GST: ИТ-компетенции для промышленности

Группа Компаний «GST» – надежный партнер в сфере информационной безопасности и ИТ-решений

С 2005 года мы обеспечиваем предприятия передовыми технологиями защиты информации и цифровой инфраструктуры. Наша команда объединяет более 70 специалистов – инженеров, аудиторов и архитекторов ИБ, работающих в **Москве, Санкт-Петербурге, Саранске, Самаре** и реализующих проекты по всей России.

Ключевые направления:

01 Информационная безопасность

02 ИТ-инфраструктура

03 Платформа для создания диалоговых тренажёров

04 Автоматизированные складские системы

КАТЕГОРИРОВАНИЕ И ЗАЩИТА КИИ

Цели:

- Определить критичные объекты КИИ
- Категорировать и разработать СОИБ
- Обеспечить соответствие требованиям ФЗ-187, ФСТЭК и ФСБ

Ключевые этапы:

1. **Защита промышленного сегмента (SCADA/ПЛК)**
   → ViPNet IDS, ARMA Industrial, KICS: изоляция, инвентаризация, мониторинг
2. **Защита IT-инфраструктуры**
   → Kaspersky EDR/UMA, PT Sandbox, Secret Net, Passwork: защита рабочих мест
3. **Сегментация сети**
   → Внедрение DMZ, межсетевые экраны: UserGate, Континент, MaxPatrol SIEM
4. **Обучение и контроль персонала**
   → Инструменты: Phishman, Traffic Monitor, разработка ОРД
5. **Резервное копирование и восстановление**
   → IRP, защита логов, контроль доступа (DallasLock)
6. **Соблюдение законодательства**
   → Аттестация, аудит, защита ПДн и КИИ

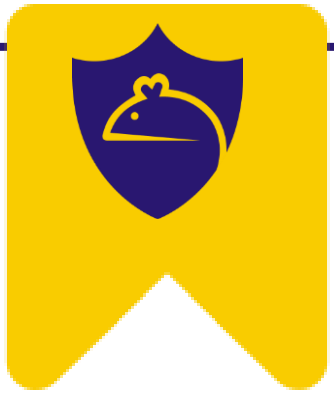
Статистика:

70%
предприятий не завершили категорирование КИИ

60%
атак на КИИ происходят из-за отсутствия СОИБ

80%
проверок выявляют несоответствие документации

Результат:



- Завершенное категорирование объектов КИИ
- Внедрённая СОИБ на уровне ЗОКИИ
- Готовность к аттестации и проверкам ФСТЭК/ФСБ

КОМПЛЕКСНАЯ ЗАЩИТА IT И OT-ИНФРАСТРУКТУРЫ

Цели:

- Сегментировать IT и OT-сети
- Защитить SCADA/ПЛК и рабочие станции
- Устранить риски фишинга и несанкционированного доступа

Ключевые этапы:

1. **Защита промышленного сегмента (SCADA/ПЛК)**
   → ViPNet IDS, ARMA Industrial, KICS: изоляция, инвентаризация, мониторинг
2. **Защита IT-инфраструктуры**
   → Kaspersky EDR/UMA, PT Sandbox, Secret Net, Passwork: защита рабочих мест
3. **Сегментация сети**
   → Внедрение DMZ, межсетевые экраны: UserGate, Континент, MaxPatrol SIEM
4. **Обучение и контроль персонала**
   → Инструменты: Phishman, Traffic Monitor, разработка ОРД
5. **Резервное копирование и восстановление**
   → IRP, защита логов, контроль доступа (DallasLock)
6. **Соблюдение законодательства**
   → Аттестация, аудит, защита ПДн и КИИ

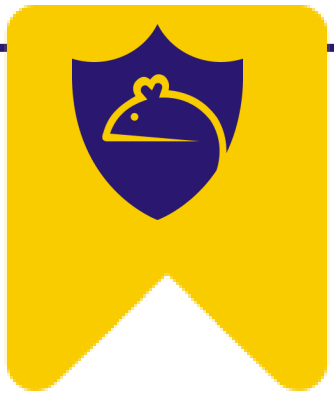
Статистика:

65%
атак на SCADA начинаются с IT-сегмента

50%
предприятий не проводят регулярное обучение по ИБ

50%
сотрудников не знают базовых принципов ИБ

Результат:



- Комплексная защита IT и OT
- Снижение числа инцидентов и фишинг-атак
- Соответствие требованиям ФЗ-152, ФЗ-187, ГОСТ и ФСТЭК

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ (ПДН)

Цели:

- Идентифицировать и классифицировать ПДн
- Обеспечить техническую и организационную защиту
- Подготовиться к проверкам Роскомнадзора

Ключевые этапы:

1. **Идентификация ПДн**
   → Обследование ИС, карта потоков данных (MaxPatrol, Traffic Monitor)
2. **Техническая защита (УЗ-1 — УЗ-4)**
   → SIEM, EDR, ViPNet, резервное копирование, Passwork, DallasLock
3. **ОРД и регламенты**
   → Политики, инструкции, уровни защиты, документация для Роскомнадзора
4. **Обучение персонала**
   → Симуляции атак, защита от фишинга, обучение подрядчиков
5. **Распределённая инфраструктура**
   → VPN, видеонаблюдение, биометрическая аутентификация
6. **Аудит и подготовка к проверке**
   → Внутренний аудит, тестирование знаний, проверка документации

Статистика:

Средний штраф за нарушение 152-ФЗ —

до 500 тыс. ₽

75%
нарушений ПДн связаны с отсутствием регламентов

60%
утечек происходят через подрядчиков или филиалы

Результат:

- Комплексная защита ПДн
- Снижение риска утечек и санкций
- Готовность к проверке Роскомнадзора

Автоматизированные складские системы

Проблемы на складах сегодня:

- Неэффективное использование складского пространства
- Дефицит складской недвижимости
- Дороговизна запуска новых складов и высокая стоимость аренды складов
- Дефицит складского персонала
- Снижение эффективности работы склада
- Снижение уровня сервиса

Решение:

- Эффективное использование объема склада
- Минимизация зависимости от цен на строительство и аренду складов
- Минимизация зависимости от высокого спроса на складской персонал
- Повышение качества и скорости складских операций
- Повышение безопасности сотрудников и хранения товара

Увеличение эффективности
на 50%

Экономия складской площади
до 85%

Улучшение управления запасами
на 70-90%

Защита содержимого и легкое управление

ИИ-платформа для автоматизации HR-процессов и корпоративного обучения

DailoDailo — это платформа для создания диалоговых тренажеров, которая помогает сотрудникам промышленных предприятий быстрее осваивать профессиональные навыки и стандарты коммуникации. Благодаря моделированию реальных производственных ситуаций, платформа позволяет учиться действовать правильно без риска для производства

Основные задачи, которые решает Dailo:

Обучение сотрудников через интерактивные сценарии

Согласно исследованию обучение с использованием симуляций позволяет сотрудникам на **70%** лучше запоминать информацию по сравнению с традиционными методами. Это достигается за счет вовлеченности и практики вблизи реальных условий

Анализ усвоения знаний и персонализированный подход

Платформа отслеживает действия сотрудников, проверяет, как они запомнили материал, и выявляет пробелы. По данным корпоративных исследований, своевременная обратная связь повышает эффективность обучения на **60%**

Повышение уверенности и квалификации персонала

По статистике, **65%** сотрудников чувствуют себя более уверенно, если предварительно прошли симуляционное обучение в безопасной среде. Dailo позволяет регулярно оттачивать навыки, соответствуя требованиям современных производств

Снижение количества ошибок и рисков на производстве

Компании, использующие тренажёры, отмечают снижение количества ошибок на **50%**, так как сотрудники заранее отрабатывают действия в нестандартных ситуациях

Адаптация новых сотрудников

Использование Dailo помогает сократить период адаптации новых сотрудников в среднем на **40%**, так как они быстрее осваивают производственные процессы без необходимости отвлекать наставников

Стандартизация обучения

Платформа обеспечивает единый стандарт обучения во всех подразделениях, что особенно важно для компаний с широкой географией. Это позволяет повысить согласованность знаний на **90%** в масштабах всей организации

Экономия времени и ресурсов

По отчетам международных обучающих платформ, переход на тренажёры позволяет компаниям сократить расходы на обучение до 30% и ускорить процесс обучения на **50%** за счёт отказа от длинных теоретических курсов

АУДИТ ИТ-ИНФРАСТРУКТУРЫ

Цель:

Провести комплексную диагностику ИТ-инфраструктуры предприятия, выявить узкие места и повысить отказоустойчивость системы

Ключевые этапы:

1. **Оценка состояния** текущей инфраструктуры, выявление устаревшего оборудования и ПО
2. **Анализ соответствия** инфраструктуры требованиям бизнеса и безопасности
3. **Разработка рекомендаций** по оптимизации затрат и повышению производительности

Статистика:

40%
организаций имеют устаревшее оборудование, что увеличивает риски сбоев и потери данных

30%
ИТ-систем не соответствуют требованиям безопасности, что повышает вероятность кибератак

Проблемы с производительностью могут замедлить операции
на 25%,
что приводит к потерям в бизнесе

Результат:

Выявление узких мест и критичных уязвимостей

Рекомендации по оптимизации, что может привести к сокращению сбоев
на 30%

Повышение отказоустойчивости системы на
на 20%
и снижение рисков кибератак
на 40%

МОДЕРНИЗАЦИЯ СУЩЕСТВУЮЩЕЙ ИТ-ИНФРАСТРУКТУРЫ

Цель:

> Обновить оборудование и ПО с минимальными простоями, интегрировать новые технологии для повышения производительности

Ключевые этапы:

1. **Разработка поэтапного плана** модернизации с минимальными простоями
2. **Интеграция новых технологий** в существующие системы
3. **Обеспечение совместимости** новых решений с устаревшими системами

Статистика:

50%
предприятий сталкиваются с длительными простоями при модернизации, что снижает производительность
на 15-20%.

Интеграция новых технологий может повысить производительность
на 30%

Совместимость с устаревшими системами необходима
для 60%,
крупных предприятий, чтобы избежать дополнительных затрат

Результат:

Успешная модернизация с минимальными простоями, что позволяет повысить производительность
на 30%

Повышение производительности и совместимости с устаревшими системами, что снижает риски
на 25%

ПРОЕКТИРОВАНИЕ СКС И ЛВС

Цель:

> Создать надежные и масштабируемые инфраструктуры для обеспечения высокоскоростной передачи данных и обеспечения безопасности, доступности и отказоустойчивости данных в сети предприятия

Ключевые этапы:

1. **Проектирование кабельных систем** с учетом масштабируемости и проектирование отказоустойчивых сетей с избыточными соединениями
2. **Учет требований бизнеса и минимизация электромагнитных помех**, внедрение решений по безопасности (VPN, межсетевые экраны, IDS/IPS)
3. **Оптимизация расположения активного оборудования** для упрощения обслуживания и обеспечение масштабируемости сети для увеличения числа пользователей и устройств

Статистика:

60%

крупных предприятий испытывают проблемы с кабельными системами, что замедляет передачу данных

на 40%

Правильное проектирование может увеличить скорость передачи данных на 50% и снизить помехи

на 30%

Обеспечение масштабируемости позволяет увеличить количество пользователей

на 70%

70%

организаций сталкиваются с потерями данных из-за неудачной реализации отказоустойчивости сети

Результат:

- Увеличение скорости передачи данных на **50%**, минимизация помех на **30%**, упрощение обслуживания на **20%**
- Повышение доступности и отказоустойчивости на **30%**, снижение атак на данные на **50%** с помощью улучшенной безопасности.
- Легкость масштабирования для увеличения количества пользователей

ВНЕДРЕНИЕ ОТЕЧЕСТВЕННЫХ СИСТЕМ И МИГРАЦИЯ

Цель:

Реализовать стратегию импортозамещения за счёт перехода на отечественные операционные системы, решения для виртуализации, службы каталогов и системы резервного копирования. Обеспечить безопасность, устойчивость и независимость ИТ-инфраструктуры

Статистика:

65%

крупных предприятий сталкиваются с высокими рисками при использовании зарубежных платформ (в том числе VMware и Microsoft), что повышает вероятность утечек данных

Переход на отечественные решения снижает технологическую зависимость

на 40%

При грамотной миграции и отказоустойчивом планировании можно сократить операционные и бизнес-риски

на 30%

Ключевые этапы:

1. **Анализ текущей ИТ-инфраструктуры и требований безопасности.** Оценка используемых решений (включая VMware vSphere, vCenter Server, ESXi, vSwitch, Distributed switch, Datastore и др.) и их соответствий отечественным аналогам
2. **Выбор и внедрение отечественного ПО:**

- Операционные системы: Astra Linux, РЕД ОС
- Службы каталогов и управление пользователями: ALD Pro 2.3 (на базе FreeIPA) — централизованное управление политиками и доступами
- Системы виртуализации: zVirt — как замена VMware vSphere, с поддержкой кластеризации, управления хранилищами, vmKernel NIC и распределёнными коммутаторами
- Системы резервного копирования: СРК, Кибер Бэкап 16 — для защиты и восстановления данных

3. **Настройка доменной инфраструктуры и рабочих мест:**

- Развёртывание ALD Pro 2.3 как службы каталогов для Linux
- Администрирование рабочих станций под управлением Astra Linux, настройка групповых политик и управления доступом

4. **Миграция данных и приложений:**

- Перенос данных с зарубежных платформ (например, с VMware-инфраструктуры) на отечественные решения
- Обеспечение непрерывности бизнес-процессов, отказоустойчивость и контроль целостности данных

5. **Обеспечение безопасности и сопровождение:**

- Настройка средств контроля доступа, логирования, мониторинга и резервного копирования.
- Поддержка инфраструктуры на базе отечественного ПО с регулярным обновлением и аудитом.

Результат:

- Полное соответствие требованиям импортозамещения.
- Надежная инфраструктура на базе Astra Linux, zVirt, ALD Pro и Кибер Бэкап.
- Централизованное управление пользователями и политиками безопасности.
- Снижение риска утечки данных на 40%.
- Масштабируемая и безопасная платформа для развития ИТ-среды.

Мы всегда на связи и готов ответить на все ваши вопросы!

gst-it.ru | gst-ib.ru | dailo.co

Салманова Полина

+ 7 906 127 78 94
p.salmanova@gst-it.ru