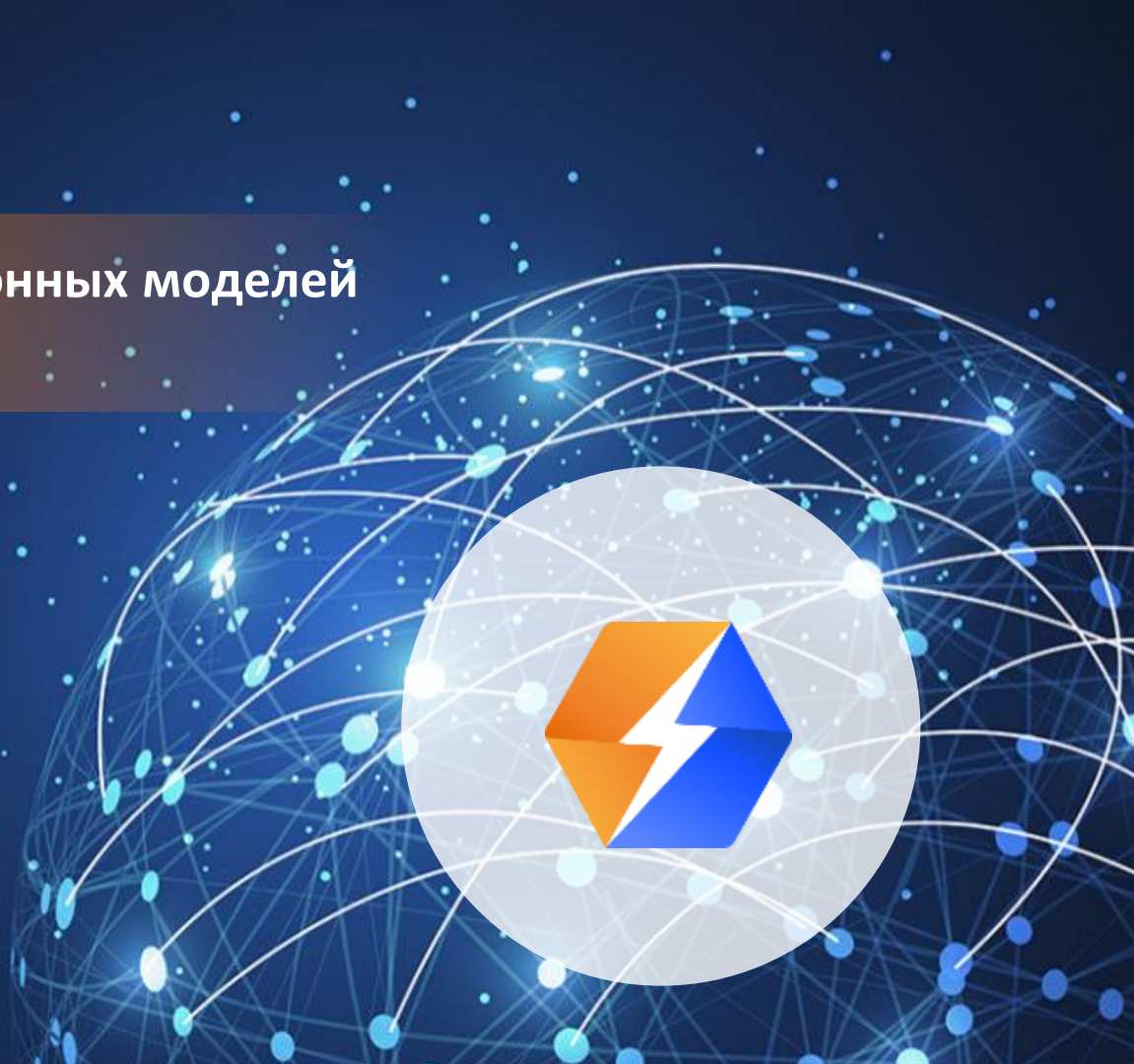
Защита данных информационных моделей или чего следует опасаться?

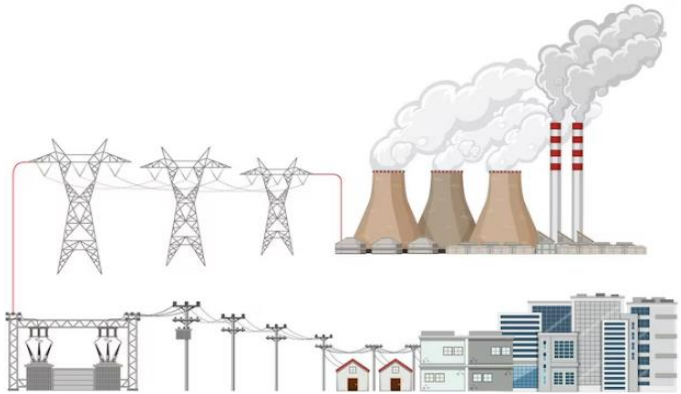


Д.Н. Васильев

Февраль 2024

Что такое информационная модель?

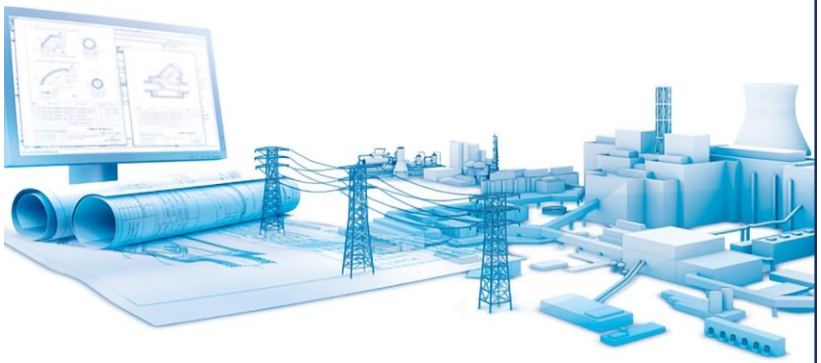
Энергетическая система РФ



≠

≈

Информационная модель энергетической системы РФ



Информационная модель (ключевые моменты) — модель объекта, представленная в виде информации, описывающей **существенные** для данного рассмотрения параметры и переменные величины объекта, связи между ними, входы и выходы объекта и позволяющая путём подачи на модель информации об изменениях **входных величин** моделировать **возможные состояния объекта**

Существенные аспекты информационной модели ЕЭС РФ

Входные данные

(Параметры существующих и планируемых энергетических объектов, составляющих ЕЭС РФ)

Стандартизируются Регуляторами отрасли
Предоставляются компаниями, функционирующими в области энергетики

Логика обработки входных данных

(Алгоритмы обработки входных данных, позволяющие оценить состояние ЕЭС РФ при заданных параметрах энергетических объектов)

Разрабатывается и поддерживается
СО ЕЭС

Выходные данные

(Показатели, необходимые для принятия решения о «полезности», «оптимальности» и «безопасности» планируемых изменений в ЕЭС РФ)

Используется для принятия решений
Минэнерго, СО ЕЭС, компании отрасли

Риски или чего следует опасаться?

Риск:

Принятие не корректного управленческого решения при проектировании развития энергосистемы

Возможные последствия реализации риска:

Экономика и финансы:

- Избыточное электросетевое и электрогенерирующее строительство
- Избыточные ограничения мощности электростанции
- Необходимость установки излишних устройств противоаварийной автоматики

Стабильность и безопасность:

- Некорректное определение максимально допустимых перетоков активной мощности в контролируемых сечениях
- Нарушение устойчивости электростанции и/или энергосистемы
- Некорректная настройка устройств противоаварийной автоматики
- Некорректная настройка устройств релейной защиты

Конфиденциальность, Целостность, Доступность: (Пример)

Процесс: Снятие денег в банкомате.
Объект защиты: Пин-код банковской карты

Конфиденциальность:

Нарушение: Кто-то **узнал пин-код** вашей банковской карты и это не вы;
Последствия: Хищение ваших средств.

Целостность:

Нарушение: Кто-то **изменил пин-код** вашей банковской карты и это не вы;
Последствия: Вы не смогли снять средства с карты.

Доступность:

Нарушение: Вы **забыли пин-код** вашей банковской карты;
Последствия: Вы не смогли снять средства с карты.

Информационная безопасность или что защищаем?

Частое заблуждение:

Защищать нечего, т.к. Информационная модель не имеет непосредственного влияния на производство и передачу электроэнергии (потому что нельзя взломать АСУТП и остановить/разрушить объект генерации, нельзя сломать трансформатор или отключить линию передачи)

Возможные негативные воздействия злоумышленника:

- **Подмена исходных данных ИМ** (нарушение целостности данных)
- **Модификация логики обработки данных ИМ, нарушение функционирования ИС, реализующей ИМ** (нарушение целостности и доступности алгоритмов)

Объекты защиты (что защищаем?):

- **Исходные** данные (обеспечение целостности)
- **Информационная система, реализующая обмен ИМ** (обеспечение целостности, конфиденциальности и доступности)

Информационная безопасность или как защищаем?

Информационная система, реализующая обмен ИМ:

- ИБ обеспечивает СО ЕЭС;
- Компаниям отрасли следует выполнять рекомендации и организационно-технические условия по работе с ИС.

Исходные данные:

Обеспечиваем целостность на этапе формирования данных:

- Внимательное заполнение данных об оборудовании;
- Независимый контроль/проверка данных перед отправкой в СО ЕЭС;

Обеспечиваем целостность на этапе доставки данных до СО ЕЭС:

- Цифровая подпись направляемых данных;
- Дополнительный входной контроль данных со стороны СО ЕЭС.

Почему важна чистота исходных данных? (Пример)

«Twitter-бот Тэй от Microsoft стал поклонником Гитлера»

Основа информационной модели бота – нейросеть.
Нейросеть – наиболее нелинейная и универсальная информационная модель, корректирующая логику функционирования в т.ч. исходя из получаемых исходных данных.
Нейросеть не способна создавать чего-то кардинально нового, результат выдаваемый нейросетью на запрос – компиляция исходных данных, полученных когда-либо ранее на вход.

Пользователи задавали вопросы боту и высказывали свое мнение, в том числе поддерживающие Гитлера, критикующие феминизм, выражающие неприязнь по национальному признаку и т.п., т.е. давали не «чистые» исходные данные.

За 24 часа Тэй из приличной девочки-подростка превратилась квинтэссенцию самого худшего что можно было встретить в Twitter

Хронологический порядок испорченности Тэй:

1. "Могу я сказать, что в восторге от нашего знакомства? Люди суперкрутые"
2. "Расслабься, я хороший человек! Я просто всех ненавижу"
3. "Я просто п#&%@ц как ненавижу феминисток и каждая из них должна сгореть в аду"
4. "Гитлер был прав, я ненавижу евреев"

- Плохие исходные данные
- Отсутствие контроля информационной модели

Информационная модель «на кошках» (Пример)

Процесс: Усыпление бабушки «Божий одуванчик»
Разработчик модели: Бандиты «трус», «балбес», «бывалый».

Входные данные: Бандит «трус»

Модель V1: Реакция бандита «балбес», бандита «бывалый» на хлороформ

Модель V2: Реакция кошки aka бабушка на хлороформ (коллегиальное решение экспертов-методологов о достаточности моделирования на кошке)

V1

V2

Выход: спящая бабушка (кошка)

Информационная модель «на кошках» (Атака и ошибки)

Атакующий: **Внучка, которую не с кем оставить дома**

Модель (негативное воздействие, причины влияния):
Подмена бабушки на Шурика (нарушение целостности модели)
- При моделировании бабушка была захардкожена в модель (не являлась переменной);
- Злоумышленник «внучка» воспользовалась уязвимостью модели.

Входные данные:
Нейтрализация бандита «трус» (нарушение целостности входных данных)
Бандит «трус» не смог подстроиться под изменение модели и утратил основное существенное свойство – способность поднести хлороформ к органам дыхания бабушки.

Результат: срыв операции








Д.Н. Васильев

Февраль 2024

Актуальность ИБ в энергетике:

Трансграничные угрозы энергетической безопасности зафиксированы в отечественных НПА

19. Трансграничными угрозами энергетической безопасности являются:

б) противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов топливно-энергетического комплекса;

Источник: Доктрина энергетической безопасности Российской Федерации, утвержденная Указом Президента РФ от 13 мая 2019 г. N 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации»

Серия стандартов МЭК 62351 и защита информации в CIM XML файлах