kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Дмитрий Правиков

Директор Научно-образовательного центра новых информационно-аналитических технологий, РГУ нефти и газа им. И. М. Губкина

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина
ФАКУЛЬТЕТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ТЭК

ГАРМОНИЗАЦИЯ ЗНАНИЙ И ПРАКТИК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭНЕРГЕТИКЕ

Директор Научно-образовательного центра
новых информационно-аналитических технологий
факультета комплексной безопасности ТЭК
РГУ нефти и газа (НИУ) им. И.М.Губкина
к.т.н. Д.И.Правиков

ЦЕНТР КОМПЕТЕНЦИЙ «КИБЕРБЕЗОПАСНОСТЬ»

EnergyNet

Объединяем компетенции и формируем системный подход к обеспечению кибербезопасности

Базовые направления деятельности:
…разработка открытой онтологической модели кибербезопасности в электроэнергетике…

Цели:
…выработать единый понятийный аппарат в сфере кибербезопасности…

ПОЧЕМУ СТАВИТЬСЯ ТАКАЯ ЦЕЛЬ?

Интеграция IT и OT

Выявление фактов воздействия на защищаемые системы не только методами информационной безопасности, но и через отклонение параметров управляемых технологических процессов

Расширение понимания безопасности систем промышленной автоматизации, не отраженное, в том числе, в нормативных документах

В ЧЕМ ПРОБЛЕМА?

- выработанные подходы к обеспечению информационной безопасности АИС применимы для обеспечения систем промышленной автоматизации только частично;
- для промышленных производств характерна необходимость обеспечения широкого перечня безопасностей: функциональной, промышленной, противопожарной, экологической, информационной и т.п. взаимосвязь которых между собой неочевидна и не регламентирована;
- попытки вендоров и интеграторов учесть специфику промышленных производств породили термин «кибербезопасность», не поддерживаемого регуляторами;
- неконтролируемое заимствование международных стандартов привело к формированию обширного нормативного поля, содержащего внутренние противоречия;
- в целом отсутствует системный подход к обеспечению кибербезопасности систем промышленной автоматизации.

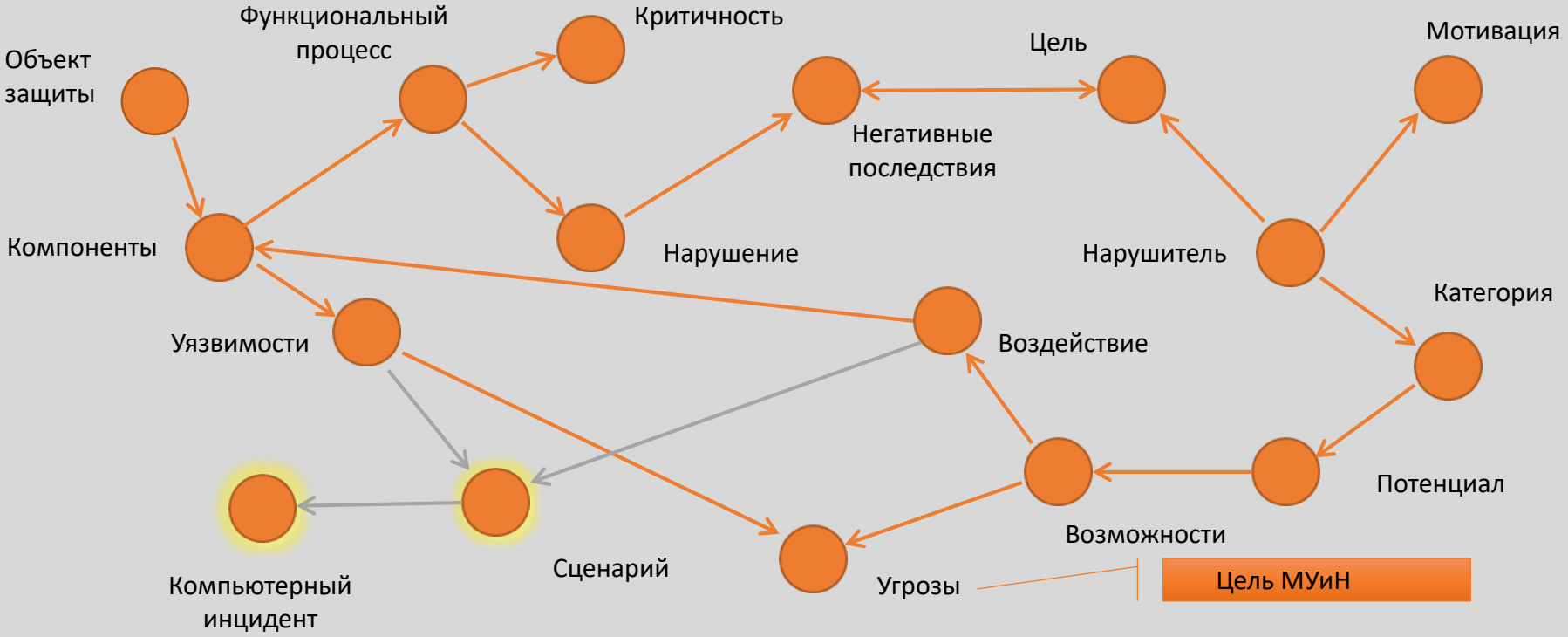
ПОНИМАНИЕ КИБЕРБЕЗОПАСНОСТИ

Кибербезопасность – безопасность защищаемого объекта, системы которого функционируют в условиях деструктивных информационных воздействий.
Группа «Кибербезопасность» ЭнерджиНет

Кибербезопасность (cybersecurity): Действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов.
ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009

- Высокая стоимость атаки
  - Уровень APT
  - Совершенствование защиты
- Эффективность выявления атаки
  - Время выявления
  - «Слабые» аномалии
- Нейтрализация последствий
  - Резервирование
  - Управляемая деградация
- Безопасная модификация системы
  - Зоны и связи
  - ZTA

ОНТОЛОГИЧЕСКИЙ АНАЛИЗ ПРОЕКТА МУИН 2020



ПРИМЕР ПРОТИВОРЕЧИЯ ПОНЯТИЙ

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

ПРИМЕР ПРОТИВОРЕЧИЯ ПОНЯТИЙ

Методика моделирования угроз безопасности информации

Компонент системы (сети): программное, программно-аппаратное или техническое средство, входящее в состав системы или сети.

Мониторинг информационной безопасности. Общие положения

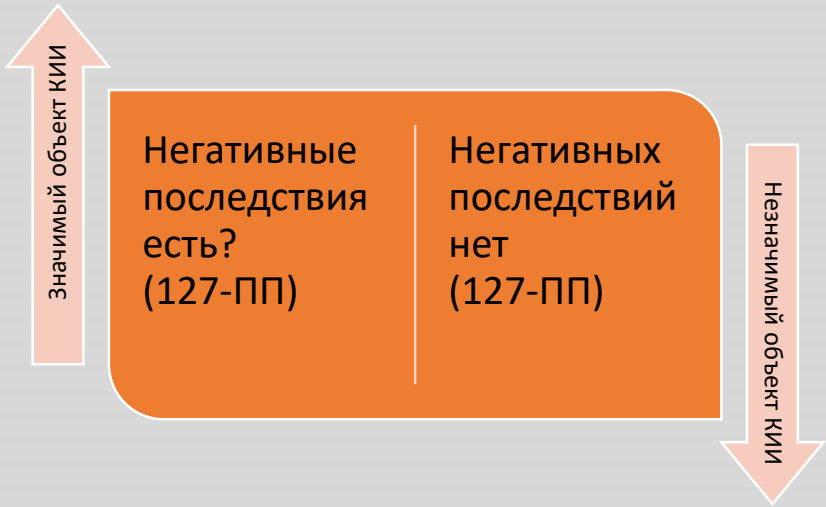
Узел информационной (автоматизированной) системы: Программно-техническое средство, предназначенное для выполнения определенных функций в составе информационной (автоматизированной) системы.

ПРОБЛЕМА ВЗАИМОСВЯЗИ ДОКУМЕНТОВ…

Проект МУиН 2020

Оценка негативных последствий	
Требования законодательства Российской Федерации	Проведенная обладателем информации (оператором) оценка ущерба (риска)

Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры ТЭК



НОСИТ СИСТЕМНЫЙ ХАРАКТЕР…

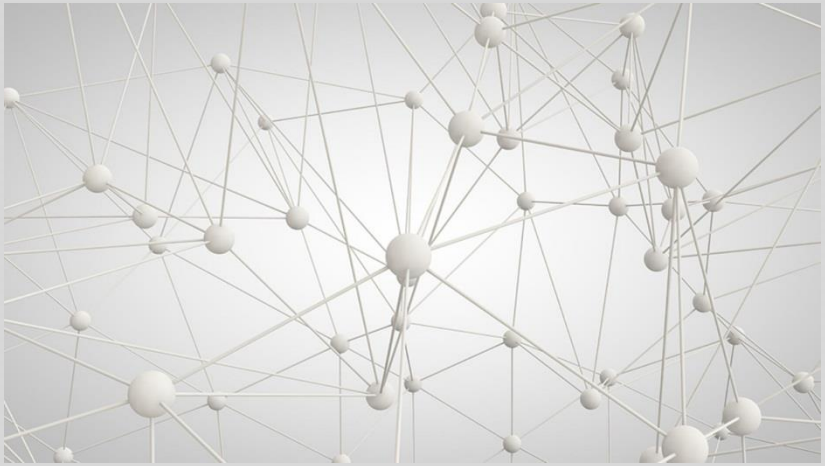
Текущая структура документов

Подмножество общих понятий

Перечень частных понятий

Набор положений (правил)

Общая картина связей



И НЕ ОБРАЗУЕТ ЦЕЛОСТНОЙ КАРТИНЫ

В общем случае отсутствует связь между конкретными требованиям, мерами, подходами и общей целью обеспечения кибербезопасности.

ПРЕДЛАГАЕМАЯ «КАРТИНА МИРА»

Общая открытая онтология кибербезопасности

- Доступна и признаваема экспертным сообществом
- Изменения редки и обусловлены существенными обстоятельствами

Нормативные и методические документы

- Имеют частные онтологии, детализирующие общую онтологию
- Описывают непротиворечивые правила и требования

Пропиетарные онтологии и продукты

- Согласуются с общей онтологией и нормативными документами
- Представляют know-how разработчиков

ПОИСК НАУЧНЫХ ПОДХОДОВ

1. Ворожцова Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности // Онтология проектирования. – 2014. - № 4(14), стр. 69 – 77.
2. И.Н. Пащенко И.Н., Васильев В.И., М.Б. Гузаиров М.Б. Защита информации в сетях Smart Grid на основе интеллектуальных технологий: проектирование базы правил // Известия Южного федерального университета. Технические науки. – 2015. - № 5 (166). – стр. 28 – 37.
3. Волошин А.А., Волошин Е.А., Бусыгин Т.Г. Разработка системы автоматического синтеза тестовых сценариев и проверки правильности выполнения ПНР комплексов РЗА ЦПС // Вести в электроэнергетике. – 2017. - № 4 (90). – стр. 44 – 50.
4. Массель А.Г., Гаськова Д.А. Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов // Онтология проектирования. – 2019. – т. 9, № 2 (32). – стр. 225 – 238

КРАТКОСРОЧНЫЙ ПЛАН РАЗРАБОТКИ ОНТОЛОГИИ

1. Формирование словаря терминов в области кибербезопасности на основании зарубежных онтологий.
2. Поиск и соотнесение с ними соответствующих терминов в российской нормативной базе.
3. Формирование единого российского словаря терминов в области кибербезопасности.
4. Формирование связей между терминами (концептами) в области кибербезопасности.
5. Гармонизация связей с зарубежными онтологиями.

НАШЕ CREDO

1. Разработка открытой онтологии кибербезопасности является открытым проектом.
2. Коллектив участников не ограничен.
3. Научный и экспертный подход, использование существующих наработок.
4. Взаимодействие с регуляторами и экспертным сообществом.
5. Результаты используются в регуляторной, научно-технической и образовательной деятельности.

БЛАГОДАРЮ ЗА ВНИМАНИЕ

dip@gubkin.pro