

ПОВЫШЕНИЕ НАДЕЖНОСТИ СИСТЕМ ЭНЕРГЕТИКИ В УСЛОВИЯХ ИННОВАЦИОННЫХ И ТЕХНОЛОГИЧЕСКИХ ОГРАНИЧЕНИЙ

Рогалев Н.Д., Литвинов П.В., Прокофьев П.С.,
Молодюк В.В., Исамухамедов Я.Ш.

**Некоммерческое партнерство «Научно-технический совет
Единой энергетической системы»**

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ СЕМИНАР им. Ю.Н. Руденко
МЕТОДИЧЕСКИЕ ВОПРОСЫ ИССЛЕДОВАНИЯ
НАДЕЖНОСТИ БОЛЬШИХ СИСТЕМ ЭНЕРГЕТИКИ

96-е заседание
«Надежность систем энергетики:
устойчивое развитие и функционирование»

15 – 19 июля 2024
г. Архангельск

Смена ландшафта

За минувшие два года произошла резкая смена технологического и политического ландшафта: широкий спектр возможностей, связанных со стремительным развитием информационных технологий и искусственного интеллекта, совпал с беспрецедентным санкционным давлением

Поскольку оба тренда: позитивный и негативный — сформировались надолго, планирование мероприятий по обеспечению надежности ЭЭС требует переосмысления и поиска новых подходов и решений.



«Старые» и новые вызовы

Осознанные вызовы:

- Энергетический переход
- Санкции
- Изменение климата
- Киберугрозы
- Терроризм

Компенсационные меры понятны и выработаны, но требуют затрат времени и денег

Новые глобальные вызовы:

- **Темп изменений** – в отрасли длительный производственный и жизненный цикл десятки лет, у новых технологий уже ~ 5 лет.
- **Структура занятости** – снижается потребность в специалистах «средней» квалификации, а именно таких готовит система образования
- **Поляризация и радикализация** – не только в межгосударственных отношениях и в политике, но и в принятии технических решений.
- **Смена поколений** – порождает новые «архетипы» поведения сотрудников, меняются понятия карьеры, ответственности, долга

Одновременное изменение окружающей среды, технологического ландшафта, политической ситуации помноженные на ускоренное развитие этих процессов дают «кумулятивный» эффект.

Мы **не успеваем** адекватно реагировать.

Это касается: системы образования, планирования развития, распределения ресурсов.

Классификация вызовов и влияния на надежность

Вызов	Степень влияния, длительность	Описание влияния
1. «Осознанные» вызовы. Компенсационные меры выработаны		
Энергетический переход	Слабое, долговременное	Положительное за счет диверсификации источников электроснабжения, отрицательное за счет оттока денежных средств
Санкции	Среднее, краткосрочное	Отрицательное на первом этапе за счет ограничения доступа к технологиям и техническому обслуживанию существующего парка устройств. Положительное в долгосрочной перспективе
Изменение климата	Значительное, долговременное	Рост числа аварий и неравномерности потребления, вызванный природными факторами
Киберугрозы	Среднее, среднесрочное	Увеличение числа компонентов и сложности систем. Появление нового класса причин отказов: вирусы, хакерские атаки, несанкционированный доступ. Усиление влияния на надежность человеческого фактора через социальный инжиниринг и сложность обслуживания
Терроризм	Сильное, краткосрочное	Физическая защита объектов энергетической структуры чрезвычайно сложная и затратная задача, ввиду пожароопасности генерации и большой протяженности распределения
2. Глобальные процессы. Отсутствие опережающего реагирования		
Темп научно-технического прогресса	Слабое, долговременное	Относительно медленное внедрение результатов научно-технического прогресса, особенно в области информационных технологий
Поляризация и радикализация общества	Сильное, среднесрочное	Проявляется в межгосударственных отношениях, политике и даже в принятии технических решений
Структура занятости в отрасли	Среднее, среднесрочное	Снижается потребность в специалистах «средней» квалификации, а именно таких массово готовит существующая система образования
Смена поколений	Значительное, долговременное	Порождает новые «архетипы» поведения сотрудников, меняются понятия карьеры, ответственности, долга

Разнонаправленное влияние ИТ на **надежность**

Информационные технологии – ядро большинства современных инноваций и именно они попали под самые сильные санкционные ограничения

- Профильный Комитет в CIGRE носит название: **D2-Information systems telecommunications and cybersecurity**
- Название отражает очень грамотную декомпозицию на **информационные системы** и **телеком** и обратную сторону медали, проблемы которые они порождают – **киберугрозы**, следовательно **информационная безопасность**
- Если мы будем смотреть на информационные технологии с точки зрения их влияния на надежность систем энергетики, то убедимся в верности поговорки:

«у каждой медали есть обратная сторона», которая в том или ином виде существует почти во всех языках.

Влияние информационных технологий вообще, а современных в частности на **надежность** разнонаправленное:

- **Повышение** главным образом, за счет расширения возможностей мониторинга, диагностики, прогнозирования, планирования, проектирования, поддержки принятия решений и автоматизации.

- **Снижение** за счет увеличения числа компонентов и сложности систем. Появление нового класса причин отказов: вирусы, хакерские атаки, несанкционированный доступ. Усиливают влияние на надежность человеческого фактора через социальный инжиниринг и сложность обслуживания.

Распределение числа атак по секторам* в 2024 г.

Энергетика по числу атак находится на 10-ом месте это «всего» 2 %

- Число атак не отражает уровень серьезности и стоимость последствий
- Информация не может быть полной о числе, не говоря уж об ущербе
- Продвинутое АРТ атаки могут готовиться и длиться годами
- Усиливаются такие опасные тенденции как:
 - политически мотивированный хактивизм;
 - кооперация хакерских группировок;
 - вовлечение «втемную» через продажу или распространение вредоносного ПО;
 - участие спецслужб недружественных стран;

В отрасли удалось обеспечить адекватное противодействие, но успокаиваться рано.

*Источник: Аналитический отчет Лаборатории Касперского «Ландшафт киберугроз», 2024 г.



Классификация тактик злоумышленников

v15.1

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques

1. Разведка
2. Подготовка инструментов и ресурсов
3. Первоначальный доступ
4. Исполнение – атака, взлом, запуск вредоносного кода
5. Обеспечение постоянного присутствия
6. Эскалация привилегий
7. Избежание обнаружения

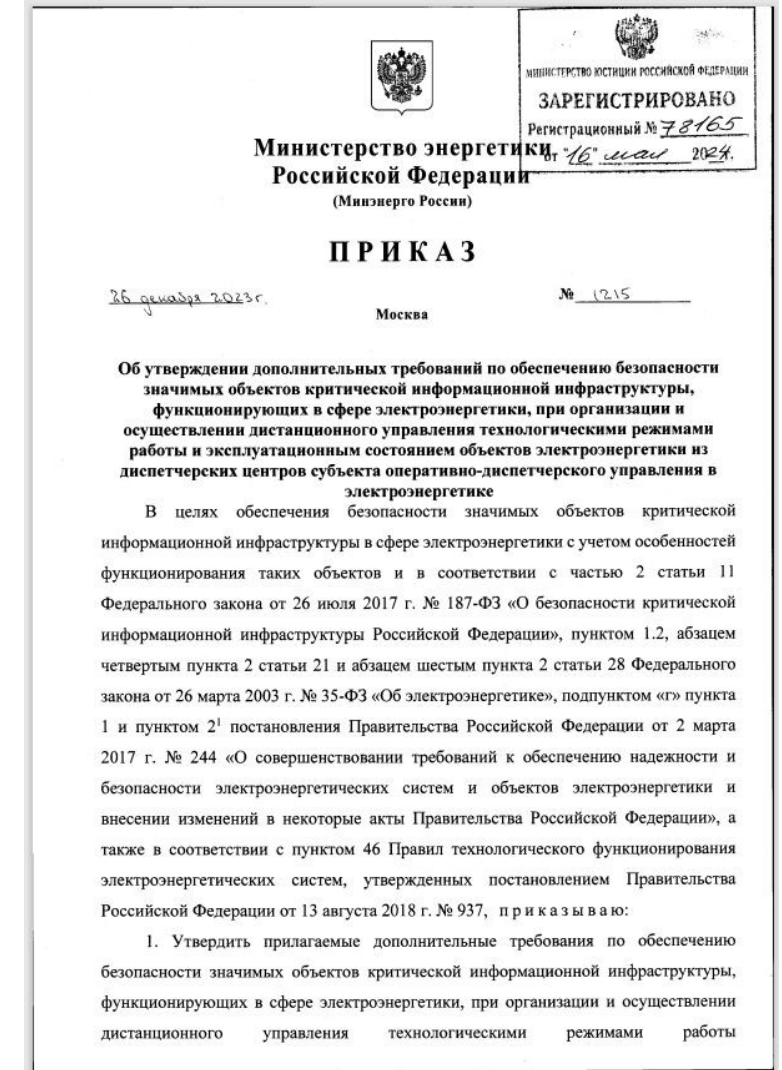
8. Доступ к учетным данным
9. Поиск и сбор данных
10. Миграция – расширения контроля и доступа
11. Сбор конфиденциальных данных
12. Управление и контроль
13. Вывод данных
14. Воздействие – продажа или уничтожение данных

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques

235 описаний техник кибератак находятся в публичном доступе и список пополняется!

Новеллы НТД

- приказ* Минэнерго от 26.12.2023 № 1215 «Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике»
 - Вступает в силу с **1 сентября 2024 г.** действует до 1 сентября 2030 г. * Полный текст (12 стр.)
 - Цель: устанавливает требования по защите трафика команд дистанционного управления средствами криптографической защиты. Выбор класса в зависимости от модели угроз.
-
- С **1 июня 2024** года вступил в силу приказ ФСТЭК России «Об утверждении Порядка проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации».
 - Данный документ важен для организаций-разработчиков СрЗИ.



Новые ограничения: сервера точного времени vs средств РЭБ

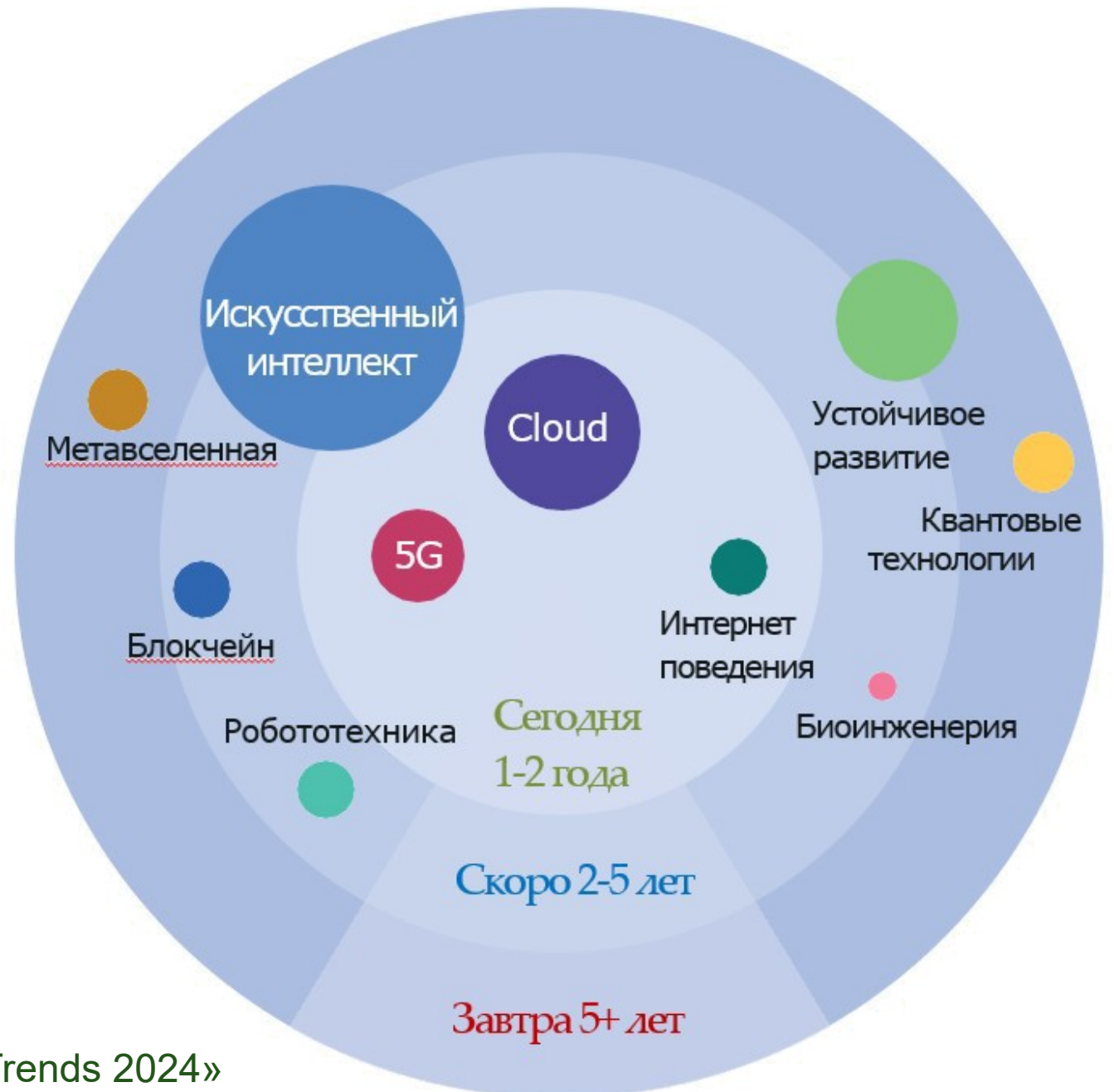
- Средства радиоэлектронной борьбы подавляют, а наиболее продвинутые искажают сигналы систем глобального позиционирования.
- Места их развертывания и график включения в работу по понятным причинам не доводится до гражданских организаций.
- Этот же сигнал используют сервера точного времени.
- Синхронизация времени критически важна для правильной работы систем релейной защиты, векторных измерений (СВИ) координации работы устройств автоматизации и т. п.
- **Этот пример показывает, как десятилетиями развивающееся и достигшее технического совершенства решение, может стать непригодным в условиях меняющейся реальности.**



Мегатренды*. Сроки, степень

Из диаграммы видно, что лидером изменений сегодня и на ближайшую перспективу является искусственный интеллект

- Наверное мы еще до конца не осознали масштаб связанных с этим изменений.
- Ранее механизмы, машины а затем и роботы освобождали людей от **тяжелого физического труда**. Компьютеры – от монотонных вычислений.
- Что происходит сейчас?
- ИИ «освобождает» нас от **легкого (пока) умственного труда** и многих видов творчества!
- Новые технологии не просто добавляют что-то в существующий мир, они кардинально меняют реальность.



* По версии HCL Technologies «HCLTech Trends 2024»

Актуальные тренды

Новые технологии уже не просто добавляют что-то в существующий мир, они кардинально и быстро меняют окружающую нас реальность

Мегатренды	Микротренды
Искусственный интеллект	Этичный, генеративный, машинное обучение
Устойчивое развитие	Глобальное отслеживание поставок, декарбонизация , зеленые информационные технологии
Облачные технологии	Мультиоблака, суверенные облака, конфиденциальные вычисления
Пятое поколение мобильной связи	5G: Сегментация , «автономный» 5G (без технологий 4G), фиксированный широкополосный доступ
Метавселенная	Виртуальная, дополненная и смешанная реальность , WEB 3.0, этичная расширенная реальность
Блокчейн	Криптовалюты, децентрализованные приложения , уникальные токены
Интернет поведения	Управление лояльностью клиентов , распознавание намерений, профайлинг
Робототехника	Автономные роботы, коллаборативные роботы
Квантовые технологии	Квантовые вычисления, квантовая криптография , квантовые технологии в машинном обучении

Перечень направлений НИОКР рекомендованных ПАО «Россети»*

№ пп	Область исследований	Актуальные направления исследований
1	Цифровой инжиниринг	Технологии Индустрии 4.0 для решения задач функционирования и развития электросетевого комплекса
		Единая цифровая модель электрической сети (СІМ-модель)
		Технологии повышения эффективности и надежности работы цифровых ПС и РЭС
		Технологии предиктивного прогнозирования и оценки эффективности их внедрения
2	Информационная и производственная безопасность	Обеспечение информационной безопасности и киберустойчивости информационных систем, информационно-телекоммуникационных систем, автоматизированных систем управления
		Перспективные технологии в области кибербезопасности технологий цифровой сети, интернета-вещей и криптографии
		Обеспечение и повышение инфраструктурной безопасности электросетевых объектов и энергосистем
3	Интеллектуальная диагностика	Системы цифрового мониторинга состояния работы электросетевых объектов
		Современные методы инструментального неразрушающего контроля выявления, верификации и ранжирования дефектов на электросетевых объектах
4	Развитие новых сервисов и услуг	Информационно-технологические архитектуры для зарядной инфраструктуры и/или управления спросом на электроэнергию
5	Интеллектуальный учет электроэнергии	Интеллектуальные системы учета электроэнергии
		Управление профилями нагрузки (база данных профилей, типизация, технологическое присоединение по профилю, разработки типовых графиков набора мощностей и т.д.)
6	Новое оборудование и технологии	Технологии и методы повышения эксплуатационного ресурса и технических характеристик оборудования ПС и ЛЭП
		Новые системы роботизации обслуживания ПС и ВЛ на отечественной элементной и программной базе
		Оборудование, технологии и материалы на базе отечественных решений для обеспечения технологической безопасности электросетевого комплекса
7	Энергосбережение и энергоэффективность	Энергоэффективные/энергосберегающие технологий и сервисы
		Технологии накопления электроэнергии для управления режимами работы энергосистем (включая автономное энергоснабжение)

*Перечень актуальных направлений исследований НИОКР, рекомендованных к реализации в группе компаний «Россети» в 2025-2027 гг.

Машинное обучение – прикладная часть ИИ

Возможности:

«Технологии предиктивного прогнозирования и оценки эффективности их внедрения» (пункт из Перечня направлений)

- Разработка новых стратегий управления, энергосбережения;
- Выявление паттернов аномалий; предотвращение аварий
- Интеллектуальная обработка данных о состоянии оборудования
- Предиктивная аналитика

Ограничения:

- Сложность выбора оптимального алгоритма или модели
- Скромная обучающая выборка по сравнению с другими отраслями
- Ограниченный круг задач требующих применения
- Конкуренция за специалистов

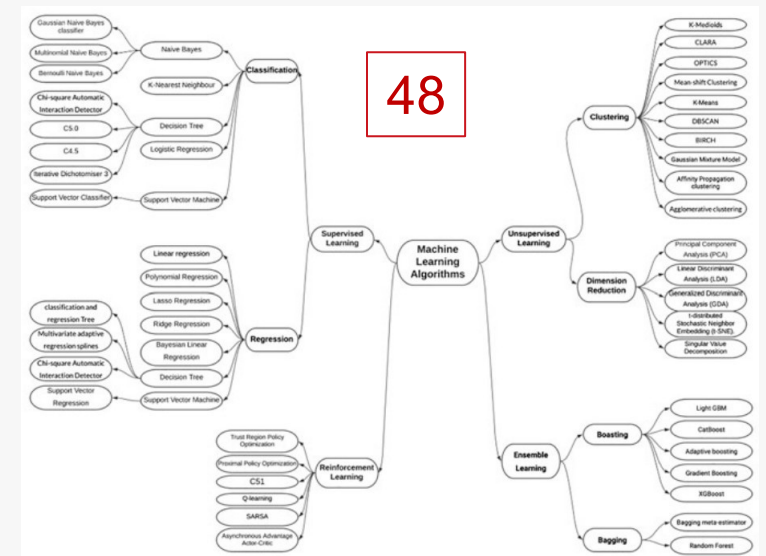
Риски:

- «Необъяснимость» результатов
- Снижение точности предсказания из-за «переобучения» модели

*Poornachandra Sarang, «Thinking Data Science», Springer 2023



Алгоритмы / модели нейронных сетей*



Виды моделей машинного обучения*

Мегатренды* 2024 г. и их перспективные направления (часть 1)

Мегатренд	Микротренды	Английские термины	Раздел НИОКР
Искусственный интеллект	Этичный, генеративный, машинное обучение	AI : Ethical AI, Generative AI, Machine Learning	Технологии предиктивного прогнозирования
Устойчивое развитие	Глобальное отслеживание поставок, декарбонизация , зеленые информационные технологии,	Sustainability: Supply Chain Track and Trace, Decarbonization, Green IT	Новое оборудование и технологии
Облачные технологии	Мультиоблака , суверенные облака , конфиденциальные вычисления	Cloud: Multi-cloud, Sovereign Cloud, Confidential Computing	Единая цифровая модель электрической сети
Пятое поколение мобильной связи	5G: Сегментация , «автономный» 5G (без технологий 4G), фиксированный широкополосный доступ	5G: Network Slicing, 5G Standalone, Fixed Wireless Access	Технологии Индустрии 4.0
Метавселенная	Виртуальная , дополненная и смешанная реальность , WEB 3.0, этичная расширенная реальность	Extended Reality (XR) (AR/VR/MR), Spatial Web, XR Ethics	Информационная и производственная безопасность (через обучение)

Мегатренды 2024 г. и их перспективные направления (часть 2)

Мегатренд	Микротренды	Английские термины	Раздел НИОКР
Блокчейн	Криптовалюты, децентрализованные приложения, уникальные токены	Blockchain: Cryptocurrencies, D-Apps, NFTs	Перспективные технологии в области кибербезопасности технологий цифровой сети
Интернет поведения	Управление лояльностью клиентов, распознавание намерений, профайлинг	Internet of Behavior: Behavioral Experience Orchestration (BEO), Behavioral Intent Recognition (BIR), Behavioral Profiling	Развитие новых сервисов и услуг
Робототехника	Автономные роботы, коллаборативные роботы	Robotics: Autonomous Robotics, Semi-Autonomous Robotics	Новые системы роботизации обслуживания ПС и ВЛ
Квантовые технологии	Квантовые вычисления, квантовая криптография, квантовые технологии в машинном обучении	Quantum Tech: Quantum Computing, Quantum Cryptography, Quantum Machine Learning	Перспективные технологии в области кибербезопасности
Биоинженерия	Персональная медицина, редактирование генома, орган на чипе	Bioengineering: Personalized Medicine, Genome Editing, Organ-on-chip	

Цикл зрелости технологии (Hype cycle) Gartner

Феномен «гражданских разработчиков» новое явление в разработке ПО, как результат развития low-code / no-code платформ

Все этапы:

- Инновационный прорыв
- Пик ожиданий.
- Пропасть разочарования
- Подъем на плато продуктивности
- **Плато продуктивности**

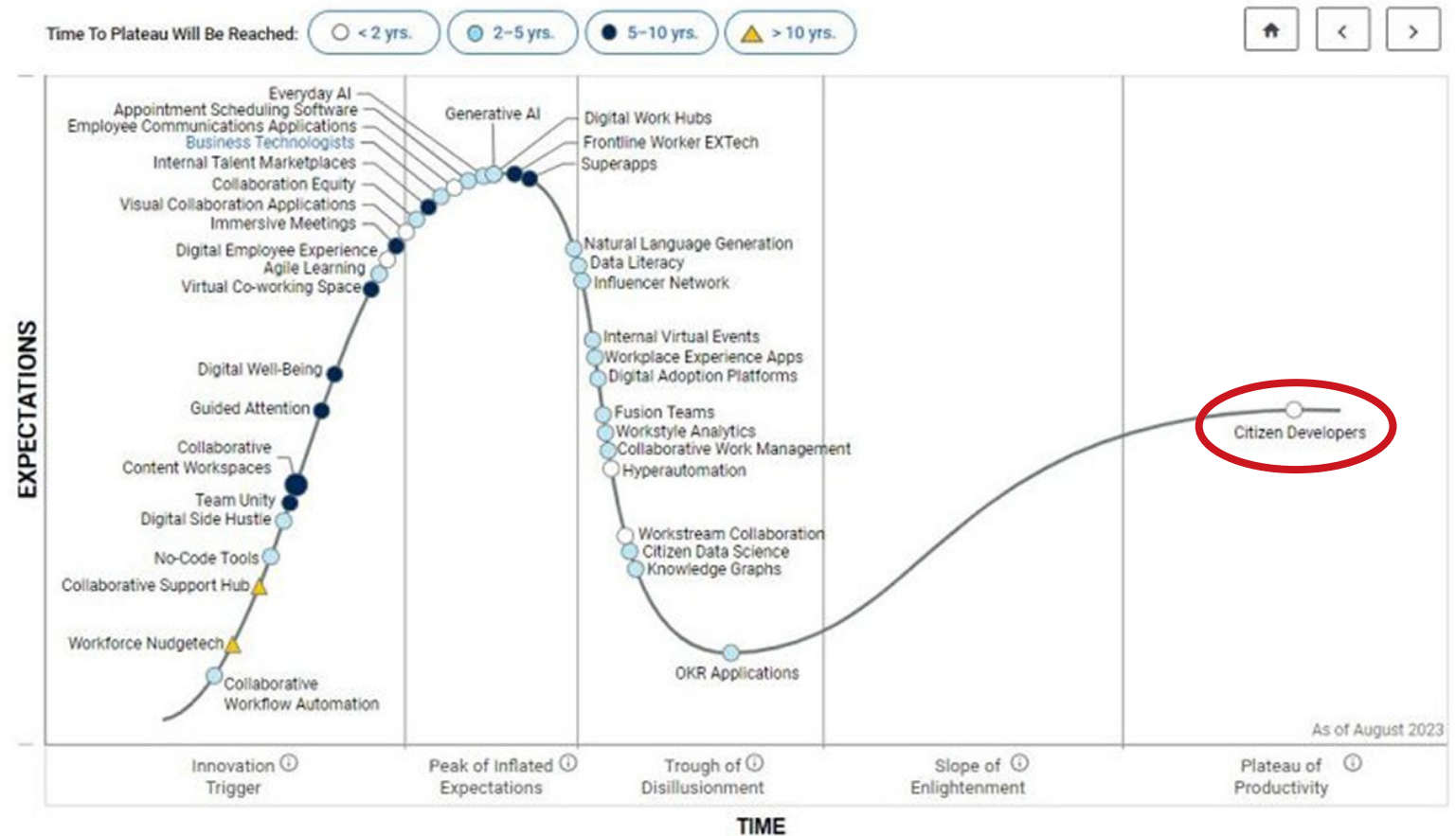
рассматривать не будем, на плато продуктивности находится только одна технология: **Citizen Developers**

Преимущества:

Снижение затрат, быстрое решение части проблем, вовлеченность, глубокая понимание специфики.

Ограничения:

Слабая безопасность, низкое качество, проблемы с этикой, отсутствие архитектуры.



Технологии и тенденции с наибольшим потенциалом

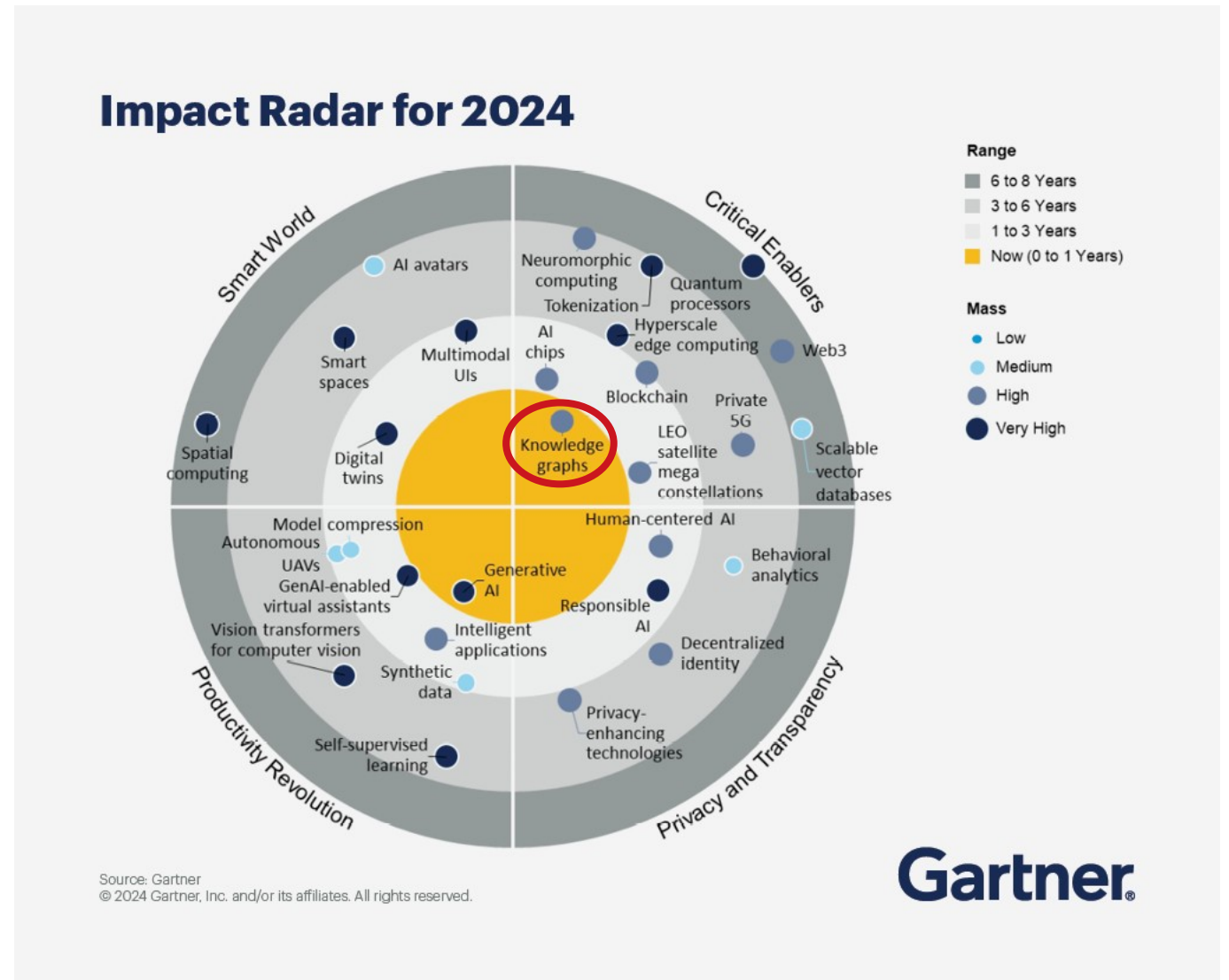
Базовым инструментом в 2024 г. объявлен **граф знаний** (knowledge graph) способ обработки, анализа и визуализации структурированных данных из различных источников, таких как базы данных, онтологии, семантические сети и т.п.

Где применить?

- «**Единая цифровая модель электрической сети (СИМ-модель)**» из программы НИОКР ПАО «Россети»
- **Преимущества:** эффективный поиск и извлечение информации, лучшее понимание контекста и связей между данными, поддержка автоматического вывода рекомендаций на основе семантического анализа.

Возможность. Создать онтологию объединяющую:

- Надежность
- СИМ-модель
- Информационную безопасность



Gartner®

Как усилить позитивное влияние ИТ на надежность?

Использовать **возможности**. Понимать **ограничения**. Управлять **рисками**.

- ❑ **Граф знаний.** Извлечение и консолидация опыта и знаний. Облегчение доступа специалистам, наглядная визуализация для лиц, принимающих решения
- ❑ **Low-code / no-code.** Возможность быстрой «разработки» и внедрения ПО специалистами отрасли уникальная возможность компенсировать недостаток прикладных программ, дефицит программистов и связанную с этим высокую стоимость и сроки разработки.
- ❑ **Машинное обучение.** Выявление паттернов и сценариев развития аварий по совокупности причин и (или) сочетанию факторов позволит своевременно предупреждать о снижении надежности.
- **Недостаток профильных специалистов.** Чем современнее технология, тем сильнее приходится конкурировать с банками, страховыми компаниями, ритейлом и девелоперами. Нужна отраслевая программа дополнительного обучения и мотивация.
- **Информационная безопасность.** Один из самых дешевых и достаточно эффективных способов – не просто убрать из открытого доступа (например ТЗ на тендерных площадках) информацию о составе информационных систем и оборудовании для их защиты, но и наводнить это же пространство дезинформацией. Расставить «наживки» (honeypot).
- **Физическая защита объектов.** Актуален знаменитый лозунг про спасение утопающих. Надо информировать силовые структуры (пример с GPS сигналом), и находить и применять недорогие «асимметричные» решения.

Программу НИОКР лучше разделить на три раздела и добавить в них «чистые» НИР и ОКР

Выводы и предложения

- **Одновременное и быстрое** изменение окружающей среды, технологического ландшафта и политической ситуации кардинально меняют реальность, включая изменение социума
- В новых условиях традиционное реактивное планирование, основой которого является принятие ответных мер на возникшие проблемы, уже не гарантирует необходимого уровня надежности ЭЭС
- Назрела необходимость перейти к **проактивному планированию**, в основе которого лежит **анализ трендов и прогнозирование будущих событий** с целью поиска новых подходов по обеспечению надежности ЭЭС
- **Опережающее применение** передовых современных информационных технологий в вопросах планирования и обучения, подготовки и переподготовки кадров будет необходимым шагом на пути к предсказуемому, эффективному и надежному развитию отрасли



НТС ЕЭС

НТС ЕЭС ▾

Новости

Коллегия ▾

Секции

События ▾

Публикации ▾

Партнеры ▾

Медиаотека ▾



Поиск

Некоммерческое партнерство
Научно-технический совет
Единой энергетической системы



НТС ЕЭС

Опыт, квалификация и
надежность

Спасибо за внимание!

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

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

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

<https://t.me/ntsees>