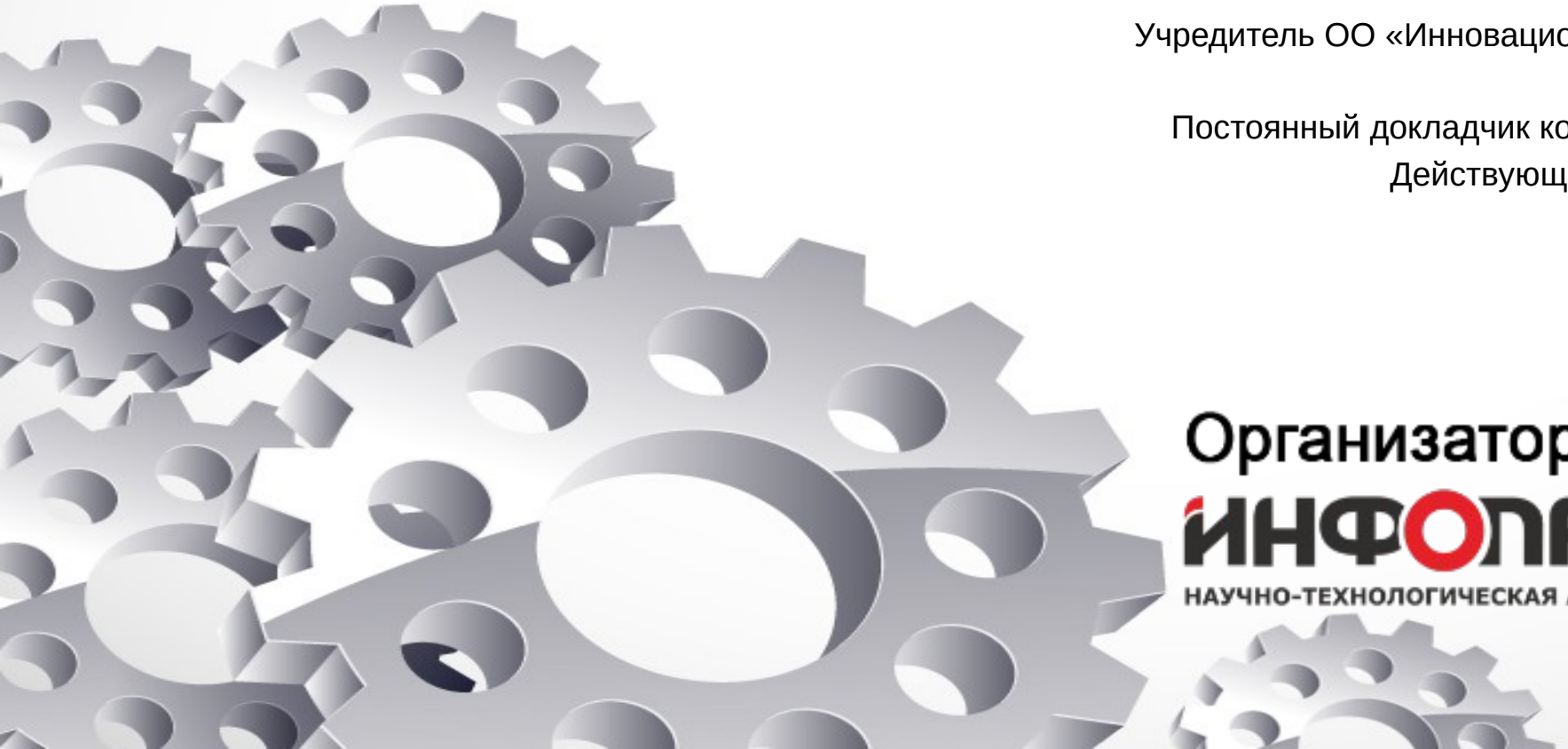
БАНКИТ'18

БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

# Структура без контроля - обречена, или как заменить инфраструктуру, основанную на картах таро, на спокойный сон

Около-Кулак Владимир Владимирович
Учредитель ОО «Инновационная инженерно-технологическая группа»
Активный член сообщества Itg.by
Постоянный докладчик конференции Best Engineer Event in Republic
Действующий системный инженер (DevOps), Appodeal



Организаторы:

ИНФОПАРК
НАУЧНО-ТЕХНОЛОГИЧЕСКАЯ АССОЦИАЦИЯ

АССОЦИАЦИЯ БЕЛОРУССКИХ БАНКОВ

НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ БЕЛАРУСЬ

# Контроль инфраструктуры:

1. Мониторинг инфраструктуры и сервисов, анализ метрик, alerting
2. Сбор и обработка логов

3. Мониторинг поведения пользователей и сотрудников
4. Внедрение и эксплуатация IDS, IPS, DLP, SIEM, NBAD
5. «Бумажная» безопасность и формальное соответствие стандартам (PCI DSS, PA-DSS, VbV/IdentityCheck, etc)

# Правильный мониторинг

Цели:
1. Упреждение аварий
2. Уведомление об авариях
3. Быстрая диагностика

Средства:
1. Точные данные
2. Полезные графики и дашборды
3. Актуальные алерты

# Что есть на рынке?

1. «Классические» решения (zabbix, nagios, etc)
2. «Кровавый энтерпрайз» по «космической» цене и «космической» же сложности
3. SaaS, MaaS, AaaS

4. «Стильно-модно-молодёжная» связка «коллектор - TSDB - визуализатор» + alert-manager (например, exporters–prometheus–grafana или telegraf–influxdb–grafana)

# Дополнительные требования:

1) Автоматизация деплоя и конфигурации
2) Поддержка динамичных окружений, интеграция с service discovery
3) Необходимость группировки
4) Большой объём данных
5) Текучка метаданных
6) Необходимость использования встроенных сущностей платформ и оркестраторов
7) Monitoring as a code
8) Alerting as a code
9) Отслеживание бизнес-метрик, алертинг по отклонениям
10) Проактивный мониторинг

Компромиссы:

a) Два стэка для разных уровней инфраструктуры
b) Интеграции со сторонними решениями

# Самое важное в современном мониторинге:

1) Автоматизация деплоя и конфигурации всех компонентов системы мониторинга
2) Учёт особенностей облачных платформ и оркестраторов
3) Monitoring as a code
4) Alerting as a code
5) Отслеживание бизнес-метрик, алертинг по отклонениям
6) Проактивный мониторинг

# А что с логированием?

Изменение подходов:
1) Отказ от локального логирования
2) Отказ от ротации логов
3) Переход на централизованный сбор логов
4) Использование отдельных утилит визуализации
5) Цепочка «коллектор–сторадж–дашборд» и ELK-подобные стэки
6) Учёт возможности работы в облаках и оркестраторах
7) Чёткое разделение систем логирования и мониторинга
8) Автоматизация деплоя и конфигурации системы логирования
9) Обеспечение горизонтального масштабирования хранилища логов

# Debug, troubleshooting

Отказ от устаревших практик:
1) ручного анализа сетевых проблем
(nc, telnet, tcpdump, nmap, wireshark)
2) tail -f /path/to/log | grep -i error
3) gdb, strace, ldd

Анализ собранных логов и данных из мониторинга

Отказ в некритичных случаях от глубокого дебага (просто редеплой сбойного сервиса, если проблема не воспроизводится часто и не связана с безопасностью)

# Почему это всё важно?

1) Упрощение и ускорение процессов поиска и устранения проблем, выявления «узких мест»
2) Увеличение прибыли и/или минимизация убытков за счёт анализа бизнес-метрик
3) Отказ от подхода «работает - не трогай»
4) Автоматизация деплоя и конфигурации не должна ограничиваться только системами мониторинга и логирования, а распространяться на всю инфраструктуру
5) Monitoring as a code и Alerting as a code как первый шаг к Infrastructure as a code
6) Упрощение внедрения отдельных практик передовых методологий (Agile, DevOps, NoOPS, SRE)

БАНКИТ 18

БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

# У меня всё

mail: kulak@itg.by
phone/telergam: +375292751078

Вопросы

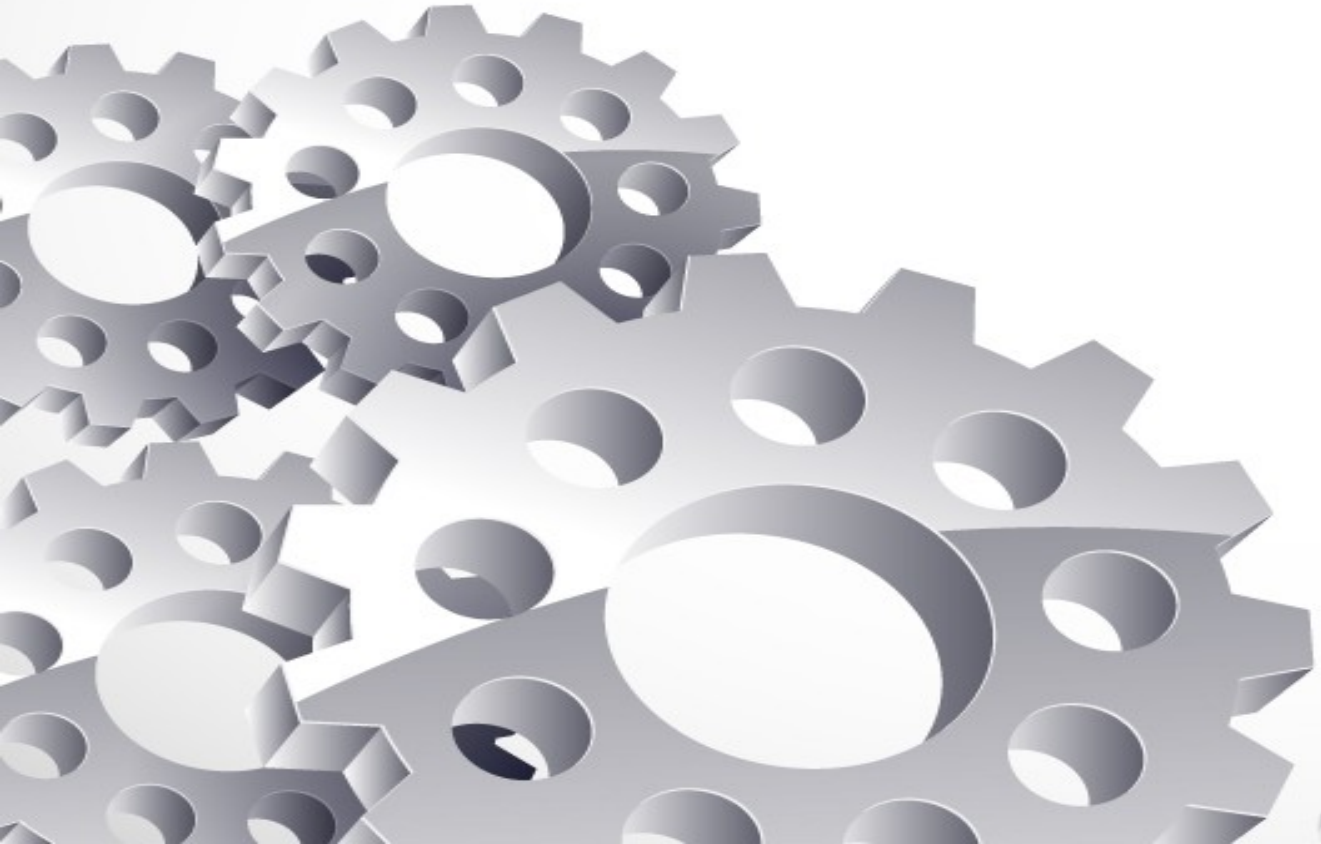
Замечания

Угрозы

Оскорбления

Предложения

...



Организаторы:

ИНФОПАРК
НАУЧНО-ТЕХНОЛОГИЧЕСКАЯ АССОЦИАЦИЯ

АССОЦИАЦИЯ БЕЛОРУССКИХ БАНКОВ

НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ БЕЛАРУСЬ