
Республики Татарстан в городе
Санкт-Петербурге и Ленинградской
области



Департамент Роскосмос
Департамент координации
производства

Как мы обеспечили стабильную ИТ-инфраструктуру для промышленного предприятия

Клиент

Российская группа приборостроительных компаний. Производит оборудование для ракетно-космической промышленности, навигации, телекоммуникаций.



Задача

Построить отказоустойчивый ЦОД и кампусную сеть для надежной передачи данных

С какими вызовами мы столкнулись

Сложная интеграция

→ Новая система должна была быть совместима с существующей инфраструктурой.

Рост нагрузки

→ Требовалось увеличить скорость передачи данных с 1 до 10 Гбит/с.

Оптимизация ресурсов

→ Упрощение эксплуатации и снижение нагрузки на инженеров

Устаревшее оборудование

→ Инфраструктура не соответствовала современным требованиям

Оптимизация бюджета

→ Максимальная надежность и масштабируемость при разумном распределении бюджета.

Как мы это решили?

Развернули микроЦОД

→ обеспечили надежное охлаждение и электропитание

Выбрали решение от ведущего производителя

→ обеспечили надежность при оптимальном бюджете

Постепенно реализовали проект

→ снизили нагрузку на бюджет, разбив внедрение на этапы

Построили отказоустойчивую сеть

→ повысили надежность на уровне ядра и оборудования

Увеличили скорость передачи данных

→ теперь между объектами передача данных до 10 Гбит/с

Как мы модернизировали ИТ-инфраструктуру промышленного предприятия

Клиент

Крупное предприятие, занимающееся производством и технологическими процессами, требующими стабильных коммуникаций.



Задача

Обновить устаревшую ИТ-инфраструктуру, модернизировав систему корпоративной связи и серверное оборудование.

С какими вызовами мы столкнулись

Устаревшее оборудование

→ Используемая система телефонии не соответствовала современным требованиям, возникали сбои..

Минимизация простоев
→ Производственный процесс нельзя было прерывать на длительное время.

Сложность интеграции

→ Требовалось сохранить существующую инфраструктуру и плавно внедрить обновления.

Оптимизация бюджета

→ Замена всей инфраструктуры была нерентабельной, нужно было точечное обновление.

Как мы это решили?

Обновили систему корпоративной связи
→ Перенесли телефонную инфраструктуру на актуальную версию, повысив стабильность.

Автоматизированный переход
→ Провели автоматическую замену программного обеспечения на IP-телефонах без остановки работы..

Интеграция с существующими системами
→ Обеспечили совместимость новой инфраструктуры со старыми решениями предприятия.

Резервные решения для отказоустойчивости
→ Настроили систему аварийного переключения каналов связи для обеспечения бесперебойной работы.

В рамках инженерной инфраструктуры создаем:



Системы
бесперебойного
электропитания



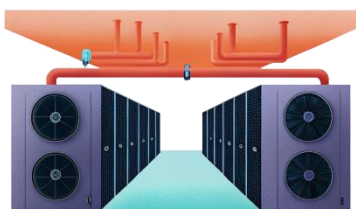
Проектно-
исследовательские
работы



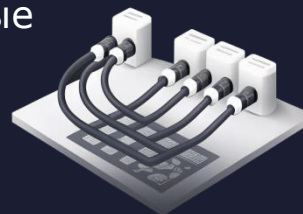
Управляемость
и безопасность



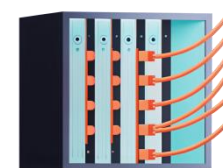
Системы
поддержания
микроклимата



Структурированные
кабельные
системы



Пассивное
телекоммуникационное
оборудование



Что такое **информационная безопасность**?

Цифровой щит вашего бизнеса, который защищает данные, системы и процессы от угроз, обеспечивая стабильность и доверие клиентов.



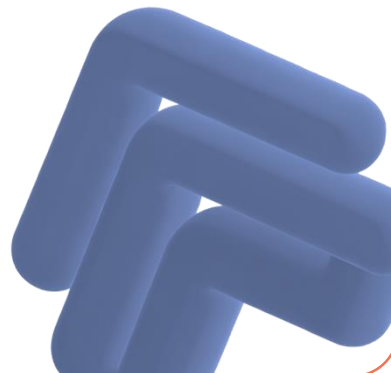
Почему это важно?

Без информационной безопасности бизнесу угрожают кибератаки, утечки данных и репутационные риски.

23,6 %

доля российских компьютеров автоматизированных систем управления (АСУ), на которых были заблокированы вредоносные объекты*

*По данным экспертов
Kaspersky ICS CERT



144

*По статистике DLBI
(сервис мониторинга
утечек данных)

Утечки данных произошло из компаний в первом полугодии 2024

99

млрд. руб.

*По данным МВД

Ущерб от IT-преступлений в 1 полугодии 2024. Всего было зафиксировано 577 тыс. IT-преступлений

на **32** %

*По данным компании
Нейроинформ

возросло использованием вирус-шифровальщиков в России в 3 квартале 2024

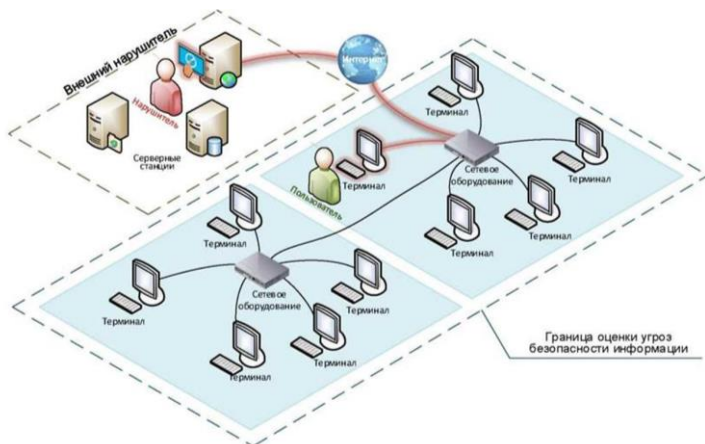


Главная угроза — не там, где вы её ожидаете

Миф или реальность?

Миф

Основные угрозы приходят извне



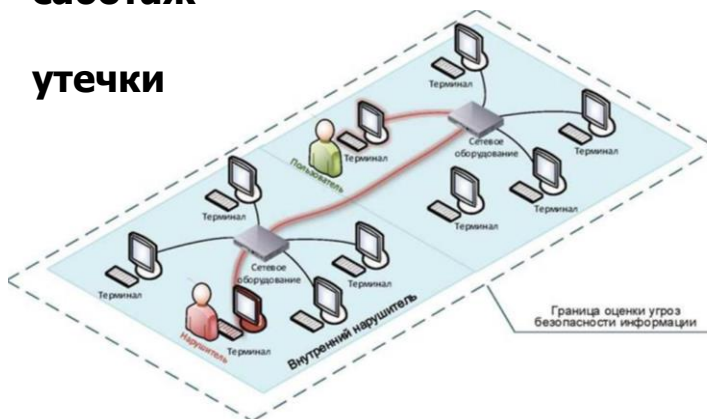
Реальность

Внутренние угрозы составляют большую часть инцидентов.

ошибки сотрудников

саботаж

утечки



78 %

[По статистике NANGS.ORG](https://nangs.org)

промышленных компаний столкнулись с внутренними инцидентами

66 %

[По данным Searchinform](https://searchinform.ru)

организаций фиксировали утечки по вине сотрудников

51 %

[По статистике Positive Technologies](https://positive-technologies.ru)

успешных атак начинались с фишинговых писем

Формула комплексной безопасности

Организационная защита информации



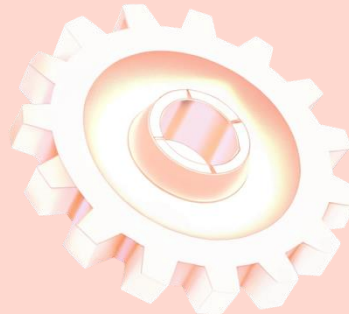
+

Техническая защита от внутренних и внешних угроз



+

Автоматизация бизнес-процессов информационной безопасности



+

Соответствие требованиям регуляторов



Обучение кибербезопасности для всех категорий сотрудников

Для всех сотрудников

- Основы цифровой безопасности: защита данных, распознавание угроз
- Безопасное поведение в сети, предотвращение утечек информации
- Фишинг, социальная инженерия и методы защиты

Для технических специалистов
(разработчиков, **DevOps**, администраторов)

- Безопасная разработка ПО: защита от уязвимостей и методы защиты
- Интеграция ИБ в процессы DevOps
- Анализ и защита инфраструктуры

Для специалистов по ИБ

- Тестирование на проникновение и анализ защищенности
- Управление киберугрозами и расследование инцидентов
- Практические тренировки в киберполигонах

Киберполигон

Практические киберучения, моделирование атак и защита в реальном времени



Мы сотрудничаем с крупными образовательными учреждениями

Киберобучение решает следующие задачи:

Освоение техник и тактик проведения тестирования на проникновение, методов защиты от компьютерных атак

Тестирование средств защиты на виртуальной инфраструктуре предприятий

Повышение навыков реагирования и расследования компьютерных инцидентов



Киберобучение по ИБ и моделированию инфраструктур предприятия





Роботизация

Основные типы промышленных роботов



Шарнирно-сочлененные роботы

Паллетирование, сварка, покраска, наплавка, сборка



Декартовы
(линейные/портальные) роботы

Паллетирование



Параллельные роботы

Упаковка, сборка,
погрузочно-разгрузочные работы



SCARA-Роботы

Сортировка, упаковка, сборка,
пайка



Цилиндрические роботы

Точечная сварка, сборочные
операции, управление машинами
литья под давлением



Промышленные транспортные
роботы

Транспортировка