ICL SYSTEM TECHNOLOGIES

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАК Я ПЕРЕСТАЛ БОЯТЬСЯ И ПОЛЮБИЛ SECAAS?

10 сентября 2019
Иркутск

Низамеев Роберт,
менеджер по развитию бизнеса

#CODEIB

Информационная безопасность - это боль!

БОЛЕВЫЕ ТОЧКИ

1 РЕГУЛЯТОРЫ

2 СОТРУДНИКИ

3 НОВЫЕ УГРОЗЫ

4 ЖИЗНЕННЫЙ ЦИКЛ ПРОЕКТА

5 САНКЦИИ

БОЛЬШИЕ БРАТЬЯ

РКН
ЕС

Требования безопасности персональных данных

(№152-ФЗ, GDPR)

ЦБ РФ

Требования Банка России
(СТО БР, 382, ГОСТ Р 57580.1 и др.)

ФСТЭК

Нормативные требования ФСТЭК
(ГИС – 17 ФСТЭК, КИИ: №187-ФЗ, АСУ ТП)

И другие

(ISO 27001, лучшие практики управления ИБ, в том числе NIST, CIS, PCI DSS, SWIFT CSP)

РАСХОДЫ НА ПЕРСОНАЛ

Фонд оплаты труда (заработная плата, премиальный фонд, начисления соцстрах и т.д.)

7 921 368 ₽/год

Расходы на содержание (сотовая связь, интернет, содержание офиса, административные и т.д.)

5 067 000 ₽/год

Обучение (цифровая криминалистика, расследования инцидентов, использование YARA, malware analysis)

2 469 749 ₽

НОВЫЕ УГРОЗЫ

300 000

УНИКАЛЬНЫХ ОБРАЗЦОВ
ВПО ЕЖЕДНЕВНО

14 сек

ПЕРИОДИЧНОСТЬ
КИБЕРАТАК

1,5 трлн. $

УБЫТКИ ОТ КИБЕРАТАК
В 2018 ГОДУ

62%

ДОЛЯ ЦЕЛЕНАПРАВЛЕННЫХ
АТАК В 2018 ГОДУ

31%

КОЛИЧЕСТВО ОРГАНИЗАЦИЙ,
КОТОРЫЕ СТОЛКНУЛИСЬ С КИБЕРАТАКАМИ

206

ДНЕЙ НА ОБНАРУЖЕНИЕ
АТАКИ

Жизненный цикл проекта

2-4 МЕСЯЦА

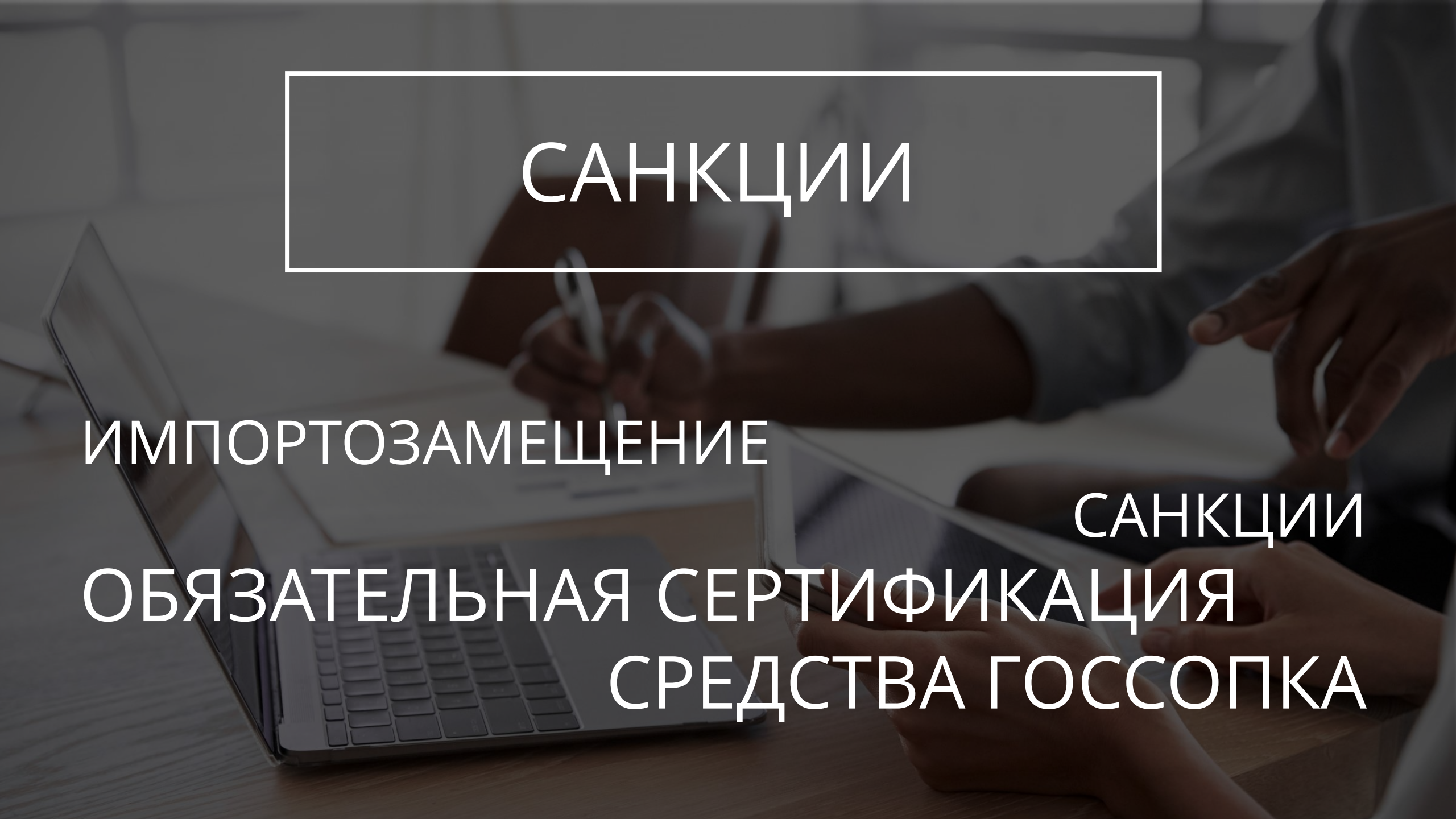
ИДЕНТИФИКАЦИЯ УГРОЗ ИБ И ОЦЕНКА РИСКОВ

2-3 МЕСЯЦА

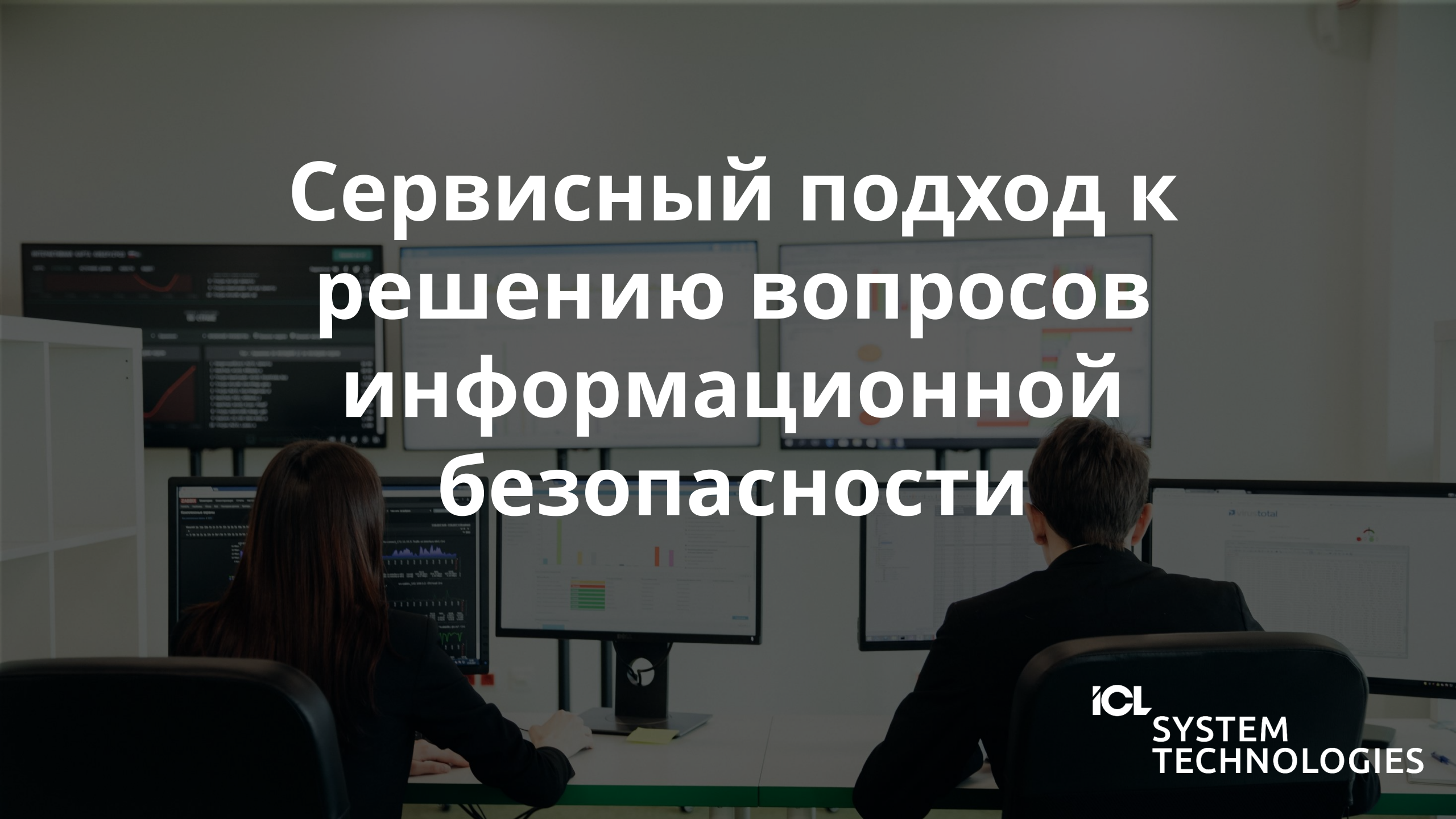
ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ

ОТ 2 МЕСЯЦЕВ ДО 1 ГОДА

ЗАКУПКА И ВНЕДРЕНИЕ


САНКЦИИ
ИМПОРТОЗАМЕЩЕНИЕ
САНКЦИИ
ОБЯЗАТЕЛЬНАЯ СЕРТИФИКАЦИЯ
СРЕДСТВА ГОССОПКА

Сервисный подход к решению вопросов информационной безопасности



ICL SYSTEM TECHNOLOGIES

ПРЕИМУЩЕСТВА СЕРВИСНОГО ПОДХОДА

ICL SYSTEM TECHNOLOGIES

Оптимизация капитальных расходов

Снижение затрат на покупку технических средств и найм персонала

Сокращение времени на выстраивание эшелона защиты

Сведение к минимуму рисков убытков

Обеспечение соответствия требований регуляторов

SOC

Функции:

1. Управление инцидентами
2. Управление знаниями
3. Управление событиями ИБ
4. Координация реагирования
5. Поддержка технологической платформы

Технологии:

1. SIEM
2. ServiceDesk
3. Log

vs

MDR

Функции:

Управление сценариями мониторинга

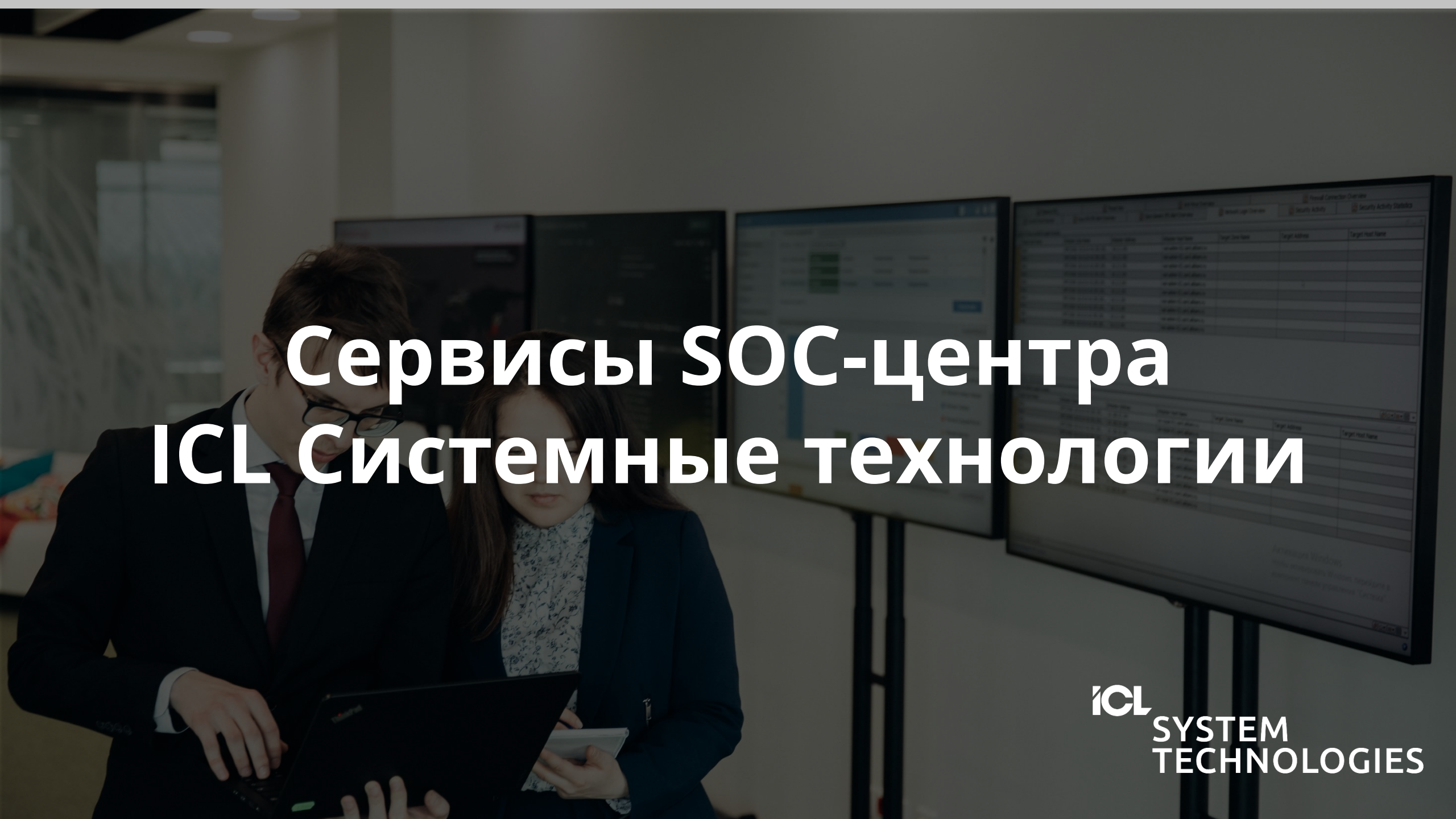
Мониторинг угроз во внешней среде

Поиск ранее неизвестных угроз

Управление уязвимостями на применимость

Технологии:

1. TIP
2. CMDB
3. Sandbox
4. Vulnerability manager
5. NTA
6. EDR



Сервисы SOC-центра ICL Системные технологии

ICL SYSTEM TECHNOLOGIES

Реализация 239 приказа ФСТЭК

ICL SYSTEM TECHNOLOGIES

V. Аудит безопасности (АУД)

АВЗ.2 Антивирусная защита электронной почты и иных сервисов

VII. Предотвращение вторжений (компьютерных атак) (СОВ)

ЗИС.16 Защита от спама

ЗИС.34 Защита от угроз отказа в обслуживании (DOS, DDOS-атак)

XII. Реагирование на компьютерные инциденты (ИНЦ)

Cyber-Kill Chain

ICL SYSTEM TECHNOLOGIES

Направления сервисов SOC-центра

ICL SYSTEM TECHNOLOGIES

- Контроль инфраструктуры
- Поведенческий анализ входящего контента
- Защита данных
- Защита web-приложений
- Анализ защищенности периметра инфраструктуры
- Аудит внутренней инфраструктуры
- Мониторинг сетевой активности
- Сервисы ГосСОПКА

Мониторинг и реагирование

Перечень сервисов:

- **Контроль инфраструктуры**
  - Предоставление системы SIEM
  - Круглосуточный мониторинг событий безопасности
  - Оповещение и реагирование на обнаруженные угрозы
- **Поведенческий анализ входящего контента**
  - Предоставление ресурсов «песочницы»
- **Мониторинг сетевой активности**
  - Предоставление средств обнаружения сетевых вторжений
- **Защита данных**
  - Предоставление средства защиты данных
- **Защита web-приложений**
  - Предоставление средства WAF
- **Сервисы ГосСОПКА**
  - Взаимодействие с НКЦКИ

Анализ защищенности

Перечень сервисов:

- **Анализ защищенности периметра инфраструктуры**
- **Аудит внутренней инфраструктуры**

КОГДА АКТУАЛЕН СЕРВИСНЫЙ ПОДХОД?

1. У ВАС ЕСТЬ АДЕКВАТНЫЙ БЮДЖЕТ ДЛЯ ПОСТРОЕНИЯ И УПРАВЛЕНИЯ ИБ?
2. У ВАС ДОСТАТОЧНО КВАЛИЦИРОВАННЫХ СПЕЦИАЛИСТОВ?
3. КАК ВЫ ПЛАНИРУЕТЕ СОХРАНИТЬ ВАШИХ СОТРУДНИКОВ?
4. ВЫ ЗНАЕТЕ, КАКИЕ ТЕХНОЛОГИИ ВАМ НУЖНЫ?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

#CODEIB

Низамеев Роберт,
ICL Системные технологии

ICL SYSTEM TECHNOLOGIES

ТЕЛЕФОН: +7 (843) 567 57 57

EMAIL: Robert.Nizameev@icl.kazan.ru

МЫ В СОЦИАЛЬНЫХ СЕТЯХ:

Телеграмм-канал @securiST

facebook.com/icl.kazan

instagram.com/icl_st

ICL SYSTEM TECHNOLOGIES

СПАСИБО ЗА ВНИМАНИЕ!