Москва, 29 сентября - 1 октября

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА

РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА ЭНЕРГОСИСТЕМ 2021

POSITIVE TECHNOLOGIES

Управление кибербезопасностью АСУ ТП и РЗА предприятий электроэнергетики

Даренский Дмитрий Анатольевич

Positive Technologies

Российская Федерация

Даренский Дмитрий Анатольевич

Обеспечиваем **практическую кибербезопасность** бизнеса

POSITIVE TECHNOLOGIES

18 лет
исследований
и опыта в обеспечении
кибербезопасности

500+
экспертов в крупнейшем
исследовательском
центре в Европе

12 продуктов
для контроля защищённости,
мониторинга, обнаружения и
реагирования в нашем портфолио

В 3 раза
быстрее растем по
сравнению с рынком
в России

80%
отечественных компаний
из списка **Expert 400**
используют наши продукты

9 лет
проводим самые
крупные в Европе
открытые киберучения

КОНЦЕПЦИЯ результативной кибербезопасности **(ИБ 2.0)**

СДЕЛАТЬ

НЕДОПУСТИМОЕ НЕВОЗМОЖНЫМ

Недопустимые события – чрезвычайные ситуации, делающие невозможным достижение предприятием операционных и стратегических целей или приводящие к длительному нарушению основной деятельности

ПРИНЦИПЫ результативной кибер безопасности

РУКОВОДСТВО ОБОЗНАЧАЕТ **ЧТО НЕДОПУСТИМО** ДЛЯ ИХ ОРГАНИЗАЦИИ

БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ ДЕЛАЕТ **НЕДОПУСТИМОЕ НЕВОЗМОЖНЫМ**

КИБЕРУЧЕНИЯ ПОДТВЕРЖДАЮТ **РЕЗУЛЬТАТ НА ПРАКТИКЕ**

ПРЕДЛОЖЕНИЕ Positive Technologies
для энергокомпаний

1

Методология построения результативной системы кибербезопасности, обеспечивающей **гарантированный результат** – неприемлемые для предприятия события становятся невозможными

КЛЮЧЕВЫЕ ЭЛЕМЕНТЫ
методологии

СЦЕНАРНЫЙ АНАЛИЗ И ВЕРИФИКАЦИЯ РИСКОВ

Определить недопустимые события на цифровом производстве и проверить их практическую релевантность и реализуемость

ФОРМИРОВАНИЕ ПРОГРАММЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ

Спроектировать целевое состояние системы безопасности цифрового производства, исключающую недопустимые события

СОЗДАНИЕ ЦЕНТРА ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ

Развернуть и настроить технические компоненты ЦПК, усилить безопасность производственных и бизнес процессов

КИБЕРУЧЕНИЯ И ПОВЫШЕНИЕ УСТОЙЧИВОСТИ

Подготовить и провести полевые кибер учения, подтвердить результативность ЦПК

Методические рекомендаций РНК СИГРЭ

как элемент методологии

Производственный риск

НАРУШИТЕЛИ

СЦЕНАРНЫЙ АНАЛИЗ

ОБЪЕКТЫ ЗАЩИТЫ И ВОЗДЕЙСТВИЯ

УЯЗВИМОСТИ

СПОСОБЫ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ

Кто ?

Как сломал ?

Что сломал ?

Какие уязвимости эксплуатировал ?

Как эксплуатировал ?

Методика моделирования угроз энергообъектов. Разработана РГ D2-B5 РНК СИГРЭ в 2017 году

ПРЕДЛОЖЕНИЕ Positive Technologies
для энергокомпаний

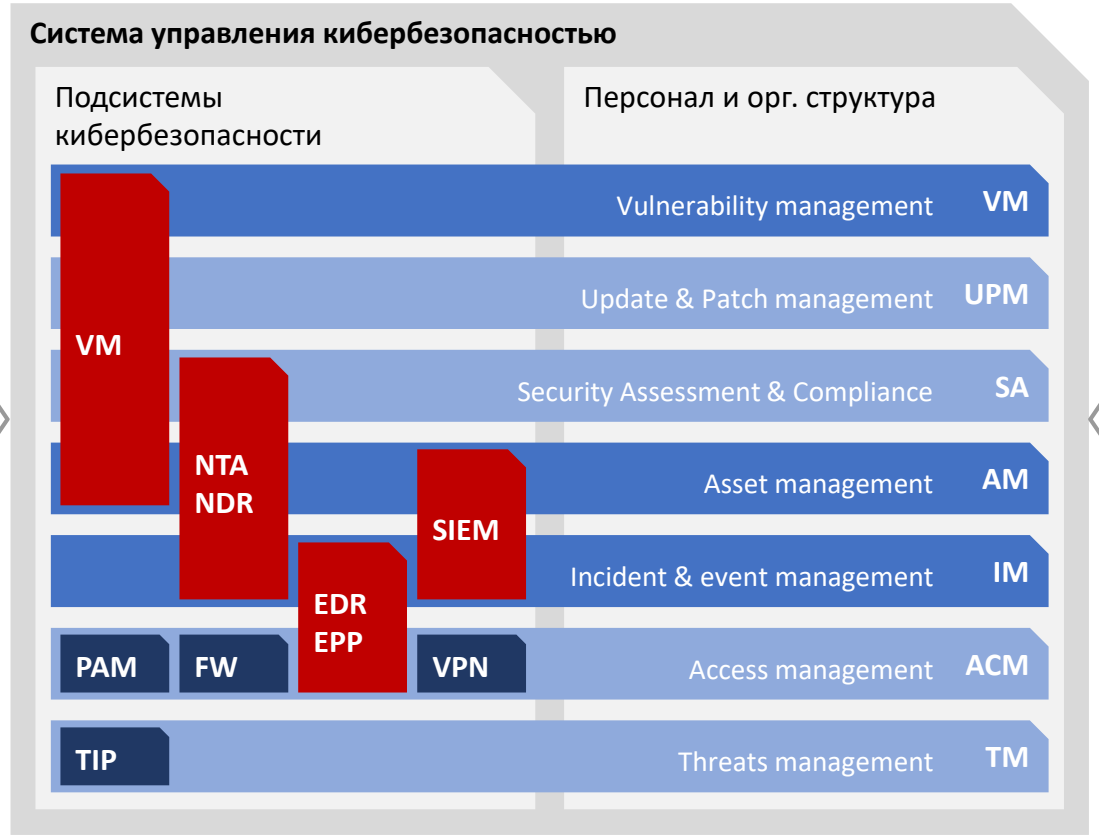
2

Методология
построения процессов управления кибербезопасностью в технологических сетях и системах промышленной автоматизации

ПРОЦЕССНЫЙ ПОДХОД
к созданию систем безопасности

Меры обеспечения безопасности
239 приказ ФСТЭК

Требования к силам и средствам
235 приказ ФСТЭК



ГОСТ Р ИСО/МЭК 27ххх
Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности

ГОСТ 51901.хх
Менеджмент риска

ГОСТ Р МЭК 62443
Сети промышленной коммуникации
Безопасность сетей и систем

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ Positive Technologies
внедрению и применение продуктов для построения и поддержания процессов управления информационной безопасностью в технологических сетях

ПРЕДЛОЖЕНИЕ Positive Technologies для энергокомпаний

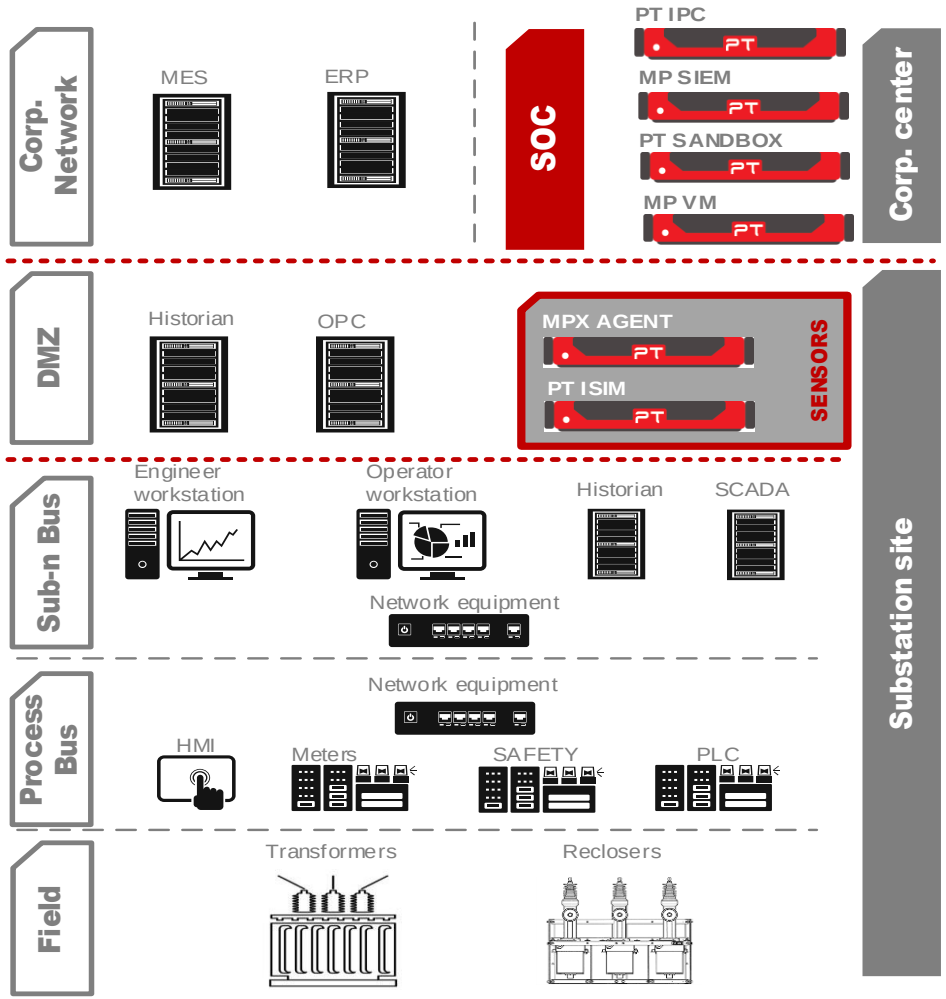
3

Комплексные технические решения **на базе продуктов** Positive Technologies, позволяющих реализовать процессы управления кибербезопасностью и обеспечить гарантированный результат – сделать **неприемлемое невозможным**

PT INDUSTRIAL CYBERSECURITY SUITE

Компоненты Industrial Cybersecurity Suite

Incident Response	PT IPC
SIEM	MaxPatrol SIEM
NTA/NDR	PT ISIM
Anti-Malware	PT MS / Sandbox
Vulnerability Management	MaxPatrol VM



СПАСИБО ЗА ВНИМАНИЕ!

Дмитрий Даренский

Руководитель практики промышленной кибербезопасности
ddarensky@ptsecurity.com

- Образование: автоматизация технологических процессов и производств
- 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