Transtelecom

**АСТАНА, 2018**

Transtelecom

# Обеспечение информационной безопасности в сфере ИКТ в КВОИКИ

*(Нормативно-правовые акты и организационно-технические мероприятия)*

## ГП Цифровой Казахстан

- **Цифровизация существующей экономики**
- **Создание цифровой индустрии будущего**
- Усиление кибербезопасности в рамках данной Программы предполагает повышение отказоустойчивости информационных систем Республики Казахстан, защиту контура в области ИКТ и общее повышение информационной безопасности, начиная от технических средств и завершая созданием культуры безопасного поведения граждан и компаний в сетях общего доступа.

## Нормативно-правовые акты

- **Закон Об информатизации**
- ПП Концепция кибербезопасности и План мероприятий.
- Правила и критерий отнесения объектов ИКТ к КВОИКИ

## КВОИКИ

- Объекты ИКТ, в том числе ИКТ "электронного правительства", нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории;

## Организационно–технические мероприятия по обеспечению ИБ

- Национального координационного центра информационной безопасности
- Отраслевых и ведомственных оперативных центров информационной безопасности
- Резервного хранилища критически важных данных информационных систем государственных органов
- Гармонизация международных стандартов, а также актуализация и разработка национальных стандартов в области информационно-коммуникационных технологий, информационной безопасности и кибербезопасности

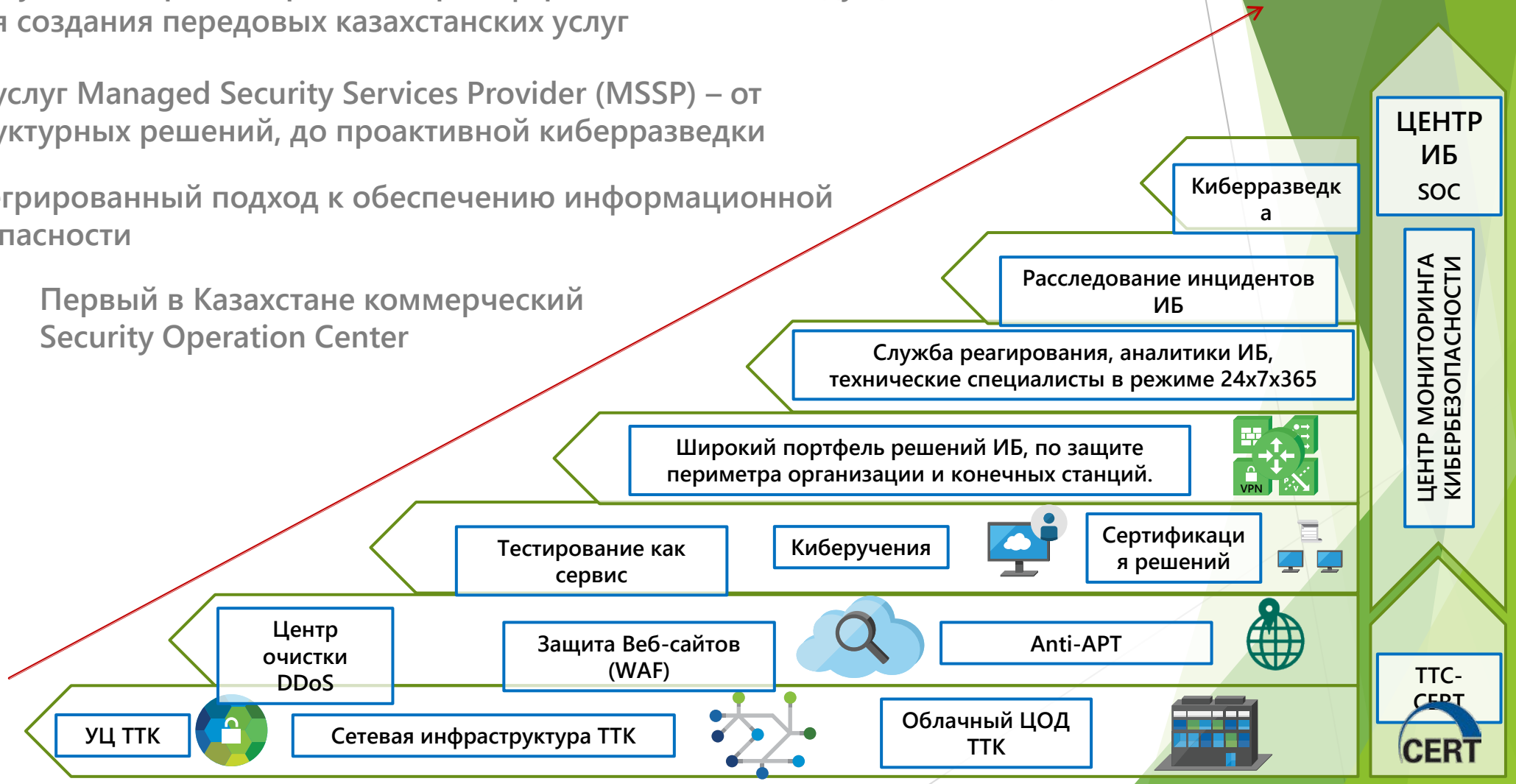
# КИБЕРБЕЗОПАСНОСТЬ

Использование лучших мировых практик и трансфер технологий от ведущих поставщиков решений ИБ для создания передовых казахстанских услуг

Развитие услуг Managed Security Services Provider (MSSP) – от инфраструктурных решений, до проактивной кибер разведки

Интегрированный подход к обеспечению информационной безопасности

Первый в Казахстане коммерческий Security Operation Center

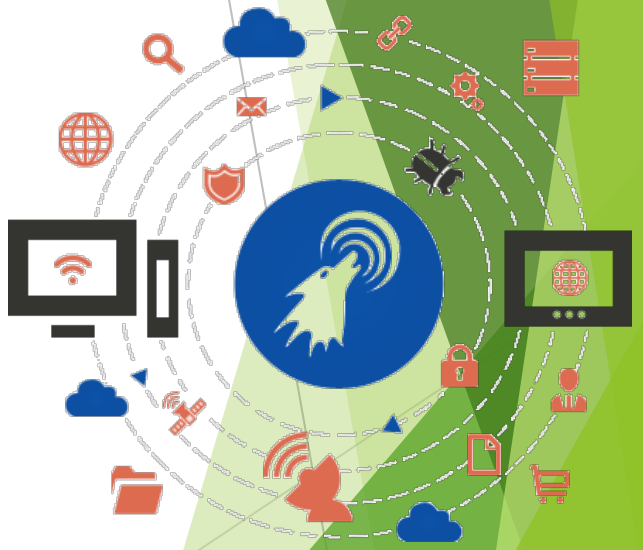


# СЕРВИСНЫЙ ПРОВАЙДЕР РЕШЕНИЙ И УСЛУГ ИБ (MSSP)

АО «Транстелеком» выводит на рынок новую уникальную для рынка Казахстана услугу: **Провайдер услуг ИБ – Managed Security Service Provider (MSSP)**.

Услуга **MSSP** включает в себя:

- предоставление аппаратных и программных средств ИБ по сервисной модели;
- управление средствами защиты «под ключ»
- удаленный мониторинг и управление средствами ИБ;
- центр управления ИБ;
- разработка практических рекомендаций по повышению уровня ИБ инфраструктуры и сервисов организаций на основе проведенного аудита ИБ или результатов расследования инцидентов;
- построение системы управления информационной безопасностью;
- эффективные рекомендации, разработанные индивидуально под каждого клиента с учетом специфики его инфраструктуры, бизнеса и заказчиков;
- предоставление специфичной для каждой отрасли информации об актуальных угрозах ИБ, мошеннических техниках, подозрительных ресурсах.



# Кейс по MSSP

**Заказчик:** Группа компаний АО «Самрук-Қазына»

**Цель:** сервис по обеспечению комплексной информационной безопасности который позволит реализовать современные и функциональные средства выявления и предотвращение инцидентов ИБ.

**Результат:** бесперебойная деятельность системы управления предприятий перевозочной деятельности, энергетики, нефтегазового, химической и атомной промышленности, машиностроения и недвижимости. Устойчивая работа финансовых систем, обеспечение своевременной обработки персональных данных клиентов, а также постоянная защита технологических сетей, автоматизированных/информационных систем поддерживающие основные деятельности группы компаний АО «Самрук-Қазына»

# *Отсутствие физических границ*
# *От компьютеров до инфраструктур*

# *Новый тип преступления и войны*

*Генерал Кит Александер, бывший командующий*

*Кибернетического Командования США*

- **«Из-за воровства интеллектуальной собственности американские компании теряют до 250 миллиардов долларов в год… потеря промышленной информации в результате кибершпионажа представляет собой самый значительный акт передачи денежных средств в истории.»**

- *Джордж Куртц, Исполнительный директор CrowdStrike «Великое Ограбление Мозга»*
- **“«Подразделение 61398… Отвечает за шпионаж в отношении западных корпораций… В любой из отраслей промышленности -проектная документация, производственные процессы, производство микросхем, телекоммуникации, фармацевтика и т.д. и т.п… Всё было украдено.»**

# 2017
# WannaCry, NotPetya, Dragonfly…
# Honda – заражённые сети в Японии, Европе, Северной Америке и Китае …
# Nissan и Renault - были вынуждены прекратить работу своих заводов в Японии, Великобритании, Индии, Франции и Румынии

- Maersk (логистика): **$300 млн.**
- Reckitt Benckiser (Lysol): **£110 млн.**
- Mondelez (Cadbury): **$150 млн**.
- Saint-Gobain (строительные материалы): **€220 млн.**
- Merck (фармацевтика): **$1200 млн.**
- FedEx, Beiersdorf (Nivea), Deutsche Post, Royal Canine ….

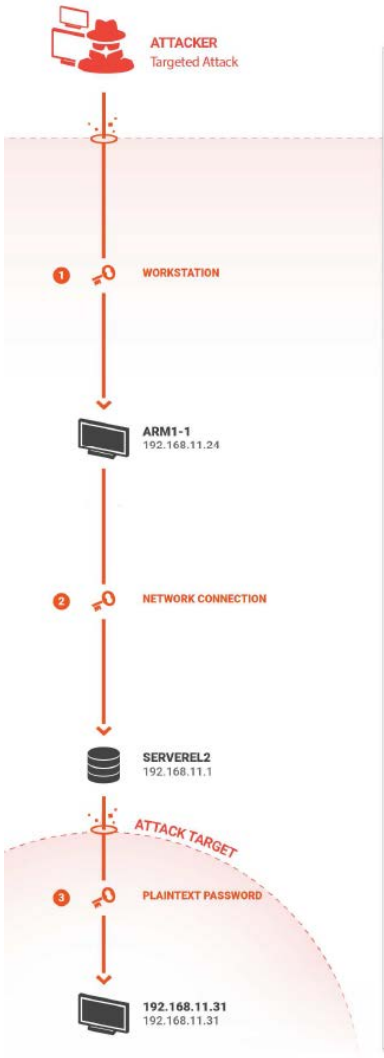
# *3 основные тенденции, вызывающие необходимость повышения уровня кибербезопасности*

| Отсутствие прозрачности | Повышенный уровень риска | Продвинутые угрозы |
|---|---|---|
| ▶ Предприятия полагаются на существующие патентованные технологии, что уменьшает обзор и мешает процессу решения проблемы | ▶ Недостаточная осведомлённость об устройствах и неспособность обеспечить их безопасность в свете возрастающего риска кибератак | ▶ Традиционные инструменты обеспечения безопасности в области IT не предназначены для защиты промышленных сетей и не смогут обнаружить вредоносное ПО |

# Промышленные сети больше не являются изолированными

- Поскольку промышленные объекты всё в большей степени используют возможности взаимодействия сетей IT и OT, они открывают критически важную сеть для более масштабных кибернетических атак и повышают уровень кибернетических рисков

# Обезличенные отчеты по аудиту защищенности АСУТП



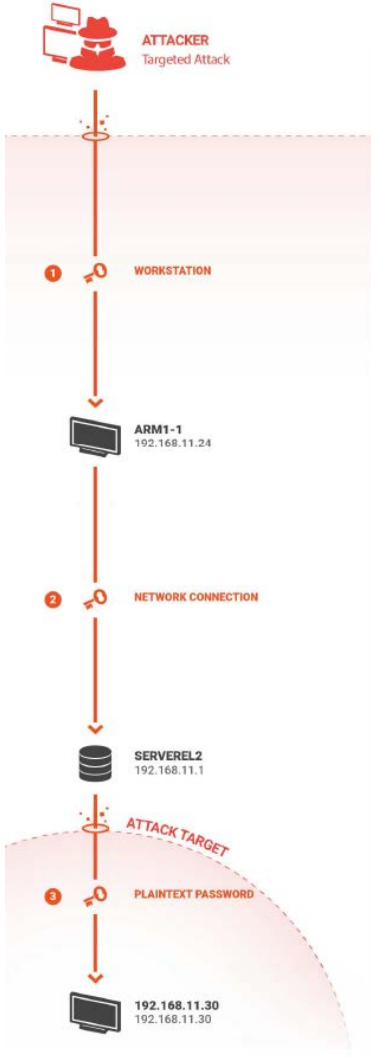

## Attack Vector #1

**(1) Workstation**
As a workstation, device ARM1-1 can be accessed by end users and can be used to initiate an attack operation

**(2) Network Connection**
Direct connection between devices

This server can be used by the attacker to persist malware in the network

**(3) Plaintext Password**
Device 192.168.11.31 can be accessed using plaintext password public, for SNMP authentication.
An attacker could extract this password from the network traffic




## Attack Vector #2

**(1) Workstation**
As a workstation, device ARM1-1 can be accessed by end users and can be used to initiate an attack operation

**(2) Network Connection**
Direct connection between devices

This server can be used by the attacker to persist malware in the network

**(3) Plaintext Password**
Device 192.168.11.30 can be accessed using plaintext password public, for SNMP authentication.
An attacker could extract this password from the network traffic

# НАЗАРЛАРЫҢЫЗҒА РАХМЕТ!
# СПАСИБО ЗА ВНИМАНИЕ!