kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Алексей Мартынцев

Руководитель направления регионального сопровождения и инспекций ИБ, ПАО «ГМК «Норильский никель», Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

НОРНИКЕЛЬ

Опыт «Норникеля» по анализу платформ киберучений и исследовательских лабораторий по кибербезопасности

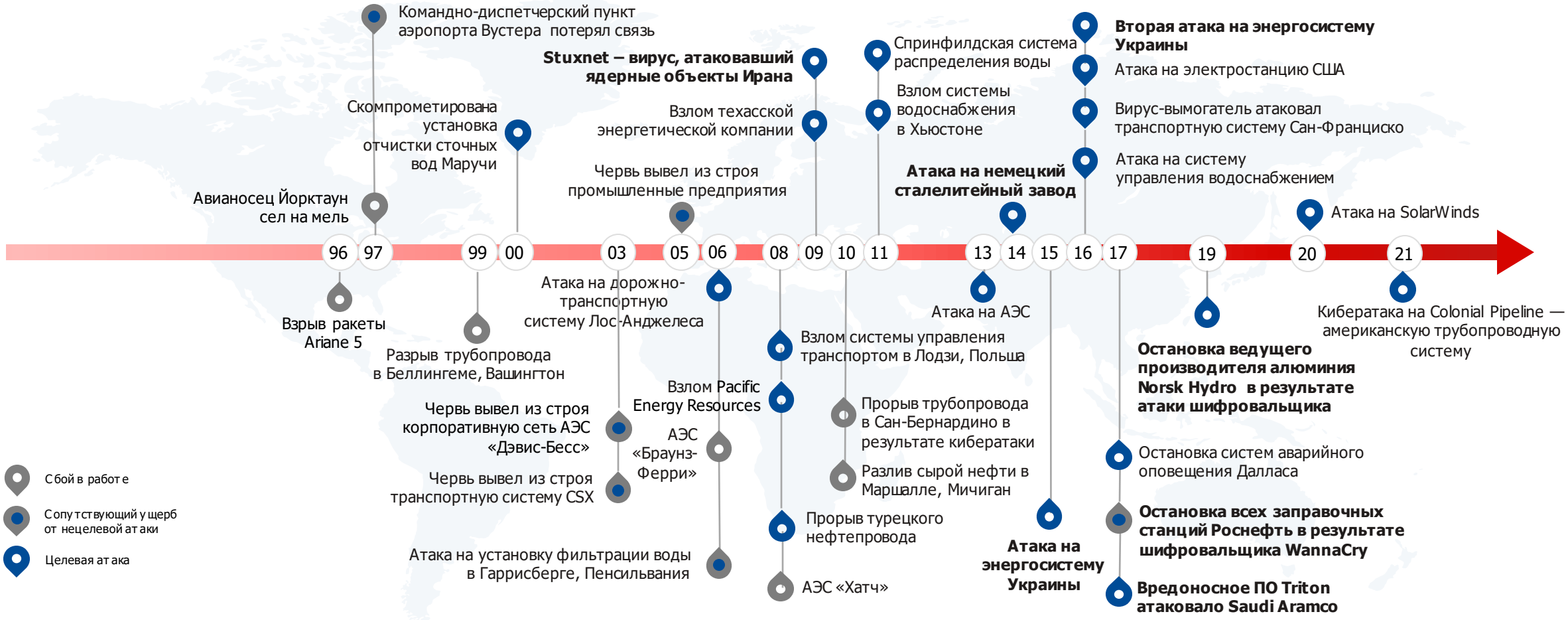
ПАО «ГМК «Норильский Никель»

СЕНТЯБРЬ 2021

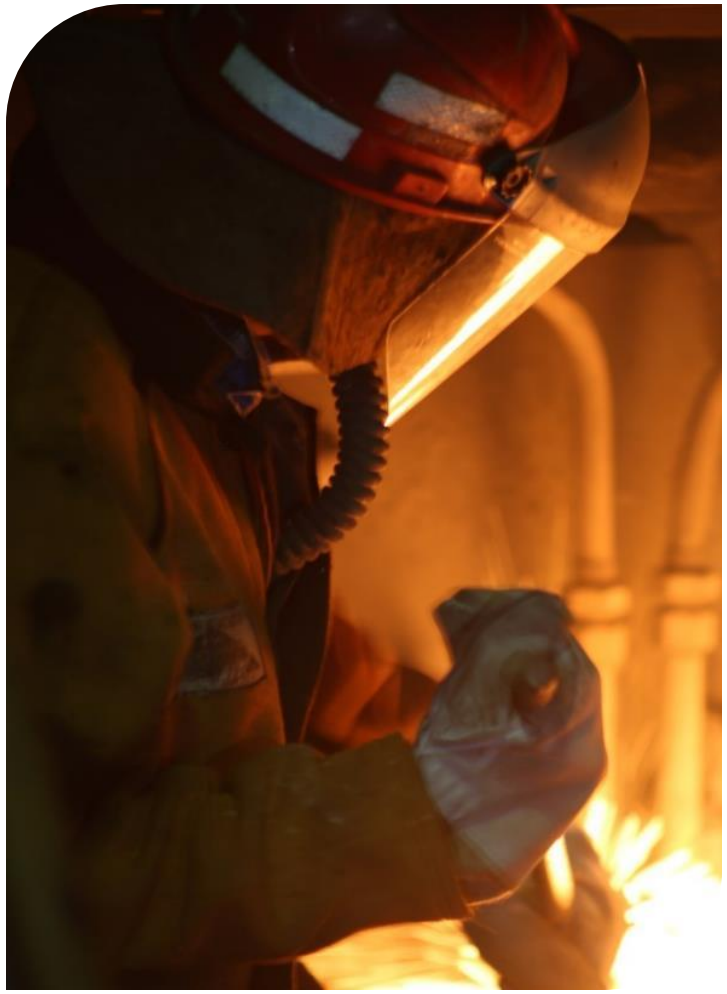
Кибератаки на промышленные объекты

НОРНИКЕЛЬ

График возрастания частоты возникновения кибер-атак на промышленные и социально значимые объекты за последние **20 лет**.у



Причины и последствия киберинцидентов



Основные проблемы

- **Устаревшие АСУ ТП**
- **Большое количество разрозненных АСУ ТП**
- **Нехватка квалифицированного персонала**
- **Отсутствие среды тестирования**
- **Существует риск присутствия недекларированных возможностей**

Возможные последствия

Добыча и транспортировка газа
Нарушение поставки газа населению и заводам

Тепло и водоснабжение\Электроэнергетика
Нарушение теплоснабжения и водоснабжения городов

Химическая промышленность
Выбросы в окружающую среду загрязняющих веществ

Производство
Разрушение оборудования и ухудшение качества производимой продукции

Ж/Д
Сбой управления Ж/Д стрелками может привести к проблемам с транспортировкой и создать аварийную ситуацию

Авиация
Воздействие на систему управления светосигнальными огнями во время посадки самолета в плохих условиях видимости может привести к катастрофе

Флот
В негативном случае воздействия на систему управления судовыми системами судно сядет на мель, что может привести к повреждению груза

Основные предпосылки создания Исследовательской Лаборатории ИБ

НОРНИКЕЛЬ

Рост количества кибер-атак на промышленные объекты

- Недостаточные компетенций сотрудников по отражению атак
- Значительный финансовый ущерб в случае реализации кибер-рисков
- Необходимость соответствия 187-ФЗ и регламенту взаимодействия с ФСБ России в рамках Соглашения по обнаружению и предотвращению атак

Потребность в среде тестирования АСУ ТП и средств их защиты

- Большое количество проектов по обеспечению ИБ АСУ ТП и внедрению СЗИ
- Необходимость пилотирования новых и зарубежных решений по защите АСУ ТП
- Необходимость тестирования отказоустойчивости СЗИ и планов восстановления СЗИ

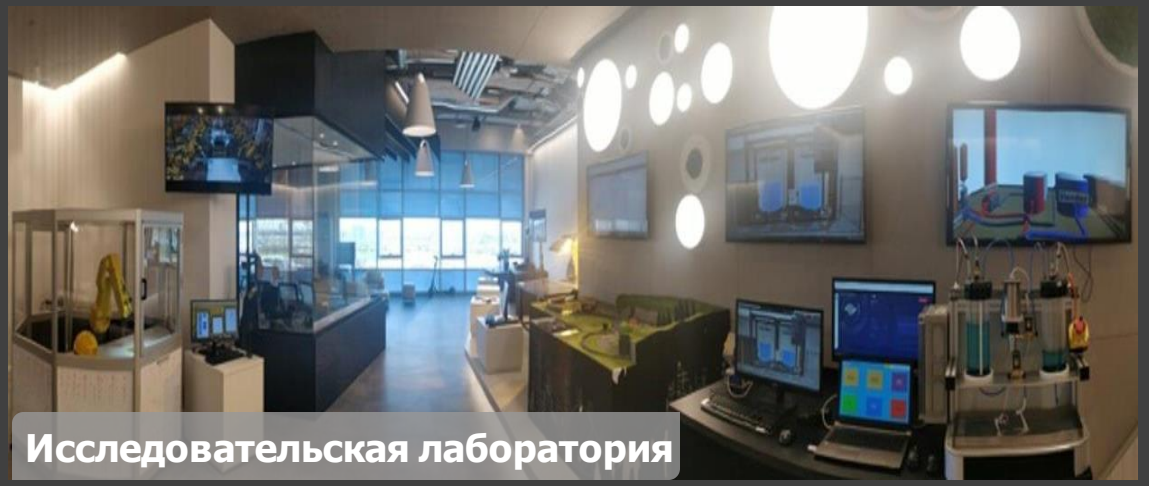
Рост цифровизации и автоматизации промышленных объектов

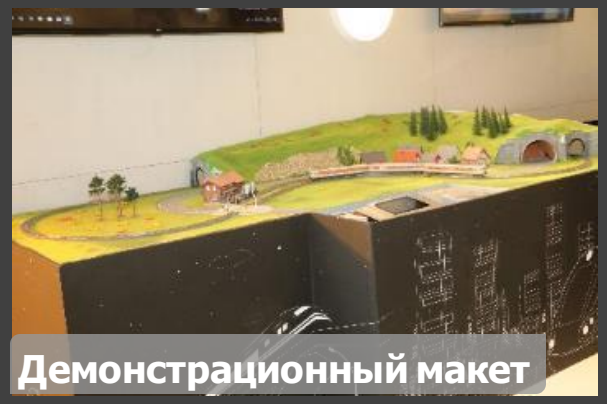
- Необходимость обеспечения кибер-безопасности при внедрении программ цифровизации
- Необходимость контроля зарубежных решений по автоматизации процессов

Что такое Исследовательская Лаборатория ИБ?

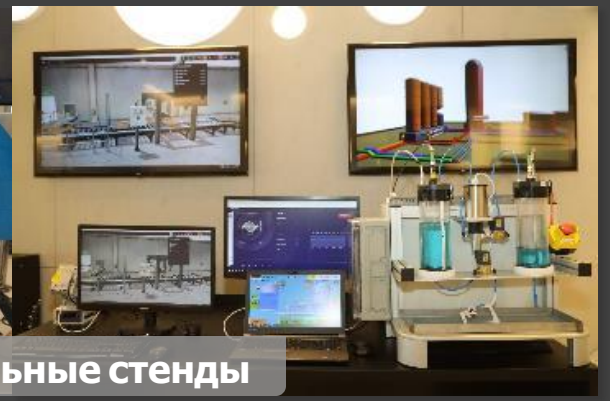
Исследовательская Лаборатория информационной безопасности

— выделенное структурное подразделение, которое с помощью набора технологий, процессов и обученного персонала осуществляет исследование современных методов обнаружения, предупреждения и ликвидации последствий компьютерных атак.


Исследовательская лаборатория


Демонстрационный макет


Испытательные стенды




Кинетический модуль

Роль Исследовательской Лаборатории в решении кризисных ситуаций

Примеры реализации похожих проектов в России и мире

В Мире

Министерство энергетики (Израиль)

Аналитический Центр Министерства национальной инфраструктуры, энергетики и водоснабжения Израиль

Idaho National Lab (Департамент энергетики, США)

Исследовательская лаборатория обеспечивающая безопасность критической инфраструктуры

Fraunhofer - ведущая в мире Компания прикладных исследований

Ростелеком Солар

Киберполигон – проект реализуемый в рамках Национальной программы «Цифровая экономика России» в 2020 году. Платформа с отраслевыми цифровыми двойниками, позволяющая проводить масштабные киберучения, соревнования и исследования в области ИБ

POSITIVE TECHNOLOGIES

Проект «The Standoff» - это защищенная платформа, позволяющая создавать виртуальные модели ключевых объектов инфраструктуры и тестировать их на устойчивость к хакерским попыткам получения незаконного доступа.

Направления Исследовательской Лаборатории ИБ

Исследования и разработка R&D

Компьютерная криминалистика и анализ инцидентов

Управление киберустойчивостью промышленных систем

Аналитика кибератак и уязвимостей ИБ

Разработка и тестирование средств защиты

Обучение и повышение осведомленности

Совершенствование процессов и разработка стандартов

Управление эффективностью и отчетность

Качественное сравнение платформ кибер-учений

НОРНИКЕЛЬ

- *достоинства*
- *недостатки*

	CYBERBIT (On-prem)	CYBERBIT (Cloud)	AMPIRE	Ростелеком Солар	PurpleGround
Цена	$$$$$ ✗	$$ ✓	$ ✓	$$ ✓	$ ✓
Импортозамещение	Израиль ✗	Израиль ✗	Россия ✓	Россия ✓	Россия ✓
Ограничения по обучающимся	До 20 ✗	До 20 ✗	Отсутствует ✓	Отсутствует ✓	Отсутствует ✓
Количество и категории сценариев атак	60 сценариев атак категории MITM, Webshells, DDoS, XSS, SQLi RCE, атаки на сегмент АСУ ТП ✓	Более 30 сценариев атак категории MITM, Webshells, DDoS, XSS, SQLi RCE ✓	6 сценариев атак на БД, файловые сервера, вирусные заражения, атаки на сегмент АСУ ТП ✗	Более 20 сценариев атак на ИТ-инфраструктуру, вирусные заражения, атаки на промышленные протоколы ✗	8 сценариев атак на ИТ-инфраструктуру, вирусные заражения, атаки на SCADA ✗
Категории СЗИ	СЗИ категории SIEM, FW, AV, NMS и др. популярных вендоров ✓	СЗИ категории SIEM, FW, AV, NMS и др. популярных вендоров ✓	Решения категории СКЗИ, OpenSource решения категории IDS/IPS, IRP и ELK ✗	СЗИ категории SIEM, FW, AV, IRP, IDS, IIDS, PAM, и др. любых вендоров . ✓	OpenSource решения категории SIEM, IDS/IPS, IRP и ELK ✗
Возможность обучения внешних сотрудников	Присутствует ✓	Присутствует ✓	Присутствует ✓	Присутствует ✓	Присутствует ✓
Конструктор сценариев	Присутствует ✓	Отсутствует ✗	В разработке ✓	В разработке ✓	В разработке ✓
Наблюдение	Расширенный функционал платформы по созданию типовых сценариев и инфраструктуры (конструкторы) из коробки.	Облачная версия CyberBit Range с ограниченным функционалом и составом сценариев.	Отсутствует конструктор сценариев и инфраструктуры, небольшой набор СЗИ из коробки. Существует возможность доработки по требования Заказчика.	Отсутствует конструктор сценариев и инфраструктуры, средний набор сценариев атаки Существует возможность доработки по требованиям Заказчика.	Гибкое, легко масштабируемое решение, предоставляющее возможность доработки под требования Заказчика.

Информация актуальна на момент проведения исследования – 2020 год

Связь с цифровизацией

НОРНИКЕЛЬ

СПАСИБО ЗА ВНИМАНИЕ

Алексей Мартынцев
MBCI, CISSP, CISM, CDPSE