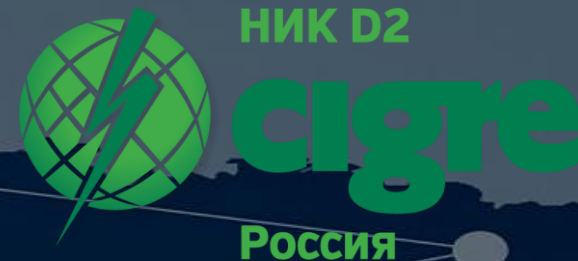


Некоммерческое партнерство
Научно-технический совет
Единой энергетической системы



Информационная безопасность – НОВЫЕ ВЫЗОВЫ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Литвинов Павел Васильевич,
эксперт РНК СИГРЭ,
зам. Председателя секции IT «НТС ЕЭС»

XII научно-практическая конференция в
рамках МФЭС 2023:

«Автоматизация и информационные
технологии в энергетике»

7 сентября 2023 г.

Новый глобальный вызов

Информационная безопасность все больше влияет на надежность электроснабжения

Что может помешать устойчивому развитию и функционированию электроэнергетики РФ?

- Серьезные ошибки в выборе траектории дальнейшего пути развития, главные из которых:
 - упустить **возможности**
 - не предусмотреть **риски**
 - ошибиться в **прогнозах**

Лучше прогнозировать

Контекст, в котором мы находимся сегодня (и это надолго):

- Будущее все труднее предвидеть, события развиваются быстро и «турбулентно»
- Неравномерность достижений и технического прогресса в разных областях
- Усиливающееся соперничество (санкции суть недобросовестная конкуренция)

Повышать конкурентоспособность

Риски и ограничения, **существующие и новые**

постоянные

Риски электроэнергетики как отрасли:

- аварии и техногенные катастрофы
- природные катастрофы
- непредвиденные изменения в спросе
- снижение инвестиций, несовершенство рынка
- изменение цен на электроэнергию и энергоресурсы
- изменение законодательства
- отток специалистов
- ошибки в проектировании и производстве
- недостатки в строительстве

новые растущие

Необходимо прогнозировать при планировании развития:

- «**Декарбонизация и энергетический переход**», инициативы по введению трансграничного углеродного регулирования, а по сути, налога на экспорт ископаемого топлива;
- «**Санкции**» – это не только ограничение доступа к технологиям, но и недобросовестная конкуренция;
- «**Изменение климата**» – количество стихийных бедствий неуклонно растет во всех категориях: геофизические, метеорологические, гидрологические, что приводит к снижению надежности энергоснабжения и увеличению потребности в электроэнергии
- «**Киберугрозы**» – вредоносное воздействие на ИТ инфраструктуру может привести к массовым сбоям, даже повреждению первичного оборудования
- «**Терроризм**» – особенно в приграничных территориях. К сожалению и ВЛ и ОРУ подстанций очень уязвимы.

Глобальные экологические и климатические задачи, стоящие перед человечеством, политики упростили. Основной угрозой назвали глобальное потепление, основной причиной – выбросы углеводородов, а виновной, без долгих научных изысканий, назначили традиционную тепловую энергетику.

Известные вызовы и способы противодействия



С какими **новыми** вызовами мы столкнулись?

В первую очередь с **модификациями** «старых»!

Наблюдаются изменения в **ресурсном обеспечении, способах и количестве атак**

- Хактивизм или «идейное» хакерство. Одно из последствий, все больше программ шифровальщиков не предусматривают восстановление данных
- Кооперация хакерских группировок. Обмен инструментами и результатами проведенных взломов. Самое неприятное, что к этому, разумеется, получают доступ и спецслужбы.
- Вовлечение «втемную». Например, предоставление инструментов для организации DDoS атак неопределенному кругу лиц, вовлечение даже несовершеннолетних.

В отрасли удалось обеспечить **адекватное противодействие:**

Благодаря «старым» инструментам:

- Выполнение приказов ФСТЭК
- Требования по шифрованию ФСБ
- Классификация объектов КИИ
- Создание центров ГосСОПКА
- Сертификация и аттестация

НОВЫЕ ВЫЗОВЫ И ВОЗМОЖНОСТИ



С чем столкнулись впервые?

Качество, спектр решений и функциональность значительного числа проектов open source ПО обуславливают его все более широкое применение. Проекты часто обновляются с целью расширения возможностей и исправления ошибок.

Преднамеренное внесение в код свободного программного обеспечения уязвимостей

- back door для облегчения последующего взлома
- Нарушение функциональности
От простого отказа в работе, до более коварного искажения результатов.
- Автоматическая активация и применение, если ПО работает на территории России или в определенных организациях

Были единичные случаи, которые сообщество разработчиков осудило, поскольку такие действия дискредитируют саму идею

Регулярная публикацией «Рекомендаций по минимизации возможных угроз ИБ» Национальным координационным центром по компьютерным инцидентам изложенных:

- понятным языком;
- максимально актуальных;
- предельно конкретных



Регуляторы активизировали общение с представителями отрасли и экспертным сообществом. Например, в рамках «Экспертной группы по кибербезопасности» Ассоциации «Цифровая энергетика»



- Можно сделать вывод, что повсеместно наблюдается отход от порочной практики «бумажной безопасности»

Common Vulnerability Scoring System (CVSS)



CVSS v.4.0



CVSS v.4.0 является развитием CVSS v.3.1

Планируется, что стандарт будет опубликован 1 октября 2023 года. Ждем официальной публикации!

– изменений не было

– существенные изменения

– добавлено в CVSS v.4.0

– отсутствует в CVSS v.4.0

ИБ с точки зрения практики



Безопасное функционирование и устойчивое развитие



Задачу обеспечения ИБ можно представить в виде аналога пирамиды Маслоу для психологии.

В основании лежит выполнение требований регуляторов – без этого невозможен легальный бизнес

Устойчивость бизнеса – это в первую очередь снижение риска катастрофических последствий

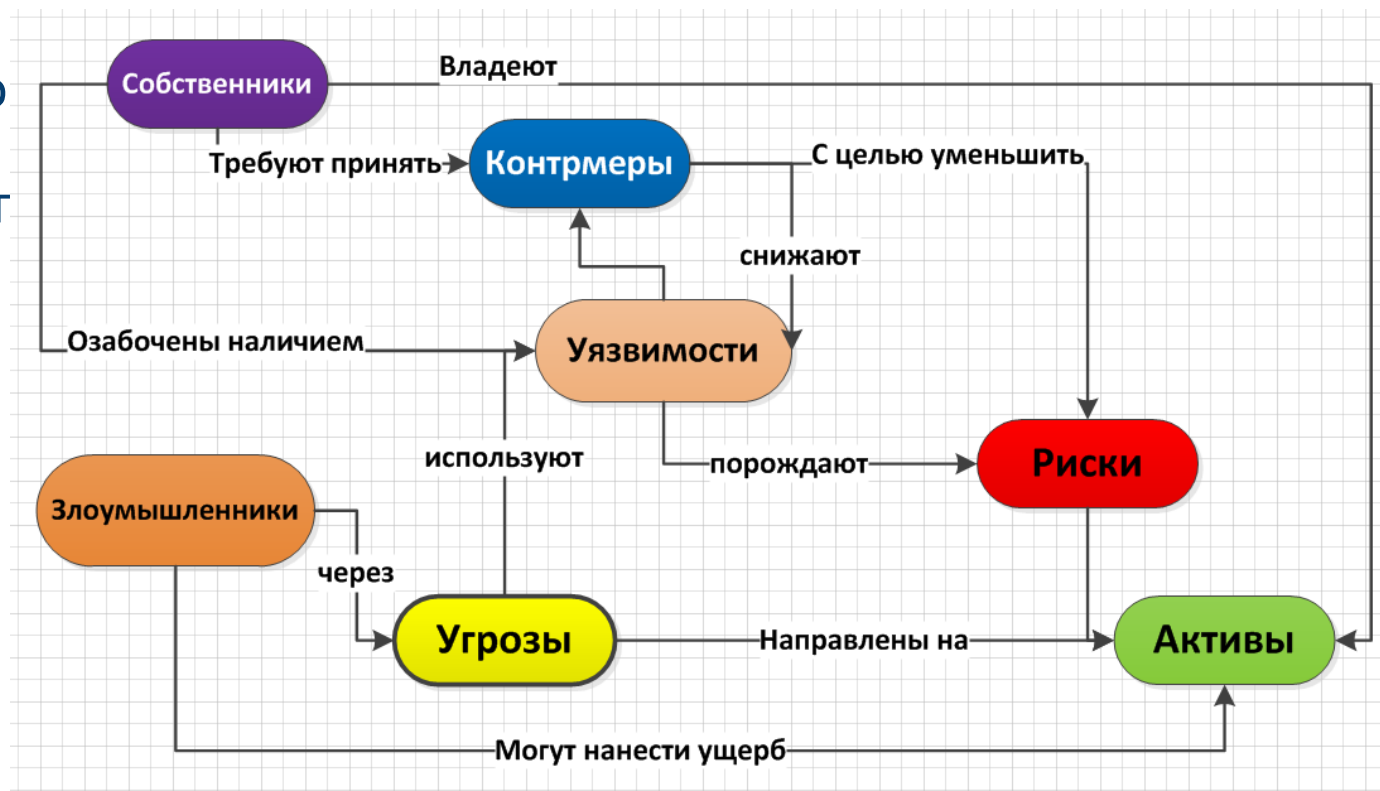
А достижение верхнего уровня – эффективности мероприятий, невозможно без ситуационной осведомленности

Частые ошибки при планировании ИБ?



Концептуальная модель информационной безопасности

- Неправильная оценка текущего состояния
- **Ошибки в распределении ресурсов**
Безопасность комплексное понятие помимо ИБ туда входит, как минимум, физическая защищенность, пожарная безопасность и т.г
- **Непропорциональный выбор решений**
ИБ – это тоже бизнес и маркетинговые компании игроков могут быть очень убедительны. Избыточные решения могут даже увеличить «поверхность для атаки»
- Пренебрежение простыми инструментами, например, организационного плана
- Ошибки в учете «человеческого фактора»



Предметная область сложна и специфична, но поддается декомпозиции :)

Как их избежать?



- Развитие и обучение собственной команды
Часть профильных специалистов должны освоить функцию ИБ, как дополнительную компетенцию
- Привлечение консультантов
- Использование передового опыта, в том числе зарубежного
Лучшие практики хорошо документированы, есть в открытом доступе, например, в рабочих группах CIGRE
- Обмен опытом со смежными компаниями в отрасли, научной школой
- Взаимодействие с ГосСОПКА, даже если вы не объект, для которого это обязательно
- Принятие решений, основанных на объективных и актуальных данных и фактах
С опорой на современные достижения статистики, аналитики технологий искусственного интеллекта и обработка данных

Стандарты и мировой опыт

- **NERC-CIP** (США и Азия);
- **BDEW White Paper** (Германия, Европа);
- **ISA-62443 (International Society of Automation)**
- **NIST Special Publications 800 series** (США);
- **ISO 27000 series** (международные)
- **Ausgrid** (корпоративный, Австралия)
- **CIGRE**



Это только источники! Каждый источник содержит десятки, иногда сотни документов.

Разумно не доверять устройствам и ПО, но специально плохих стандартов не напишут :)

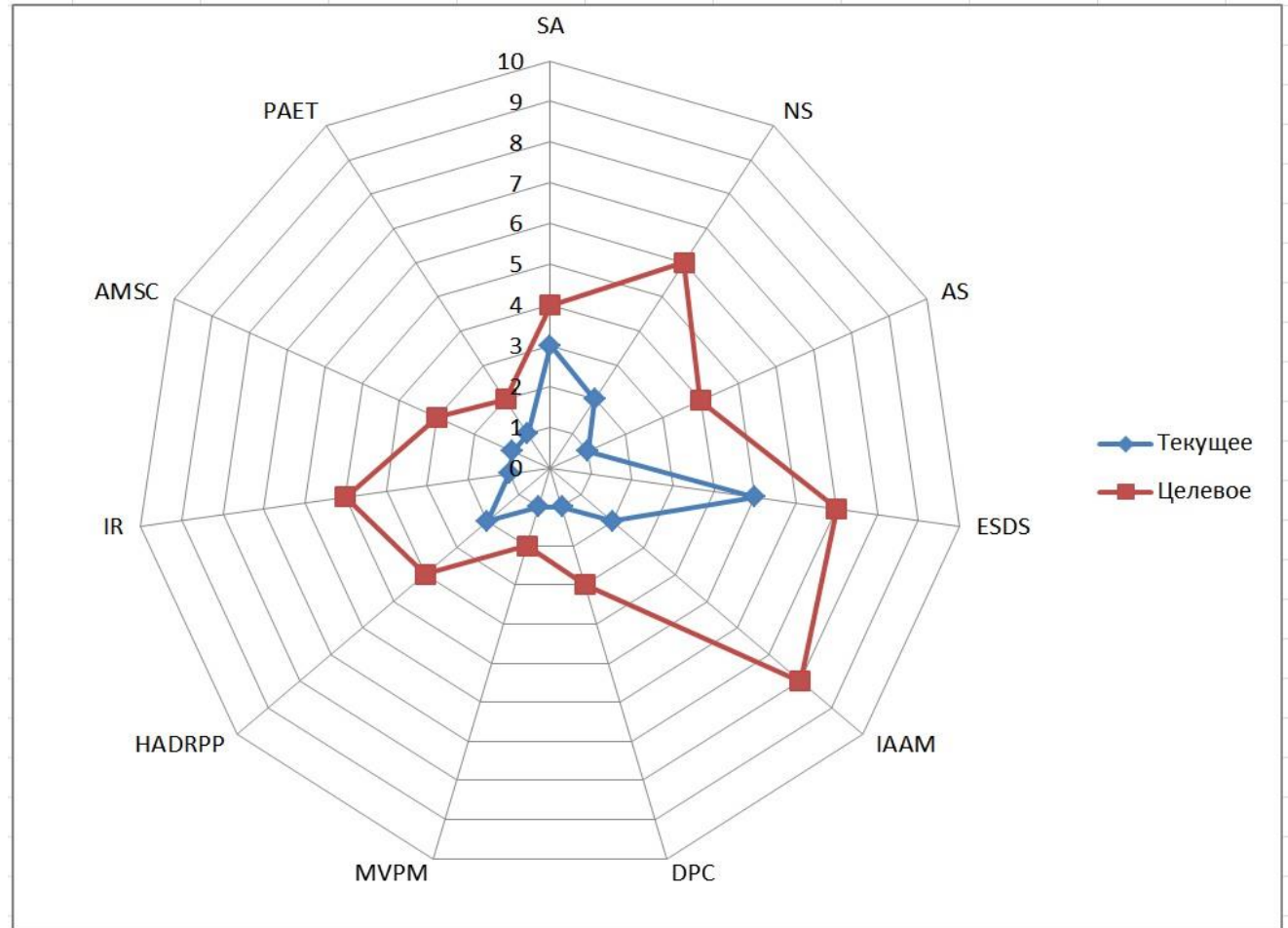
Планирование или другой способ декомпозиции



Наглядное представление текущего и целевого состояния

Вариант сегментации мероприятий по обеспечению ИБ

- Системное администрирование (SA)
- Сетевая безопасность (NS)
- Безопасность приложений (AS)
- Безопасность рабочих станций, серверов и устройств (ESDS)
- Идентификация, аутентификация и управление доступом (IAAM)
- Защита данных и криптография (DPC)
- Мониторинг, управление обновлениями (MVPM)
- Аварийное восстановление и физическая защита (HADRPP)
- Реагирование на инциденты (IR)
- Управление активами и поставками (AMSC)
- Политики безопасности, аудит и обучение персонала (PAET)



В зависимости от выбранного стандарта количество доменов может колебаться от 10 до 35!

Перспективные подходы



Другая парадигма. Безопасность должна быть не наложенной, а встроенной: неотъемлемой частью архитектурных и технических решений;

Использование достижений искусственного интеллекта. В энергетической системе можно создать аналог иммунной системы, когда нетипичное или технологически опасное поведение диагностируется, локализуется и автоматически блокируется;

Эшелонированная оборона. Слишком дорого поддерживать уровень максимальной киберзащищенности. Разумно использовать уровни угроз и план действий для каждого из них;

Использование «honeypot». Позволяет обнаружить атаку, оценить перечень средств и методов хакера и автоматически перевести критические компоненты системы в защищенный режим;

Технологии распределенного реестра. Для ряда технологических задач технологии блокчейн могут быть лучшей альтернативой шифрованию;

Создание отраслевых SOC или подключение к уже существующим сервисам.

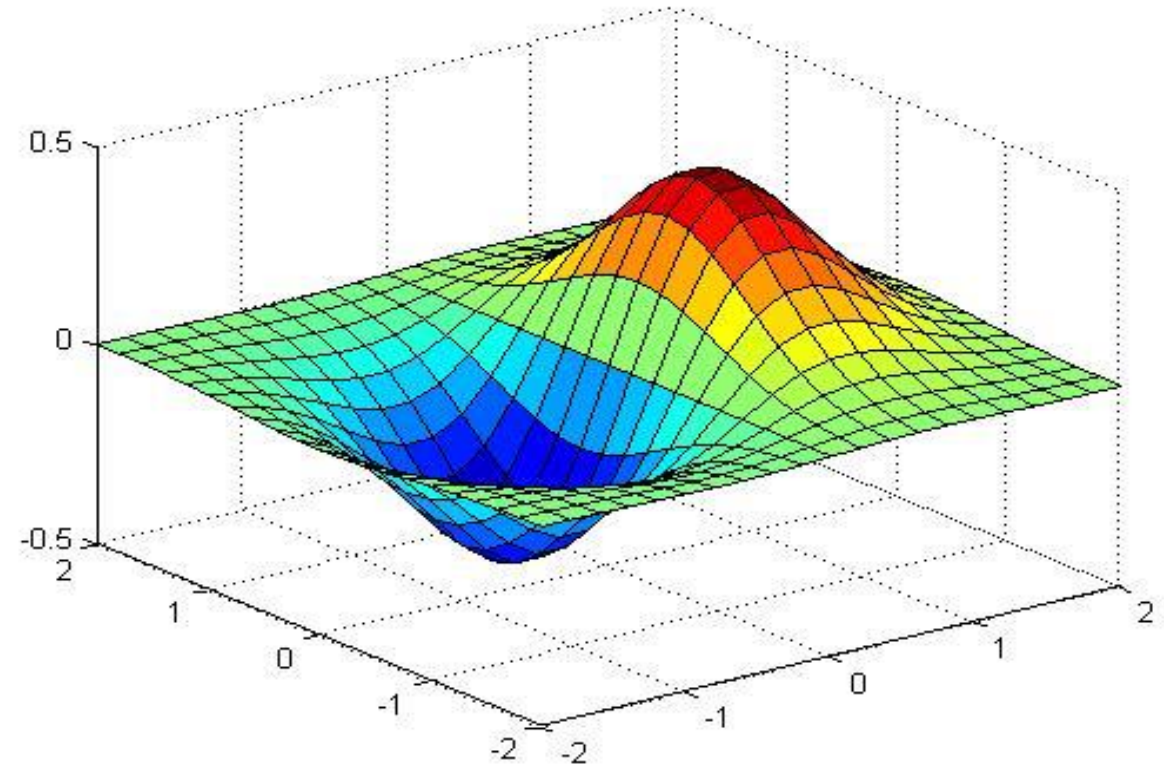
Имитационное моделирование и цифровой двойник. На модели можно «проигрывать» множество сценариев «что если» и в результате более обосновано планировать организационные и технические мероприятия по обеспечению информационной безопасности.

Простыми их назвать нельзя... Это долгая дорога!

Имитационное моделирование



- Имитационное моделирование новый быстроразвивающийся тренд, который позволяет строить модели на стыке разных дисциплин. Например, экономики, ИБ и технологии.
- **ИТ инфраструктура и ее защищенность успешно описывается графами**
- Многофакторный анализ сложная задача, но математический аппарат, хорошо разработанный для других областей, пока мало используется в ИБ
- И специалистам и лицам, принимающим решения остро не хватает наглядной визуализации и простых метрик.



Модели могут стать одним из факторов, снижающих нагрузку на специалистов по ИБ, и позволяющие получить объективную картину путем расчета большого количества сценариев

Специализированные информационные системы



Активы	Процессы	Уязвимости	Угрозы	Риски	Контрмеры (защита)	Инциденты	Документы	Отчеты	Справочники	Утилиты
Активы	Организационная модель	Объекты защиты	Классификатор активов	Реестр активов						
Процессы	Классификатор процессов	Бизнес-процессы	Технологические процессы	Процессы ИТ						
	Матрица ответственности	Процессы менеджмента ИБ	Процедуры ИБ	Аудит ИБ						
Уязвимости	Классификатор уязвимостей	Форма регистрации выявленной уязвимости								
Угрозы	Классификатор угроз	Классификатор нарушителей	Реестр угроз							
Риски	Классификатор рисков	Мониторинг рисков	Оценки рисков	Анализ рисков	Коммуникация рисков					
Контрмеры (защита)	Политика ИБ	Цели ИБ	Критерии ИБ	Объект защиты	Профиль защиты	Защитные меры				
Инциденты	Классификатор инцидентов	Форма регистрации инцидента								
Документы	Законы	Стандарты	Инструкции							
Справочники	Технологии защиты	Поставщики решений	Решения по защите	Глоссарий терминов						
Утилиты	Генератор отчетов	Импорт	Экспорт	События триггеры	Уведомления					

- Область сложна и очевидна потребность в ИС для планирования, документооборота, отчетности и т.п.!

- У бухгалтерии 1С, юристов – Гарант, отдел сбыта – CRM, производство – ERP.

- С чем работают Ваши «безопасники»?!

Меню перспективной специализированной информационной системы, «Моделирования и поддержки жизненного цикла решений по обеспечению безопасности»

Практические рекомендации

Изолировать не критичные для бизнеса решения

Например, если ваш корпоративный сайт находится в той же серверной, что и производственные сервера, перенесите его на сторонний хостинг;

Уменьшить поверхность для атаки

Пересмотрите все унаследованные решения, которые мало используются, но продолжают работать в инфраструктуре, откажитесь от них;

Задуматься над политикой «нулевого интернета» в корпоративной сети

Ваши сотрудники все что им надо для общения и даже для работы смогут получить на своих смартфонах, планшетах, ноутбуках, не подключенных к корпоративной сети. Мобильный интернет в России быстрый и дешевый!

Пересмотреть политику резервирования. Убедиться, что можно подняться из Backup

Зачастую критичные для бизнеса файлы можно уместить на «бытовом» NAS;

Остерегаться субподрядчиков

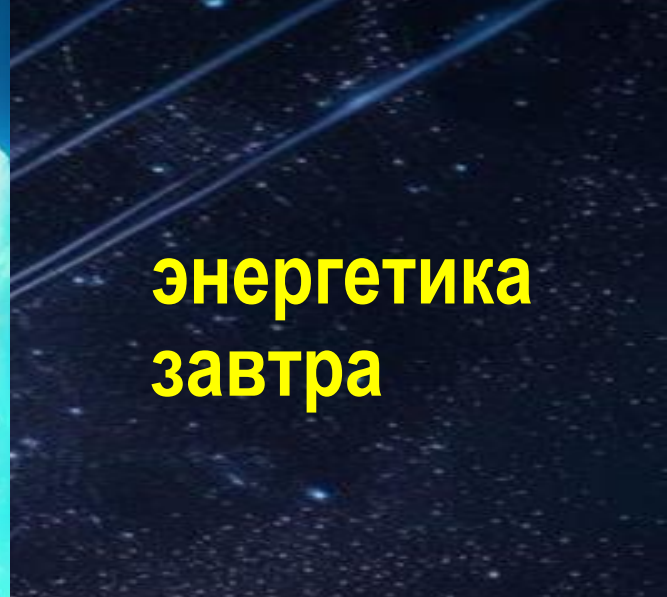
Если взломают, например, компанию, которая поставляет вам воду для кулера, а это сделать легко они не объект КИИ, то при наличии излишнего доверия «инфекция» может проникнуть и ваши ИС;

Вести журналы и логи событий, защищать их от изменений

Без них ни ваши сотрудники ни эксперты не смогут провести расследование атак и уязвимостей;

Не увлекаться борьбой с АPT угрозами

Как показывает практика, чаще всего проблемы возникают из-за элементарных просчетов и ошибок



**энергетика
завтра**

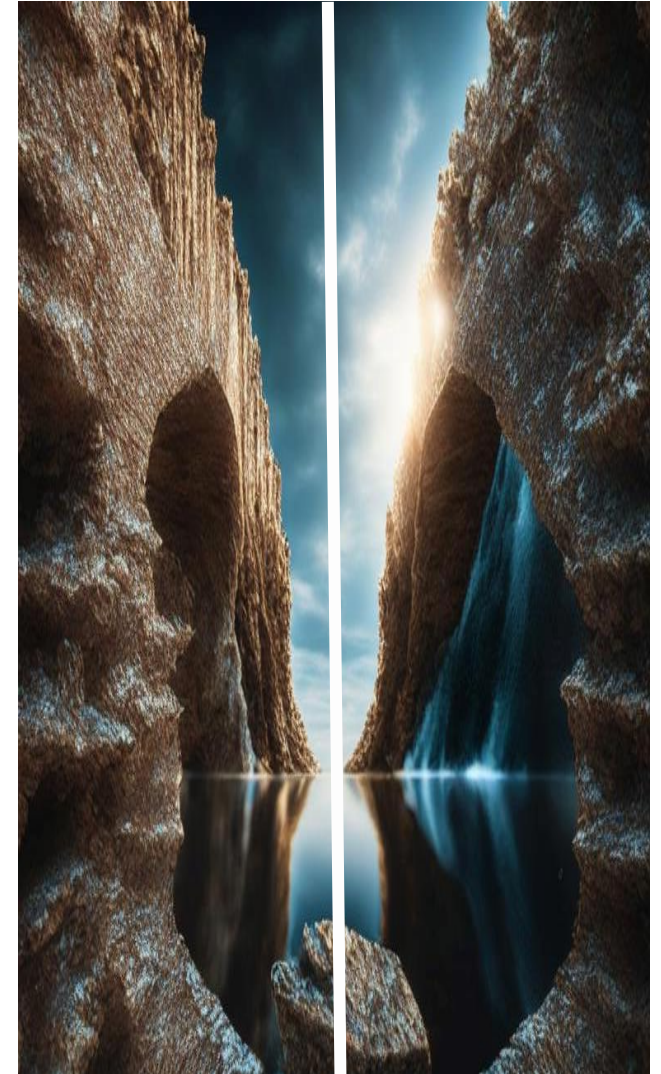


**надо уметь
мечтать**



Новая парадигма **обеспечения надежности** и => **ИБ**

- ✓ Переход к **управлению надежностью** с оптимизацией совокупных расходов энергетиков и потребителей на обеспечение надежности (**экономические стимулы**)
- ✓ Потребители принимают максимально активное участие в управлении нагрузкой, локальной генерации и резервировании (**концепция интернета энергии или ЭНЕРНЕТ**)
- ✓ Современные достижения в области информационных и телекоммуникационных технологий становятся **фундаментом** интеллектуальных электрических сетей (ИЭС).
(прикладной уровень – набор технологий smart grid)
- ✓ Государственная политика, закреплённая в программе «Цифровая экономика РФ» (**новая регуляторная база**)

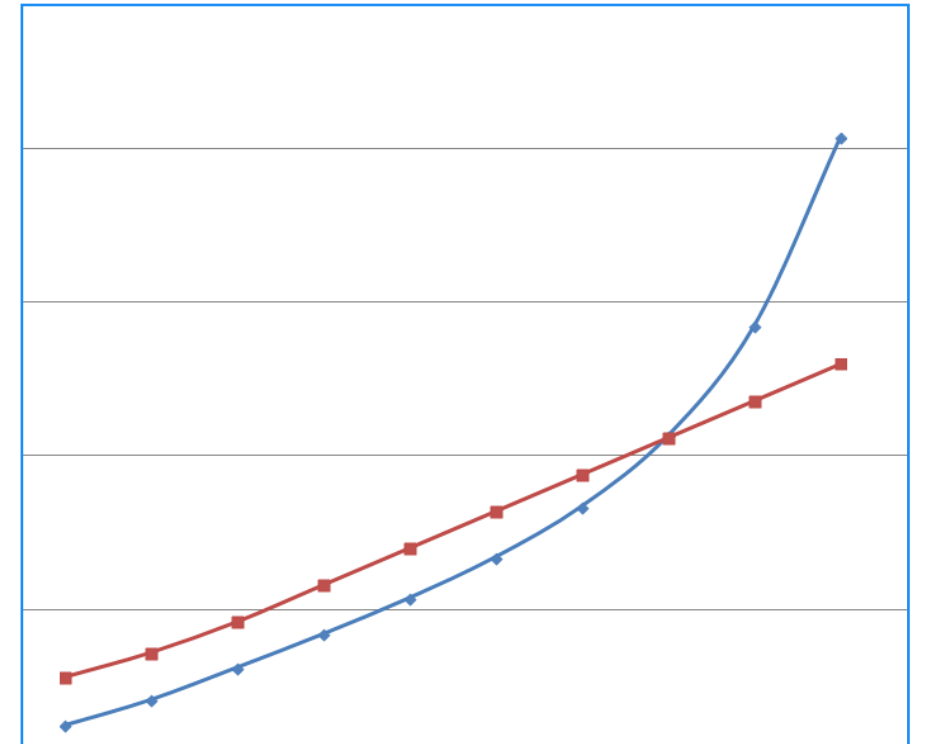


Эффект от перехода к **управлению надежностью**

$$\text{Риск} = \text{Вероятность (энергетики)} * \text{Ущерб (потребитель)}$$

- Задача энергетиков **уменьшить вероятность** перебоев в электроснабжении
Потребитель в свою очередь, должен принимать меры к **минимизации ущерба** от перерывов в электроснабжении.
- Это экономически целесообразно:
 - расходы на достижение и поддержание более высоких уровней надежности растут быстро и нелинейно (иногда экспоненциально!)
 - убытки от перерывов в электроснабжении, если предотвратить катастрофические последствия, линейно пропорциональны времени

—◆— Расходы энергетиков на повышение надежности
—■— Расходы потребителей на защиту от перебоев в электроснабжении



Как объединить существующие и **новые подходы?**

Начать можно с имитационного моделирования

- Методы расчетов структурной и балансовой* надежности электроэнергетических систем хорошо изучены и успешно применяются
- Результаты этих расчетов и существующую статистику отказов можно использовать для параметризации и верификации модели
- Можно начинать с верхнеуровневых моделей
- Брать в расчет только самые существенные факторы, влияющие на риски и гипотезы об их изменениях в ближайшие 10 лет.
- В качестве критерия, подлежащего оптимизации можно использовать совокупные расходы энергетиков и потребителей на компенсацию рисков.

В первом приближении составить реестр рисков и заполнить матрицу

Вероятность	Редко	Однажды	Случайно	Часто	Регулярно
Ущерб					
Незначительный	Light Green	Light Green	Light Green	Yellow	Yellow
Малый	Light Green	Light Green	Yellow	Yellow	Orange
Умеренный	Light Green	Yellow	Yellow	Orange	Orange
Большой	Yellow	Yellow	Orange	Orange	Red
Катастрофа	Yellow	Orange	Orange	Red	Red

Задача сложная, вероятность и ущерб определяются суперпозицией влияющих факторов и причинно-следственных связей, являющихся сложной функцией времени. Одни события могут быть триггерами для других и (или) существенным образом влиять на вероятность и ущерб.

* СТАНДАРТ СТО 59012820.27.010.005-2018
«Методические Указания по проведению расчетов балансовой надежности»

Выводы и предложения

- **Смена парадигмы: от обеспечения безопасности к управлению безопасностью** – техническая, экономическая и законодательная поддержка новых отношений энергетиков-производителей и потребителей – Интернета энергии или ЭНЕРНЕТ
 - **Цифровая трансформация на службе надежности**
– составить реестр возможностей современных интеллектуальных информационных и коммуникационных систем и трендов, которые можно использовать для предотвращения рисков информационной безопасности снижения ущерба
 - **Онтология**
приступить к решению амбициозной задачи – перехода от словарей, таксономий, тезаурусов и тематических карт к отраслевой онтологии – новому уровню возможностей и семантической строгости (плюс машиночитаемость!)
 - **Информационная база** – аккумулировать в базе данных колоссальные объемы отраслевых знаний, опыта и идей, накопленные в научных статьях, диссертациях, результатах НИОКР, материалах CIGRE, патентах посвященные теме надежности. Провести индексацию и анализ* с применением технологий Natural Language Processing, NLP
- * Хороший шанс найти идеи, которые в прошлом было сложно реализовать и про них забыли



НТС ЕЭС

НТС ЕЭС ▾

Новости

Коллегия ▾

Секции

События ▾

Публикации ▾

Партнеры ▾

Медиаотека ▾



Поиск

Некоммерческое партнерство
Научно-технический совет
Единой энергетической системы

Спасибо за внимание!



НТС ЕЭС

Опыт, квалификация и
надежность

Секция
Информационных
Технологий

[nts-ees.ru](https://www.nts-ees.ru)

<https://www.nts-ees.ru>

litvpv@yandex.ru

[@ntsees](https://t.me/ntsees)

<https://t.me/ntsees>