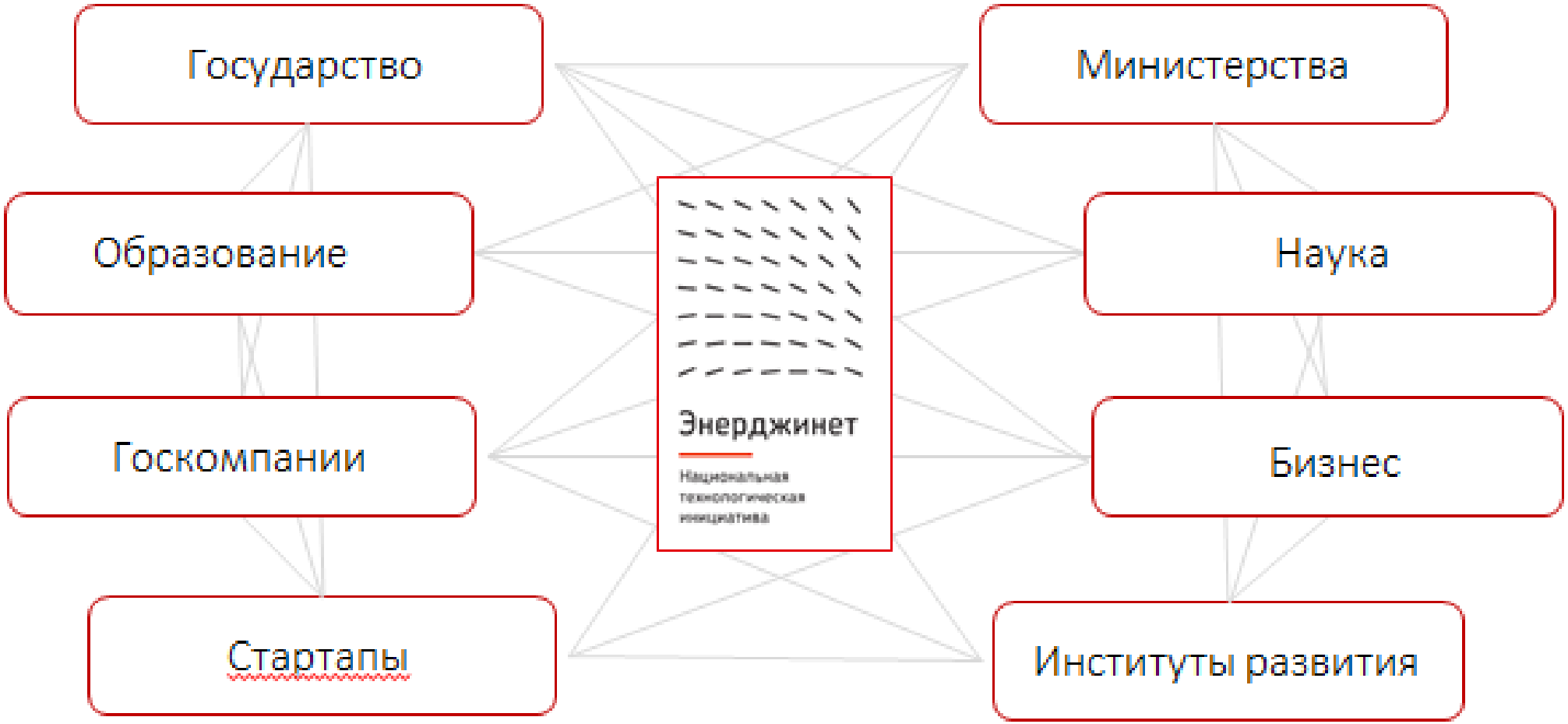
EnergyNet

Подгруппа по кибербезопасности

# Открытая база знаний Информационной безопасности

# Национальная технологическая инициатива Энерджинет / EnergyNet

**(НТИ Энерджинет)**



# Структура НТИ Энерджинет

Рабочая группа

Инфраструктурный центр

Архитектурный комитет

Группа НПА

**Подгруппа по кибербезопасности**

Экспертный совет
по нормативному регулированию

Межвеомственная рабочая группа по разработке и реализации НТИд

Сформирована в целях **выработки решений по информационной и кибербезопасности в электроэнергетике**.

Базовые направления деятельности:
— **Консалтинг и экспертиза** в части информационной и кибербезопасности

— **Разработка, внедрение и сопровождение** решений по информационной и кибербезопасности

— **Создание открытой базы знаний информационной безопасности** в электроэнергетике

# Потребности в открытой базе знаний информационной безопасности

Требуется **единая терминология** по информационной безопасности

Требуют **«синхронизации» НПА** для формирования единой картины требований и подходов к защите

Требуется **создание машино и человеко читаемой базы знаний**, для применения знаний по информационной безопасности в проектах

# Пример противоречия (2020)

**Методика моделирования угроз безопасности информации**

***Угроза*** *- неправомерные действия и (или) воздействия на информационные ресурсы или компоненты систем или сетей, в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей, повлекшее наступление негативных последствий*

**Мониторинг информационной безопасности. Общие положения.**

**Угроза** (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

*Данные противоречия устранены с выходом «Методики оценки угроз безопасности информации» 05.02.2021.

# Открытая база знаний информационной безопасности

## Функции первого этапа (2021)

1. **Выделение** основных терминов из текста и их **проверка на смысловое противоречие** друг другу
2. **Анализ документов** по существующей нормативной базе с целью формирования «базы исходных данных» (Автоматическое приводиться ссылки о том, в каком месте какого документа используется данное определение/термин)
3. **Словарь ИБ**, синхронизированный с нормативной базой

## Детали:

1. Форма визуализации и работы с базой – веб сайт
2. Предусмотрена возможность предлагать свои термины/корректировки к терминам через запросы к модераторам
3. Границы работ - ТЭК

# Открытая база знаний информационной безопасности

## Принцип работы

1. Существующие документы переводятся в машиночитаемый формат (в ручную, ограниченный перечень документов, ≈20 документов НПА РФ)
2. Создаётся ПО, способное понимать слова и термины, коррелировать их между собой на базе данных документов
3. Создаётся сайт для взаимодействия с ПО

## Особенности:

1. «Обучение» по смысловому пониманию слов и терминов выполняется человеком
2. Логика принимаемых ПО решений чётко регламентирована / прозрачна и корректируемы
3. Для вовлечения в проект не требуется специальных знаний по программированию

# Открытая база знаний информационной безопасности

## Ожидаемые эффекты

1. Оптимизация нормативной базы (инструмент будет полезен ФОИВ)

2. Повышение качества разрабатываемых / актуализируемых документов пользователями (все участники сферы ИБ)

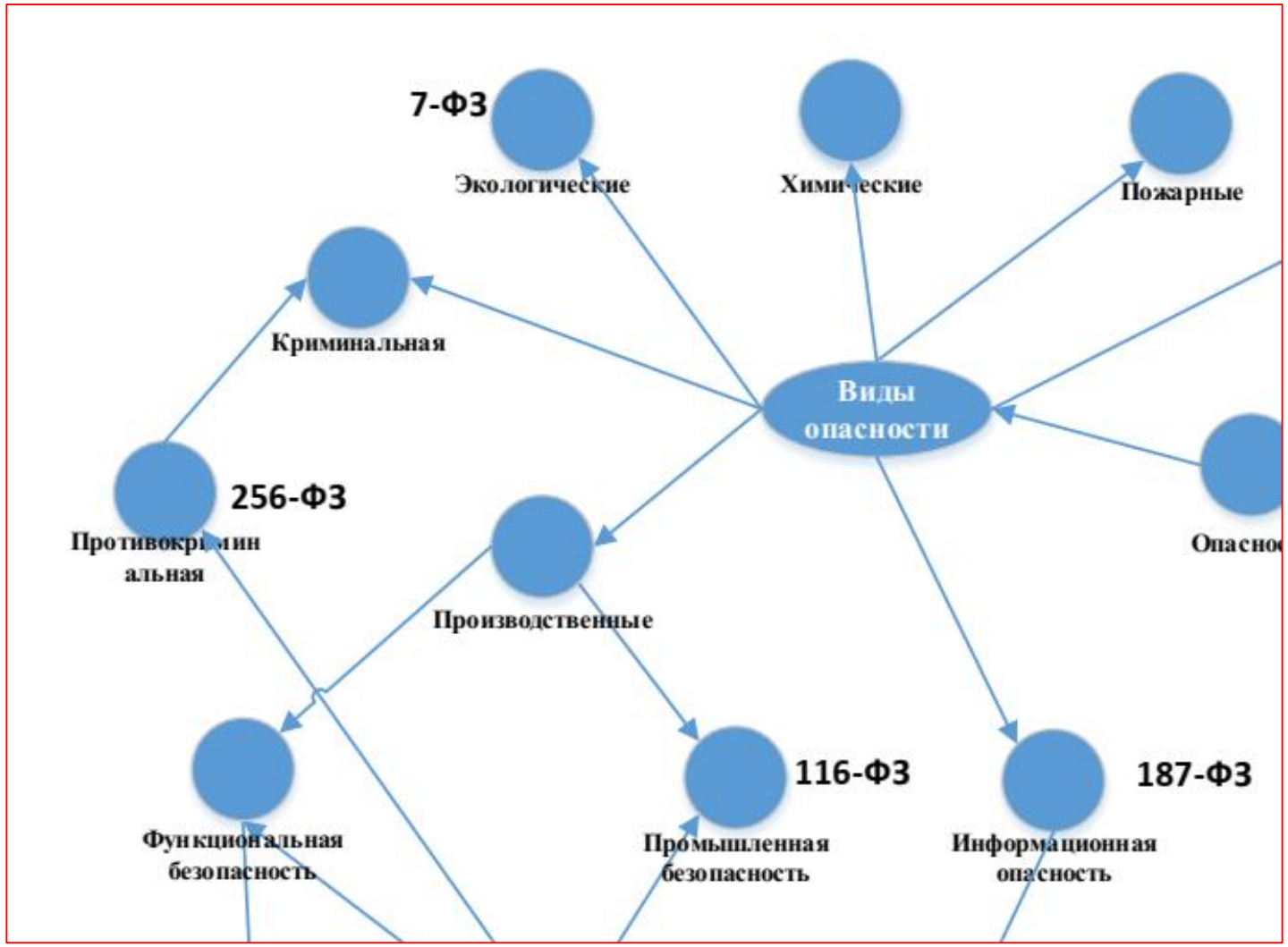
3. Создание платформы, для системного и интерактивного развития нормативной базы (все участники сферы ИБ)

kaspersky

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ и ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) имени И.М. ГУБКИНА

УЦСБ

# Открытая база знаний информационной безопасности



# Открытая база знаний информационной безопасности

| Русскоязычный термин | Определение | Источники |
|---|---|---|
| Объект защиты информации | Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации. | ГОСТ Р 50922-2006. Защита информации. Основные термины и определения |
| Недостаток (слабость) | Систематические слабые места (systematic weakness): Недоработки, которые могут быть устранены или влияние которых уменьшено только введением модификаций в проект, производственный процесс, процедуры эксплуатации, документацию или замены нестандартных компонент компонентами с более высокой надежностью. Остаточные слабые места (residual weakness).<br>Слабые места, которые не являются систематическими. остаточные слабые места (residual weakness): | ГОСТ Р 51901.6-2005. Менеджмент риска. Программа повышения надежности |
| Уязвимость | Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации | ГОСТ Р 56545-2015 |

# Присоединяйтесь!

EnergyNet

**Подгруппа по кибербезопасности**

Инфосистемы Джет

СИБИНТЕК

INFOWATCH®

МОИ

СИСТЕМА

kaspersky

iGrids интеллектуальные сети

РГУ нефти и газа
имени И.М. Губкина