innoSTage
группа компаний

Сервисы киберзащиты как решение актуальных задач ЦОДа

Лобзин Алексей Вячеславович
менеджер по развитию сервисов киберзащиты CyberART, ГК «InnoSTage»

Последствия цифровизации

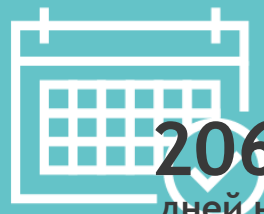
1,5 трлн. $
убытки
от кибератак

300 тыс.
уникальных образцов
вредоносного
ПО ежедневно

54%
доля
целевых атак

14 сек.
периодичность
кибератак

31%
организаций,
столкнувшихся
с кибератаками



206
дней на
обнаружение
вторжения

Система нормативных правовых актов

Федеральный закон
от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Нормативные правовые акты Президента Российской Федерации
(Указы Президента)

Нормативные правовые акты Правительства Российской Федерации
(Постановления Правительства)

Нормативные правовые акты отраслевых министерств и федеральных органов исполнительной власти (ФОИВ) (Приказы, Руководящие документы, Методические рекомендации и др.)

ФСТЭК России

ФСБ России

Минкомсвязь России

Банк России

Создание системы обеспечения информационной безопасности объектов КИИ

innoStage
группа компаний

1 Организационные меры

Разработка ОРД.

2 Технические мероприятия

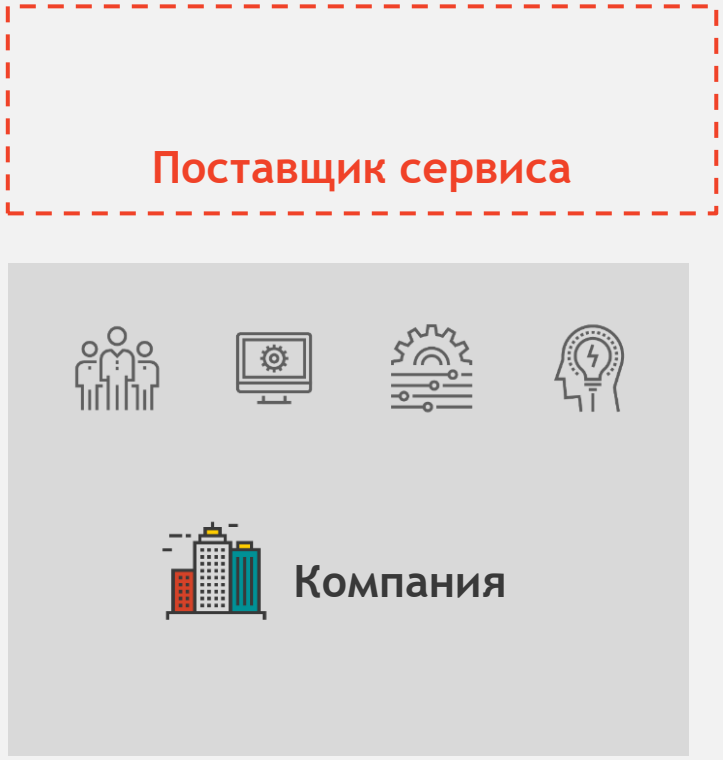
Антивирусная защита (АВЗ), защита технических средств и систем (ЗТС) и др.

3 Процессные мероприятия

Аудит безопасности (АУД), реагирование на инциденты информационной безопасности (ИНЦ) и др.

Модели обеспечения ИБ

Внутренняя модель



Аутсорсинговая модель

Гибридная модель

Особенности реализации процессов

1. Дефицит специалистов ИБ
2. Длительное внедрение
3. Обеспечение требований регуляторов
4. Отслеживание новых угроз
5. Серьезные инвестиции

Сервисы для реализации процессных мер

Преимущества:

- Быстрое выполнение мероприятий
- Получение недостающих ресурсов: персонал, средства, знания
- Сервисы в рамках SLA

Сервисы:

- **Аудит компьютерной безопасности**
- **Мониторинг безопасности и реагирование на инциденты**
- **СЗИ по сервисной модели**

SOC.Сервисы.

innoStage
группа компаний

Аудит компьютерной безопасности:

- сбор сведений об информационных ресурсах
- выявление уязвимостей информационных ресурсов
- анализ угроз информационной безопасности
- разработка и реализация защитных мероприятий

SOC.Сервисы.

innoSTage
группа компаний

Мониторинг безопасности:

- Сбор данных о событиях безопасности
- Прием сообщений о компьютерных инцидентах от персонала
- Анализ событий информационной безопасности
- Регистрация компьютерных атак и инцидентов
- Установление причин, реагирование и ликвидация последствий компьютерных инцидентов

Предоставление средств защиты информации по сервисной модели

- SIEM
- IRP
- Песочницы
- Средства защиты конечных узлов, EDR
- Системы анализа трафика, NTA, NGFW
- Средства защиты веб-приложений, WAF
- Антивирусы
- Средства защиты от DDOS-атак

Центр мониторинга - инструмент решения задач киберзащиты

innoStage
группа компаний

Знания

Процессы

Технологии

Команда

Команда


SOC
Группа эксплуатации
Группа анализа защищенности
Группа мониторинга и реагирования
Группа контроля качества
Группа развития
Администраторы технических средств
Специалисты по анализу защищенности и пентестам
Специалисты дежурной смены
Аналитики информационной безопасности
Сервис-менеджеры
Аналитики киберугроз (threat hunters)

Инвентаризация информационных ресурсов

Задачи

- Сбор и учёт сведений об информационных ресурсах
- Сбор данных об информационных ресурсах из систем заказчиков
- Проведение регулярного сканирования внутренних сетей для инвентаризации

Инструменты

- Сетевые сканеры
- SIEM
- Комплексная система управления информационной безопасности

Анализ защищенности

Задачи

- Сканирование периметра контролируемых сетей
- Выявление критических уязвимостей
- Подготовка рекомендаций по устранению
- Организация процесса устранения выявленных уязвимостей
- Расширение состава сканируемых узлов (внутрисетевое сканирование)

Инструменты

- Сетевые сканеры
- Комплексная система управления информационной безопасности «КСУИБ»

Анализ угроз ИБ

innoStage
группа компаний

Задачи

- Получение сведений об актуальных угрозах из открытых источников
- Получение сведений об актуальных угрозах по каналам информационного взаимодействия
- Самостоятельный анализ образцов ВПО
- Разработка рекомендаций по противодействию
- Расширение состава подписок на базы об актуальных угрозах

Инструменты

- Инструменты сбора информации
- OSINT-инструменты
- Средства замкнутой среды выполнения программ
- Threat Intelligence Platform

Мониторинг событий ИБ

innoSTage
группа компаний

Задачи

- Типовые направления мониторинга (ВПО, ЦУ и ботсети, фишинг, несанкционированный доступ и др)
- Профилирование и выявление отклонений
- Анализ периметрального трафика
- Анализ трафика внутри сети

Инструменты

- SIEM системы
- База знаний
- Аналитика больших данных
- IDS/IPS системы
- Потоковые песочницы
- Комплексная система управления информационной безопасности «КСУИБ»

Реагирование на инциденты

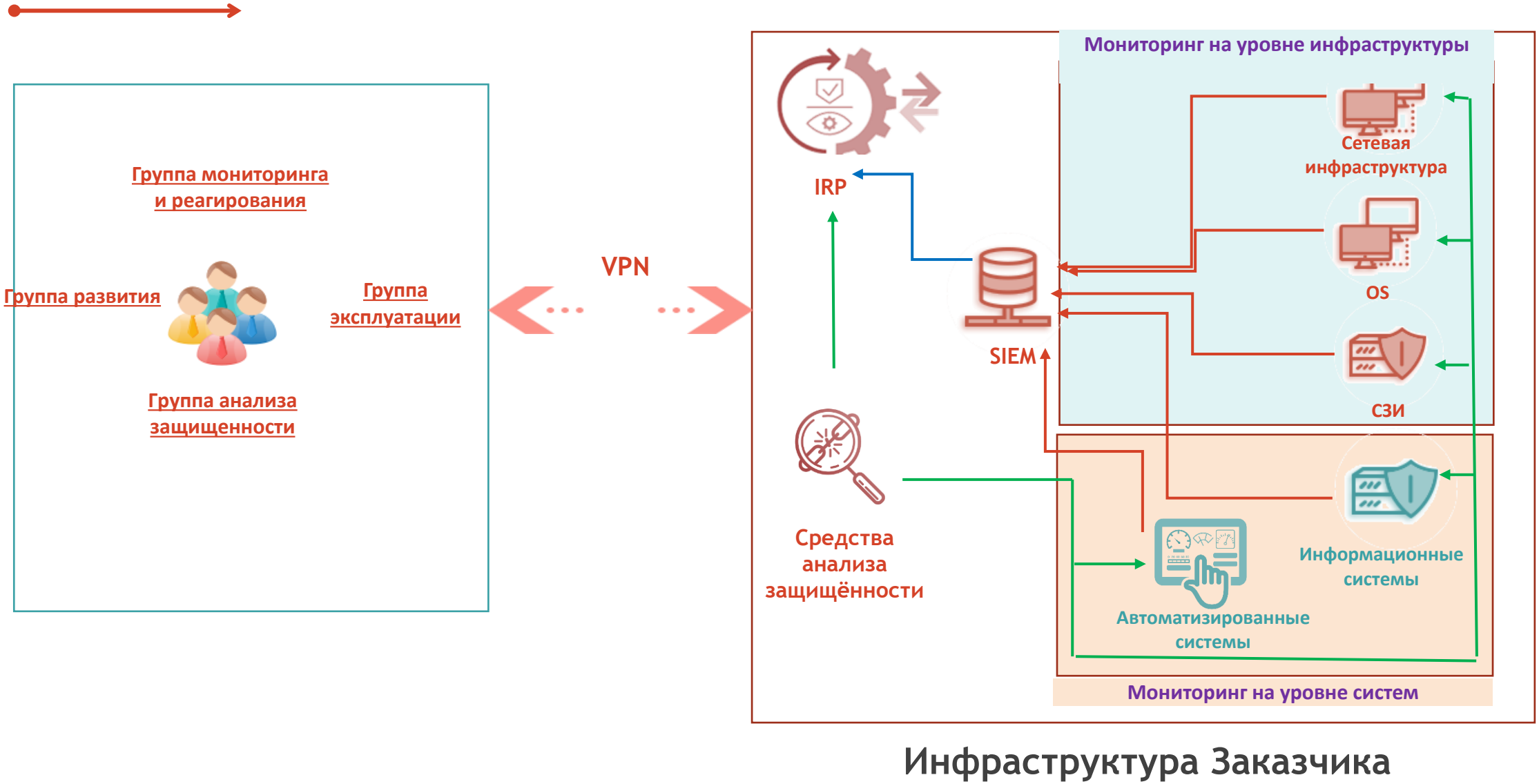
Задачи

- Регистрация и учёт инцидентов ИБ
- Автоматизация процедур реагирования
- Автоматизация взаимодействия
- Оркестрация и управление средствами защиты

Инструменты

- Комплексная система управления информационной безопасности «КСУИБ»

Схемы взаимодействия с Заказчиком



Почему вообще это нужно?

innoStage
группа компаний

- Систему защиты нельзя настроить раз и навсегда – она должна реагировать на появление новых угроз и изменения в инфраструктуре

- Без мониторинга практически невозможно отследить целевые атаки, направленные на конкретную организацию

- Тотальная блокировка уже не работает. Защитные решения должны отслеживать ситуацию, а не кардинально ограничивать бизнес

Сегодняшний бизнес ЦОД и SOC

ЦОД:

Актуальные сервисы:

- Размещение оборудования (Colocation)
- Аренда серверов
- Виртуальная инфраструктура

SOC:

Актуальные сервисы:

- Выявление и реагирование на компьютерные инциденты
- Аудит защищенности информационной инфраструктуры
- Взаимодействие с НКЦКИ

Кто клиенты ЦОД и SOC

Нефтегаз

Энергетика

Банки

Промышленность

Госсектор

Телеком

Предпосылки для дальнейшего роста отраслей

innoStage
группа компаний

- Цифровизация экономики
- Уход заказчиков от капитальных затрат
- Развитие законодательной базы и суверенного Интернета

Риски

innoStage
группа компаний

Azur всех победит: универсализация игроков и сервисов- все из одного окна

Демпинг как основной инструмент

Необходимость отстраиваться от конкурентов

innoStage
группа компаний

ВОЗМОЖНОСТЬ

Создание совместных сервисов киберзащиты информационной инфраструктуры

О группе компаний InnoSTage

ГК InnoSTage - ИТ-компания, специализирующаяся на решении нестандартных задач и задач, связанных с кибербезопасностью.

100% Российская компания

150+ Клиентов, работающих с нами

20 лет Проектный опыт основного состава специалистов

600+ Штат группы компаний

100+ Проектов, реализованных специалистами

60+ Регионов РФ, где реализовываем проекты

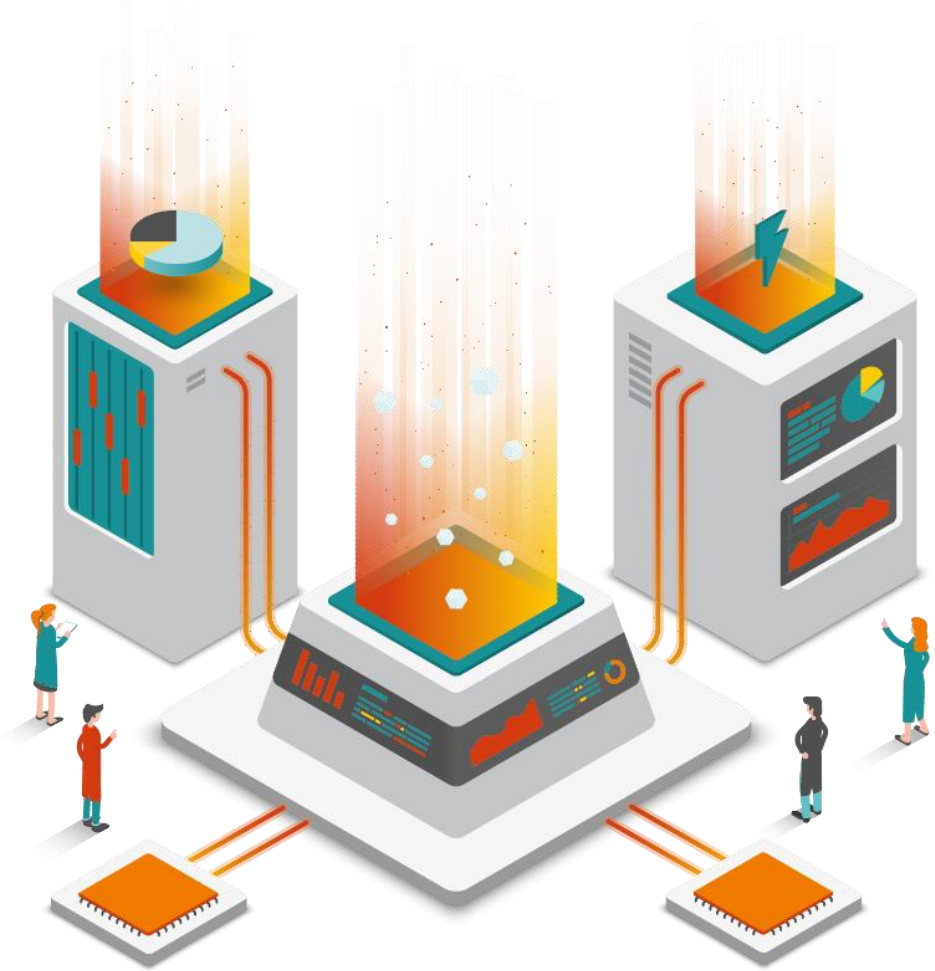
Экспертиза и ключевые направления

Группа компаний Инностейдж работает по нескольким направлениям. Экспертиза каждого строится на современном технологическом стеке, проектном опыте, постоянном повышении квалификации имеющихся специалистов и привлечении в команду новых профессионалов и новых знаний.

- **Информационная безопасность**
- **Сервисы кибербезопасности**
- **Разработка**
- **Бизнес-решения**
- **Лаборатория анализа данных**
- **IT-инфраструктура**
- **Инфокоммуникационные решения**

Отличия CyberART

innoSTage
группа компаний



- Собственная комплексная система управления информационной безопасностью и реагирования на компьютерные инциденты **NextSTage IRP**
- Круглосуточный Центр мониторинга и реагирования на компьютерные инциденты (Security Operation Center, SOC), **работающий с 2016 года**
- Собственный пакет экспертизы для выявления актуальных компьютерных угроз **CyberART Analytics**
- **Платформа обмена** оперативной информацией о киберугрозах и компьютерных атаках

Бонус

Для развертывания средств мониторинга информационной безопасности клиентам потребуются новые вычислительные мощности!