

# Аутсорсинг ИБ. Так ли это страшно?

---

Алексей Морозков  
Руководитель центра управления кибербезопасностью

# Немного теории

## Аутсорсинг ИБ

Передача части или всех функций обеспечения ИБ на управление и поддержку другой компании.

## Управляемые сервисы ИБ

Комплекс услуг ИБ, предоставляемый заказчику на базе SLA в рамках договора с провайдером управляемых услуг



Одноразовые проекты по ИБ

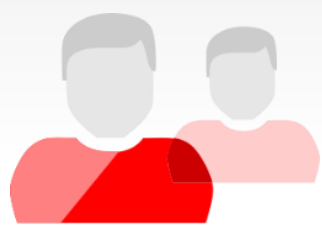


Услуги ИБ на постоянной основе

## Примеры задач ИБ для передачи на аутсорсинг

- Внедрение и поддержка СЗИ
- Аудит ИСПДн 152-ФЗ
- Анализ защищенности
- Проектирование и внедрение SIEM / XDR
- Межсетевая защита
- Обнаружение и реагирование на киберугрозы
- Анализ исходного кода на безопасность
- Безопасность АСУ ТП

# Почему имеет смысл переходить на аутсорсинг ИБ?



## Люди

- Дефицит квалифицированных кадров
- Отдел ИБ «зашился» в рутинных операциях
- Нужен фокус на основной бизнес



## Процессы

- ИБ «на бумаге»  
Отсутствие KPI по эффективности работы
- Непонятная отчетность для руководства
- Соответствие требованиям регуляторов



## Технологии

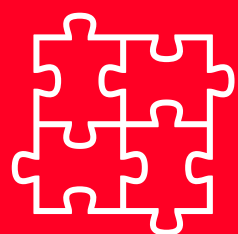
- Отсутствие возможностей для противодействия угрозам ИБ
- Рост и усложнение ИТ-инфраструктуры и ее уязвимостей

Ограниченный бюджет и нежелание собственников бизнеса увеличивать OPEX на непрофильные для бизнеса траты

\* OPEX – операционные затраты



# Типовые «вызовы» при переходе на аутсорсинг ИБ



Сложность оценки эффективности процессов ИБ



Отсутствие механизмов автоматизации процессов



Сопротивляемость изменениям и низкий уровень доверия



Разрыв в корпоративной культуре



Отсутствие понятного плана с чего начать переход



Отсутствие четких границ работ и размытая ответственность



Нет понимания об объеме выполняемых работ и о их качестве



Требования регуляторов

# Как «облегчить» переход на аутсорсинг ИБ



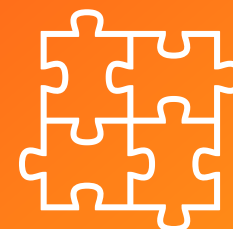
Комплексный аудит ИБ и  
дорожная карта развития



Согласование  
рекомендованных SLA, KPI  
и других метрик



Передача одной простой  
задачи ИБ на аутсорсинг



Внедрение основных  
процессов ИБ  
Матрица ответственности



Понятное всем описание  
услуги и регламент  
предоставления



Организация эффективного  
взаимодействия между  
провайдером и командой  
заказчика



**Размер  
инфраструктуры:**  
500+ серверов  
500+ пользователей

**Технологии и вендора:**  
Kaspersky  
Astra  
Usergate  
Positive Technologies  
Yandex

# Построение инфраструктуры ИБ “с нуля”

## Цели проекта

- Соответствие регуляторам и сертифицированное ПО
- Безопасная облачная инфраструктура локального вендора
- Надлежащий мониторинг и реагирование на киберугрозы

## Решение

- Инфраструктура, с использованием только отечественных СЗИ
- Инфраструктура, самописное ПО и нестандартные источники подключенные к мониторингу
- Внедрены регламенты и процессы ИБ. Интеграция с системой мониторинга и ITSM
- Разработана отчетность, автоматизированы регулярные операции

## Контекст

- Отсутствие централизованного управления ИБ и регламентов
- Ограниченные возможности серверов
- Наличие требований, которые нужно соблюдать в ходе проекта
- «Зоопарк» самописных приложений

## Результаты:

- Готовая облачная инфраструктура за 3 месяца
- KPI по покрытию 99% устройств
- Круглосуточный мониторинг и реагирование на киберугрозы
- Обнаружение угроз под особенности инфраструктуры и требования Заказчика
- Подробные отчёты по кибербезопасности. Инциденты ИБ, отсортированы по тактикам MITRE ATT&CK и по уровню критичности.

# Перспективы увеличения спроса на аутсорсинг ИБ в РФ



# Наши услуги:



Внедрение / миграция  
и сопровождение СЗИ,  
в т.ч. защита АСУ ТП



Обнаружение и  
реагирование на  
киберугрозы (SOCaaS)



Защита данных и  
корпоративные риски  
(аутсорсинг DLP)



Консалтинг, аудиты и  
комплексное  
обследование  
инфраструктуры ИБ



Аудит на соответствие  
требованиям  
законодательства  
(152-ФЗ, 187-ФЗ)



Анализ защищённости  
и тестирование на  
проникновение



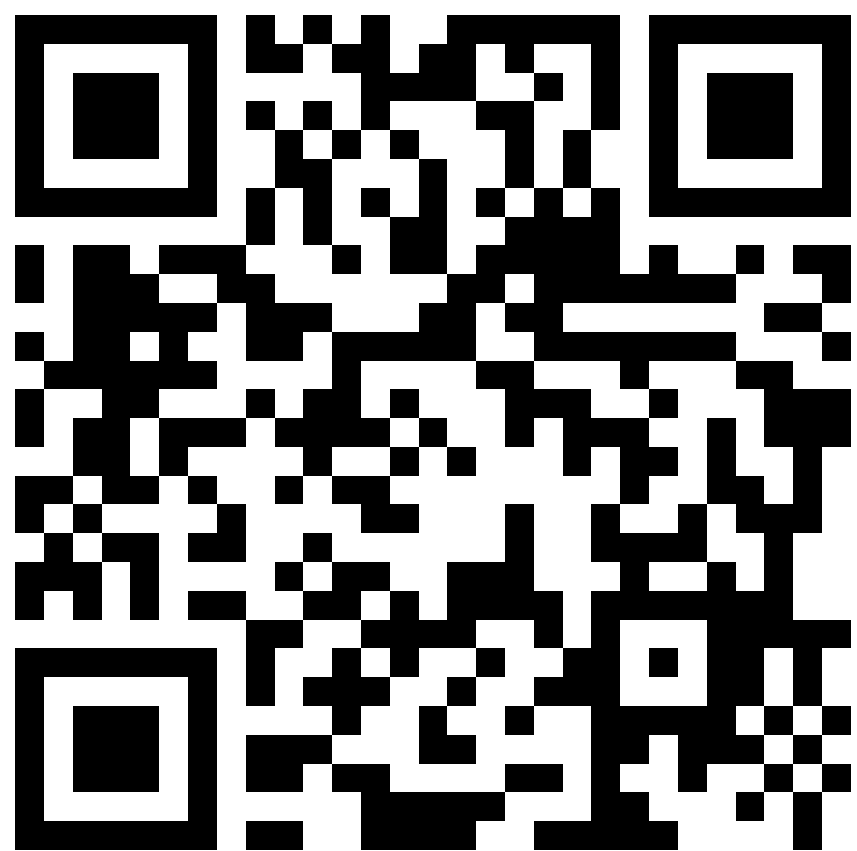
Управление  
уязвимостями  
внутреннего и  
внешнего периметра



Поставка ПО,  
оборудования, ПАК



# Чек-лист готовности перехода на аутсорсинг ИБ



Напишите нам и мы его Вам отправим

# СПАСИБО ЗА ВНИМАНИЕ



ОЭЗ «Иннополис», 422616, Республика Татарстан,  
Лаишевский район, с. Усады, ул. Дорожная, д. 42, к. 2



 [icl-services.com](https://icl-services.com)

 8 800 333 98 70

 [pr@icl-services.com](mailto:pr@icl-services.com)