Эффективное управление защитой информации

В СВЕТЕ НОВЫХ УГРОЗ ИБ

CNews ФОРУМ 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

Системный оператор ЕЭС

Структура Общества

ИА с центральным диспетчерским управлением (ЦДУ)
7 объединенных диспетчерских управлений (ОДУ)
51 региональное диспетчерское управление (РДУ)
14 представительств

Основные задачи

- управление технологическими режимами работы объектов ЕЭС России в реальном времени
- обеспечение перспективного развития ЕЭС России
- обеспечение единства и эффективной работы технологических механизмов оптового и розничных рынков электрической энергии и мощности

Особенности управления

Ориентировка на доступность и целостность.

Трехуровневая модель управления: ИА - ОДУ - РДУ

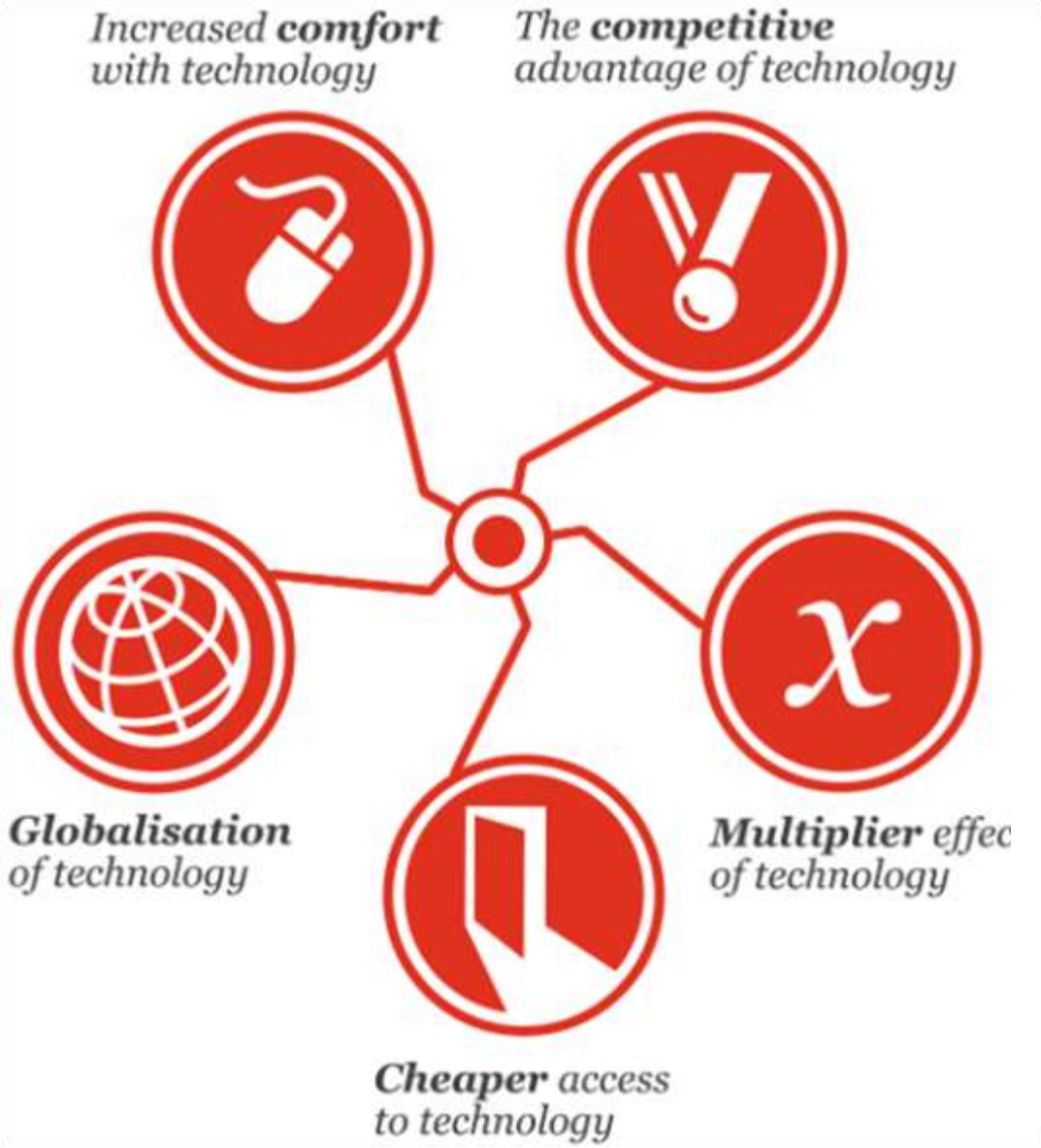
Исторически сложившаяся практика восприятия филиалов как самостоятельных единиц

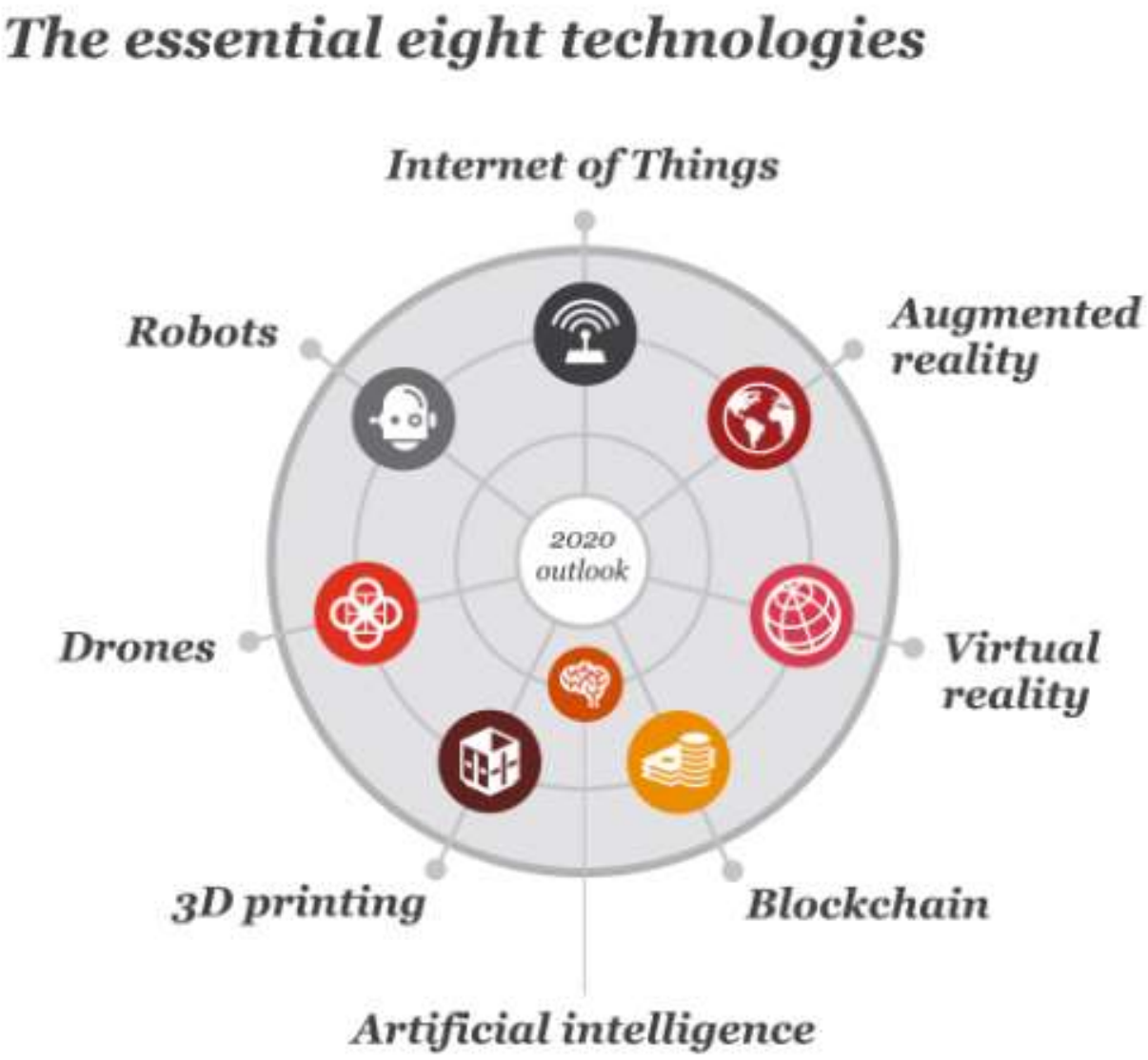
Каскадная модель управления проектами

Ограничения, вызовы, следствия

- Воздействие систем ИБ на критические элементы инфраструктуры должно быть НЕ ЗАМЕТНЫМ
- Для определения векторов совершенствования ИБ должны быть НАКОПЛЕНЫ ДАННЫЕ о событиях ИБ
- Для обеспечения оперативного реагирования на угрозы требуются ВЫВЕРЕННЫЕ ПРОЦЕДУРЫ

Мировые тренды развития ИТ





Что актуально для ТЭК?

«ДОРОЖНАЯ КАРТА» «ЭНЕРДЖИНЕТ» НАЦИОНАЛЬНОЙ ТЕХНОЛОГИЧЕСКОЙ ИНИЦИАТИВЫ

одобрена президиумом Совета при Президенте Российской Федерации по модернизации экономики и инновационному развитию России **28.09.2016**

15.12.2016 межведомственной рабочей группой по разработке и реализации НТИ при президиуме Совета при Президенте Российской Федерации по модернизации экономики и инновационному развитию России **одобрен первый пилотный проект НТИ «Энерджинет» — «Цифровой РЭС — Янтарьэнерго»**

Приоритет: развитие отечественных комплексных систем и сервисов интеллектуальной энергетики и обеспечение лидерства российских компаний на новых высокотехнологичных рынках мировой «энергетики будущего» в ближайшие 15-20 лет.

ОСНОВНЫЕ ПРОЕКТНЫЕ НАПРАВЛЕНИЯ «ДОРОЖНОЙ КАРТЫ»

Надежные и гибкие сети:

- Проект «Цифровой РЭС»
- Оборудование цифровой сети, системы управления
- Стандарты

Интеллектуальная распределенная энергетика:

- Микроэнергосистема (кампус, район города, промышленная площадка и т.д.)
- Агрегатор энергоресурсов
- Самоорганизующиеся энергосистемы

Потребительские сервисы:

- IoT в энергетике (на базе открытой платформы)
- Аналитика, биллинг и платежные сервисы

Комплексные решения:

- «Умный город»
- Адаптивные коммунальные системы города

ЭТАП 1
Цифровая инфраструктура и сервисы

ЭТАП 2
Адаптивная инфраструктура и сервисы

ЭТАП 3
Самоорганизующаяся инфраструктура и сервисы

2015 Краткосрочная перспектива (5 лет) — 2018 — 2020 Среднесрочная перспектива (10 лет) — 2025 Долгосрочная перспектива (25 лет) — 2035

Уязвимости, статистика

$3.63 млн – средняя СТОИМОСТЬ утечки данных

АБСОЛЮТНО КАЖДАЯ исследованная сигнальная сеть УЯЗВИМА

98% приложений содержат УЯЗВИМОСТИ

Более 100 уязвимостей в среднестатистическом приложении

Угрозы

Утрата информации

Недоступности информационных систем

Утечка информации

Искажение информации

Количество компонентов АСУ ТП, доступных в сети Интернет, ориентировка на IoT

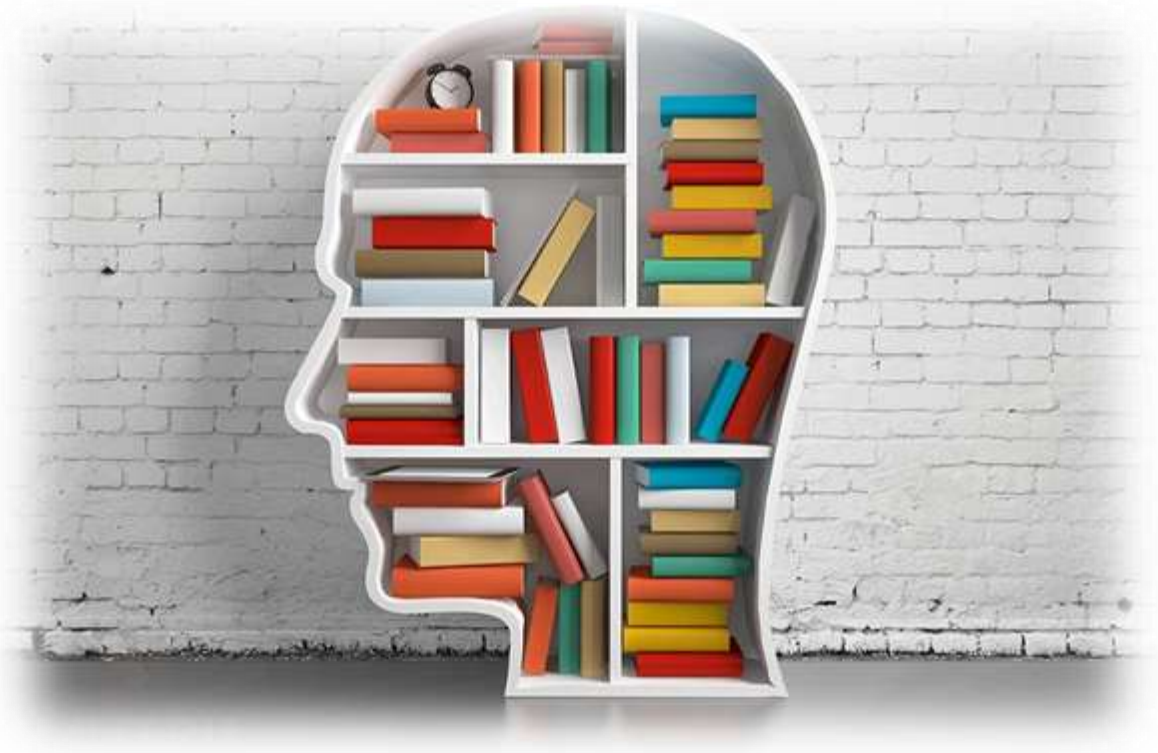
Каскадная связность систем

Взаимопроникновении инфраструктурных и технологических компонентов

Упор на автоматизацию управления

Управление ИБ

ИЛИ



Проблемы и ограничения

НЕТ озвученных КЕЙСОВ, ПРИМЕРОВ реализации угроз и путей их нейтрализации

НИЗКАЯ зрелость процессов

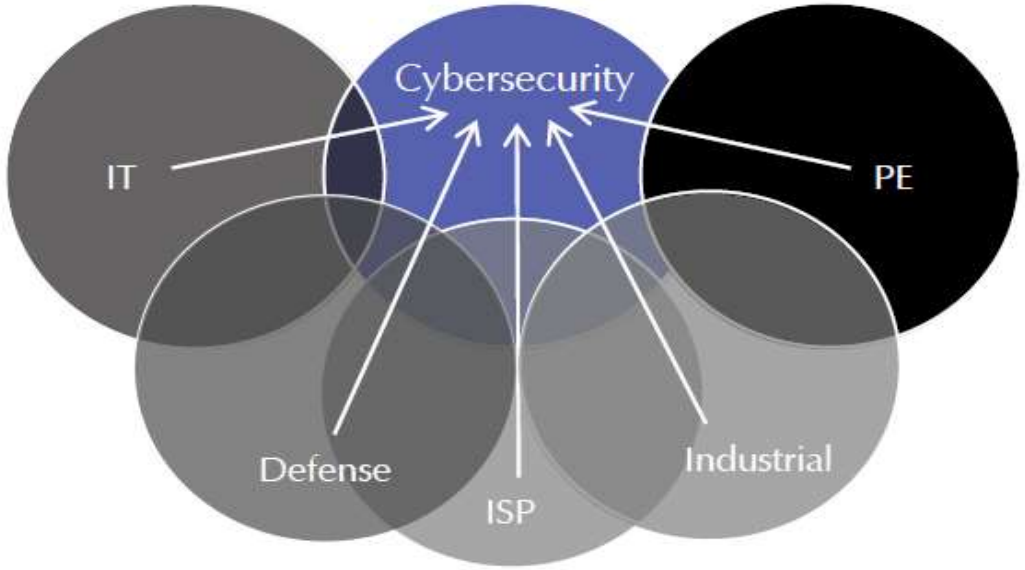
КУЛЬТУРА компании или «ИСТОРИЧЕСКИ СЛОЖИЛОСЬ»

ИМПОРТОЗАМЕЩЕНИЕ и БЮДЖЕТИРОВАНИЕ

Предвидение VBA

Strategic Moves For Competitive Advantage Accelerating

The Landscape Of Buyers For Cybersecurity Companies Has Expanded Over Time.



Most Active Acquirers

intel Security, cisco, THOMA BRAVO, paloalto, Google, FireEye, MARLIN EQUITY, proofpoint, RAPID7, IBM, Symantec, Vista Equity Partners, Microsoft

Notable Deals By Sector

PE

- Vista Equity Partners → Infoblox — 9/16: $1.3B / 3.5x
- TPG → McAfee — 9/16: $4.2B / NA
- Vista Equity Partners → PingIdentity — 6/16: $600M / NA

IT

- ORACLE → palerra — 9/16: NA / NA
- avast! → AVG — 7/16: $1.5B / 3.4x
- cisco → CloudLock — 6/16: $293M / 10.0x+
- Symantec → BLUE COAT — 6/16: $4.7B / 7.9x
- FireEye → iSIGHT PARTNERS — 1/16: $275M / 6.9x
- splunk> → Caspida — 7/15: $190M / NA

Industrial / IoT

- HARMAN → TOWERSEC — 1/16: NA / NA
- BELDEN → tripwire — 12/14: $710M / 6.0x
- ROHDE&SCHWARZ → gateprotect — 7/14: NA / NA

ISP

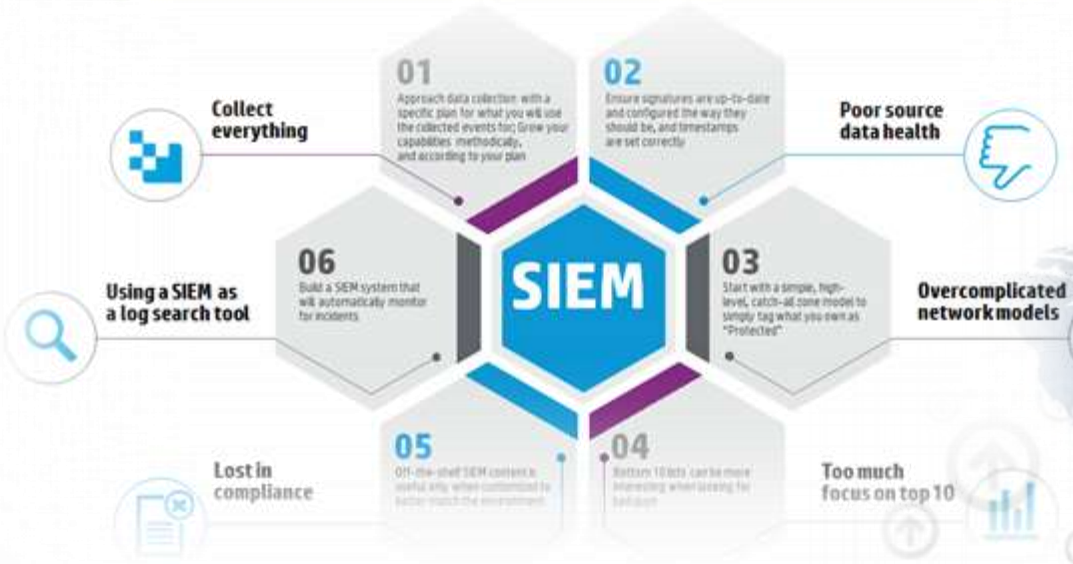
- Ruckus → Cloudpath — 10/15: $9M / NA
- Level(3) → Black Lotus — 7/15: NA / NA
- SingTel → Trustwave — 4/15: $786M / 3.6x

Defense

- THALES → Vormetric — 10/15: $400M / 7.5x
- Raytheon → websense — 4/15: $1.9B / NA
- BAE SYSTEMS → SilverSky — 10/14: $233M / 3.0x

Source: Momentum Partners.

Аналитика больших данных



Vulnerability Management Lifecycle

Чего не хватает?

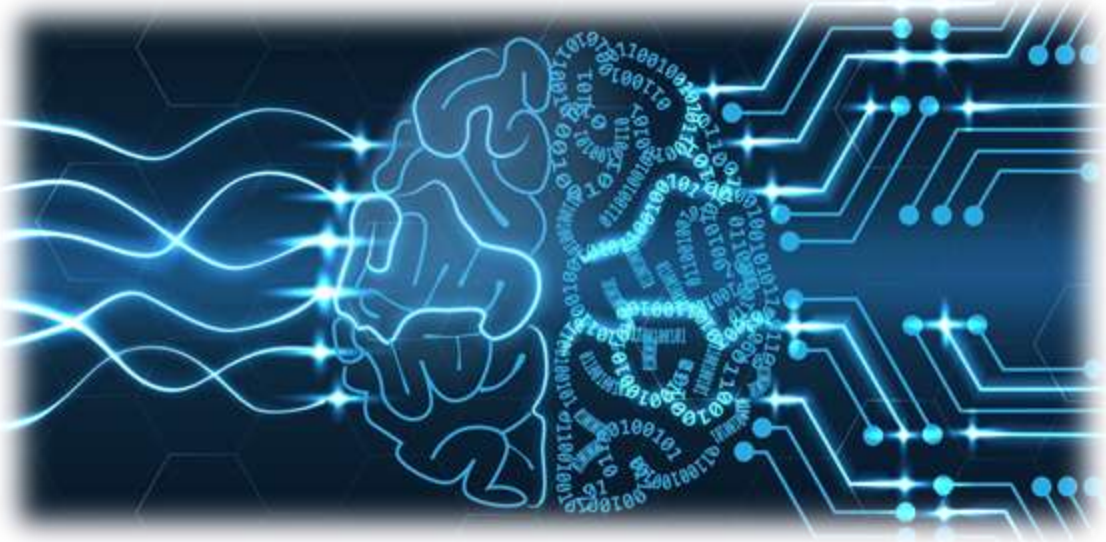
ОПЕРАТИВНОСТЬ РЕАГИРОВАНИЯ – пример WannaCry, Petya, etc.

ДИНАМИЧНАЯ ПОДСТРОЙКА решений автоматизации под новый тип угроз

ПУБЛИЧНОСТЬ кейсов по реализации систем защиты

ОРИЕНТИРОВКА регуляторного нормотворчества на изменения
во внешней среде

Искусственный интеллект vs белковый оператор



или

Что сделано в АО «СО ЕЭС»

Сделано:

- Централизованный контроль интернет-трафика, единая политика ограничения доступа в сеть интернет
- Централизованная организация процессов предоставления сетевого доступа
- Агрегация, хранение и аналитика информации о событиях ИБ в Центре
- Ежемесячная и ежеквартальная отчетность о событиях и инцидентах ИБ с вовлечением руководителей ИТ
- Ежеквартальные семинары с участниками команды SOC филиалов
- Внесение изменений в план проверок ИТ на основе анализа состояния ИБ

Планируется:

- Развитие существующих систем, выведение качества информации и эффективности внедренных процессов на новый уровень
- Автоматизация системы отчетности о состоянии ИБ
- Внедрение системы управления уязвимостями

Направления развития

Спасибо за внимание!

Палей Лев
АО «СО ЕЭС»

CNews ФОРУМ 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

CoNews FORUM 2017
2007-2017 лет