# Управление информационной безопасностью АСУ ТП в условиях современных вызовов

РГ «Кибербезопасность» НТИ «Энерджинет»

к.т.н., Никандров Максим
Директор ООО «Интеллектуальные Сети»

# Сильное изменение политической обстановки

С февраля 2022 года и началом СВО, большинство кибератак в СМИ приняли выраженный политический оттенок, регулярно стал употребляться термин «кибервойна», заговорили о спонсируемых государствами хакерских группировках.

# Уход с рынка ведущих иностранных игроков ИБ

STONESOFT

FORTINET

cisco

BlueCoat

Barracuda

KerioControl

FORCEPOINT
POWERED BY Raytheon

Check Point
SOFTWARE TECHNOLOGIES LTD.

paloalto
NETWORKS

Microsoft Forefront

Symantec

McAfee SECURE

# Атаки на российские компании пищевой промышленности

**26 февраля**
Атака на систему управления холодильником агрохаба Селятино.
Злоумышленник **проник в сеть дистанционного мониторинга*** работы холодильных устройств и изменил температурный режим с -24° С на +30 градусов.
Испорчено 40 тонн замороженного мяса и рыбы.


**18 марта**
Холдинг Мираторг **был атакован шифровальщиком**** Bitlocker.
Атаке подверглись складские и бухгалтерские информационные ресурсы. Также была нарушена система обработки электронных ветеринарных сопроводительных документов. Пострадали 18 компаний, входящих в холдинг.

**24 марта**
Кибератаке **подвергся ***** холдинг “Тавр”
Согласно официальному заявлению, работа компании, в том числе производство, была временно парализована, нанесен значительный экономический ущерб.
Представитель холдинга оценил произошедшее как «тщательно спланированную масштабную диверсию».

Отчеты ICS Лаборатории Касперского:
- https://ics-cert.kaspersky.ru/away?url=https://1prime.ru/state_regulation/20220228/836207752.html
- https://ics-cert.kaspersky.ru/away?url=https://www.securitylab.ru/news/530695.php
- https://ics-cert.kaspersky.ru/away?url=http://agrocomgroup.ru/ru/news/kompaniya-tavr-podverglas-hakerskoy-atake

# Атака на станции зарядки электроавтомобилей в России

**28 февраля 2022**
На трассе М11 станции зарядки электроавтомобилей были деактивированы, а на экранах выводились политические лозунги.

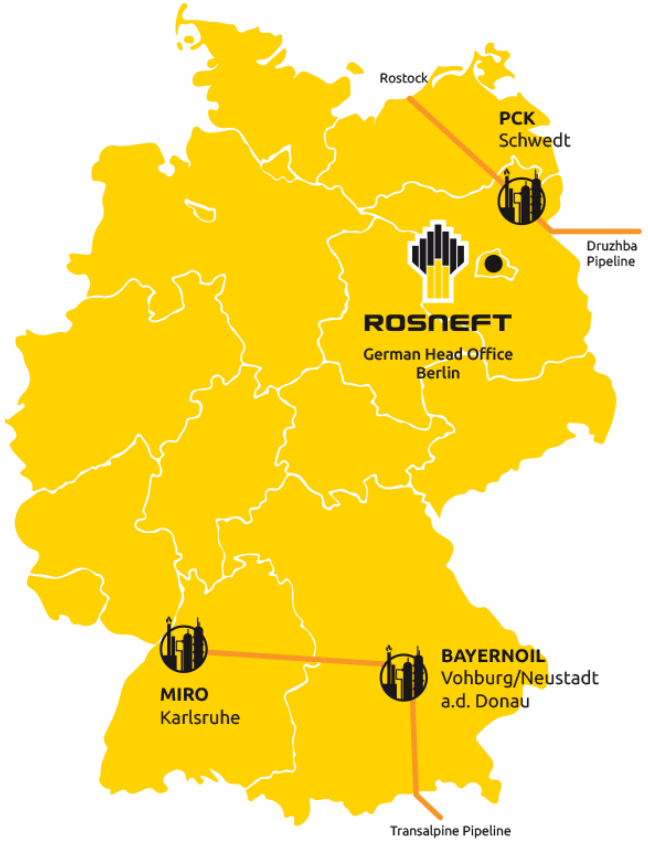
Как выяснилось, разработка этих станций была отдана на аутсорс в компанию, которая расположена в Харькове.

# Атака на компании нефтегазового сектора

В середине марта немецкая «дочка» Роснефти (Rosneft Deutschland GmbH) **подверглась*** кибератаке.

В результате атаки предположительно были нарушены внутренние процессы компании, а именно работа с контрактами. Согласно официальным заявлениям, других серьезных последствий не было.

В опубликованном заявлении Группа Anonymous сообщила, что стоит за этой атакой. Злоумышленники утверждали, что у Rosneft Deutschland было похищено 20 Тб данных.




Отчет ICS Лаборатории Касперского:

- https://ics-cert.kaspersky.ru/away?url=https://www.securityweek.com/hackers-target-german-branch-russian-oil-giant-rosneft

# Рельсовая война в Белоруссии

Январская и февральские атаки на **инфраструктуру Белорусской Железной Дороги***.

В результате атак было зашифровано множество систем БЖД.

За расшифровку данных атакующие требовали от правительства Беларуси перестать оказывать помощь российским военным.

Ответственность за атаку взяла на себя группа под названием «Кибер Партизаны».


Отчет ICS Лаборатории Касперского:

- https://ics-cert.kaspersky.ru/away?url=https://arstechnica.com/information-technology/2022/01/hactivists-say-they-hacked-belarus-rail-system-to-stop-russian-military-buildup/

# Защита персональных данных - большие проблемы

# Переход от экономической мотивации к политической

- **Рост цен на вредительство.** Пример — $2000 за установку вредоноса на рабочем месте в конкретной компании. Раньше это стоило $100–200
- **Усиленная вербовка в российских объектах КИИ.** Пример — объявление о поиске контактных лиц, отвечающих за маршрутизаторы в Ростелекоме, за большое вознаграждение и релокацию с семьями
- **Рост потока денег в медийную сферу.** Пример — размещение объявлений и предложений в телеграм-каналах подорожало в 3–5 раз

**Ежесуточные траты на эти и другие атаки такого типа — десятки млн рублей. Кто-то это оплачивает.**

Из презентации Н. Касперской

# В целом КИИ выдержала

Практика показывает что оперативно принятые меры позволили избежать крупных и массовых инцидентов у субъектов КИИ.

# Атаки на «цепочки поставок»

- Отсутствие обязательных требований подрядчиков Субъектов КИИ о защите своей информационной инфраструктуры;

- Не хватает финансов и кадров для обеспечения ИБ процессов проектирования и пуско-наладочных работ.

# Опросы показывают сильное изменения отношения

Анонимный опрос центра компетенции Кибербезопасность «Энерджинет» НТИ, проведенный с целью с целью выявления наиболее острых проблем в области осведомленности и вовлеченности работников и руководства организаций в проблематику обеспечения информационной безопасности.

## Апрель 2022 г.

### Финансирование ИБ


## Сентябрь 2022 г.

### Финансирование ИБ

# РГ «КИБЕРБЕЗОПАСНОСТЬ»

EnergyNet

*Объединяем компетенции и формируем системный подход к обеспечению кибербезопасности*

EnergyNetCS@ya.ru