Результативная кибербезопасность в электроэнергетике

...и причём здесь CIM?

Дмитрий Даренский

руководитель практики
промышленной кибербезопасности
ddarensky@ptsecurity.com

- **Образование**: автоматизация технологических процессов и менеджмент пром. предприятий
- **15** лет опыта строительства технологических сетей и систем связи
- **10** лет опыта создания систем АСУ ТП, ТМ, АСТУЭ, АСКУЭ, СДТУ
- **9** лет опыта создания комплексных систем безопасности в промышленности

20 лет экспертизы в исследованиях и разработке

11 продуктов **10** сервисов **5** комплексных решений

1200+ сотрудников

7 офисов

Мы проводим исследования, создаем продукты и сервисы с **единой целью** — не дать хакерам реализовать кибератаки с недопустимыми последствиями для бизнеса, отрасли, страны

positive technologies

партнеры

50+ крупнейших мировых производителей программного обеспечения

300+ ведущих интеграторов в сфере информационных технологий

клиенты

2000+ клиентов

80% российских компаний из рейтинга «Эксперт-400»

Тренд на результативную кибербезопасность

99% компаний можно взломать всего за несколько шагов

Бизнес формирует запрос на кардинальные изменения

- ✓ Государство поддерживает этот запрос и создает условия для изменений
- ✓ Первые лица компаний уже сейчас лично вовлекаются в постановку целей кибербезопасности
- ✗ Но текущие подходы не позволяют получить измеримый для бизнеса результат
- ✗ Индустрии не хватает экспертизы по кибер-безопасности и правильного целеполагания

Сравнение подходов к обеспечению кибербезопасности

РЕЗУЛЬТАТИВНАЯ КБ		КЛАССИЧЕСКАЯ ИБ
Концентрация усилий на мониторинге целевых активов и уровня безопасной настройки (харденинга) компонентов инфраструктуры	 МОНИТОРИНГ	**Стремление к полному покрытию** активов средствами мониторинга и защиты
Понимание целей атакующего и атрибуция злоумышленников для адекватного и эффективного реагирования **Предотвращение** наступления недопустимого события с последующей программной роботизации рутинных процедур	 РЕАГИРОВАНИЕ	**Отсутствие четкого представления о цели атаки** и, как следствие, максимально возможное количество работ по реагированию **Обработка** инцидентов и реагирование по пред заготовленным скриптам (playbook)
Постоянная инвентаризация активов и их классификация с учетом недопустимых для бизнеса событий и реальных способов развития кибератаки	 УПРАВЛЕНИЕ АКТИВАМИ	**Периодическая инвентаризация активов и их классификация** по принципу «конфиденциальность, целостность, доступность»

Что такое недопустимые события

Всегда есть события, которые недопустимы для предприятия

делающие **невозможным достижение** организацией операционных и стратегических **целей** или приводящие к **длительному нарушению** её основной **деятельности, в том числе в результате кибератак**

Выполняет все свои функции	Выполняет свои функции частично	Не выполняет свои функции
допустимый ущерб	ущерб ниже порогового значения	ущерб выше порогового значения

- крупные финансовые потери
- потеря доли рынка
- остановка производственных процессов
- публичные судебные разбирательства
- срыв контрактных обязательств

Недопустимые события на энергообъектах

Источники	**ФЗ в редакции от 01.07.2021 № 116 «О промышленной безопасности опасных производственных объектов»**	**ПП РФ от 28 октября 2009 г. № 846 «Об утверждении правил расследования причин аварий в электроэнергетике»**	**ПП РФ от 13.08.2018 N 937 "Об утверждении Правил технологического функционирования электроэнергетических систем "**	**Приказ Минэнерго от 12.07.2018 N 548 "Об утверждении требований к обеспечению надежности электроэнергетических систем..."**
Примеры недопустимых событий	Приостановка эксплуатации опасного производственного объекта... в случае аварии или инцидента на опасном производственном объекте, а также ... обстоятельств, влияющих на промышленную безопасность;	Отключение объектов электросетевого хозяйства (высший класс напряжения 110 кВ и выше), генерирующего оборудования мощностью 100 МВт и более на 2 и более объектах электроэнергетики...	Прекращение или угроза прекращения топливообеспечения тепловых электростанций ...суммарной мощностью свыше 10 % всей располагаемой мощности электростанций в операционной зоне диспетчерского центра, а также прекращение (угроза прекращения) топливообеспечения тепловой электростанции мощностью 200 мегаватт и более.	Повышение напряжения в контрольных пунктах выше верхней границы графика напряжения или на оборудовании объектов электроэнергетики выше наибольшего рабочего напряжения

Недопустимые события как следствие кибератак

АТАКУЮЩИЙ

Изменение режимов работы и/или остановка турбины

Прекращение генерации электроэнергии

РЕЗКИЙ СБРОС МОЩНОСТИ В ЭНЕРГОСИСТЕМЕ

2019

80% территории Венесуэлы осталась без света более чем на сутки
Власти Венесуэлы назвали кибератаки на ГЭС «Гури» причиной блэкаута

ИНЦИДЕНТЫ → НЕДОПУСТИМОЕ СОБЫТИЕ ДЛЯ ЭНЕРГООБЪЕКТА → НЕДОПУСТИМОЕ СОБЫТИЕ ДЛЯ ОТРАСЛИ

КАК ЭТО ПРОИСХОДИТ В ЖИЗНИ

АТАКУЮЩИЙ

Перекос частоты или достижение наибольшего допустимого уровня напряжения

Отключение линий передачи электроэнергии

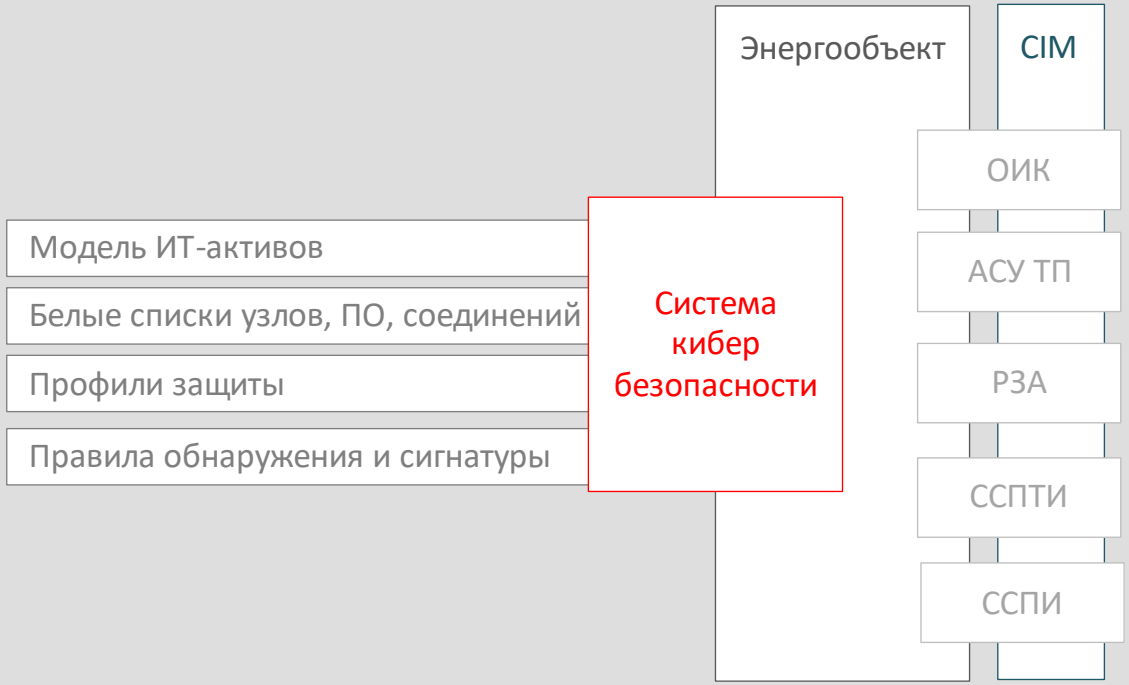
КАСКАДНОЕ ОТКЛЮЧЕНИЕ ЭЛЕКТРОСЕТЕЙ

Массовое отключение электроэнергии в Индии на несколько часов
Причиной назвали кибератаку со стороны Китая

2020

ИБ в энергетике сегодня
Что с ней не так?

Безопасник:
Видит только ИТ-события без понимания текущих режимов и технологического состояния объектов



Диспетчер:
Контролирует режимы и не допускает аварий без учёта причин вызванных кибератаками и событиями в ИТ-инфраструктуре

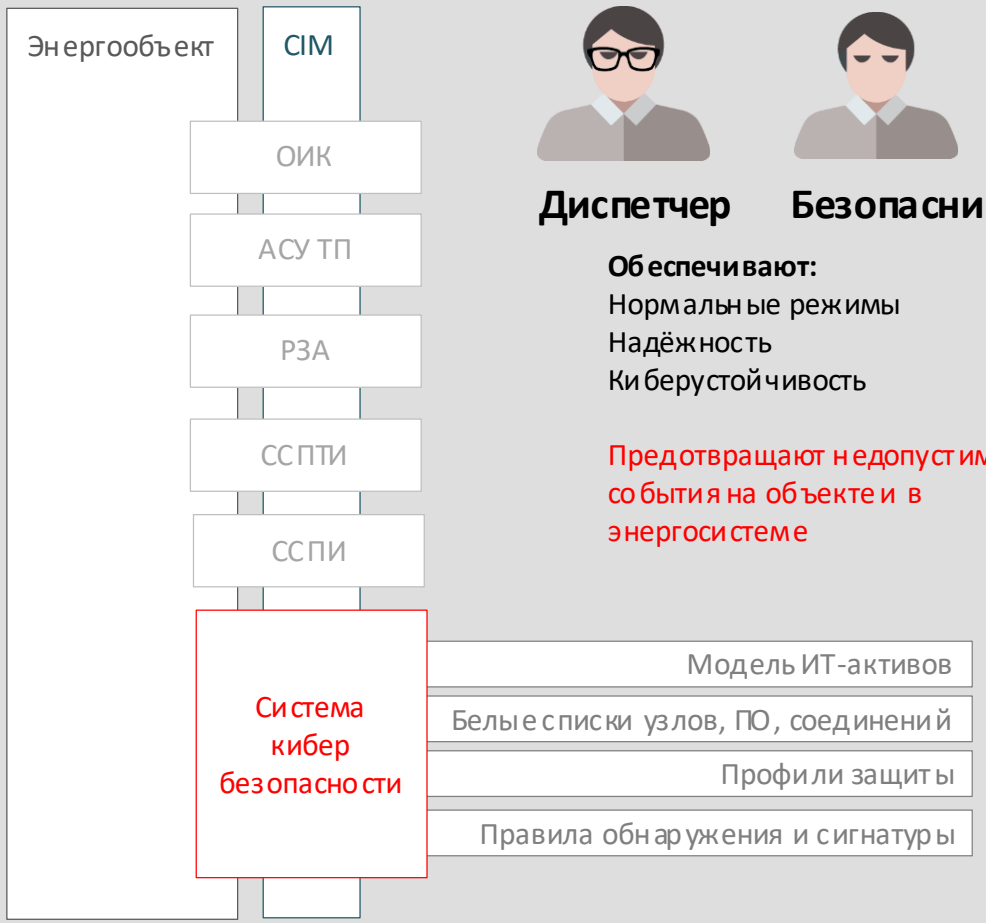
Отсутствует измеримый результат. Система безопасности работает. Безопасник на месте.

Кибератаки продолжают быть успешными. **Киберустойчивость энергосистемы остаётся под вопросом**

Условия для достижения результата

РЕЗУЛЬТАТИВНАЯ КБ		УСЛОВИЯ
Концентрация усилий на мониторинге целевых активов и уровня безопасной настройки (харденинга) компонентов инфраструктуры	 МОНИТОРИНГ	Система кибербезопасности должна знать основные критичные элементы энергообъекта, его пороговые эксплуатационные параметры и оперативные данные нормальных режимов
Понимание целей атакующего и атрибуция злоумышленников для адекватного и эффективного реагирования **Предотвращение** наступления недопустимого события с последующей программной роботизации рутинных процедур	 РЕАГИРОВАНИЕ	Система кибербезопасности должна знать сценарии реализации недопустимых событий посредством кибератак и автоматически реагировать с учётом всех данных об энергообъекте и режимах
Постоянная инвентаризация активов и их классификация с учетом недопустимых для бизнеса событий и реальных способов развития кибератаки	 УПРАВЛЕНИЕ АКТИВАМИ	Система кибербезопасности должна иметь актуальную информацию об энергообъекте, представленную в едином формате с системами технологического управления и защит.

Результативная безопасность в электроэнергетике



Диспетчер **Безопасник**

Обеспечивают:
Нормальные режимы
Надёжность
Киберустойчивость

Предотвращают недопустимые события на объекте и в энергосистеме

Взаимодействие специалистов выстраивается в понятные процессы управления безопасностью

Системы кибербезопасности решают необходимые прикладные и отраслевые задачи, помогают предотвращать недопустимые события, а не абстрактно «защищают информацию»

Технологическое управление и кибербезопасность строятся на единой информационной модели

Безопасность обеспечивается на уровне регламентов, процессов, технологий и ИТ-инфраструктуры

Результат: недопустимые события для объекта и энергосистемы становятся невозможными

Спасибо за внимание

О Positive Technologies

20 лет
исследований и опыта в обеспечении кибербезопасности

300+
экспертов в крупнейшем исследовательском центре в Европе

10 лет
проводим самые крупные в России и Европе киберучения

80%
отечественных компаний рейтинга «Эксперт-400» используют наши продукты и услуги

Positive Technologies уже 20 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400». Следите за нами в соцсетях,а также в разделе «Новости» на сайте ptsecurity.com.