Киберучения как новая форма производственной деятельности, направленной на повышение защищенности и устойчивости функционирования систем промышленной автоматизации

Карантаев Владимир

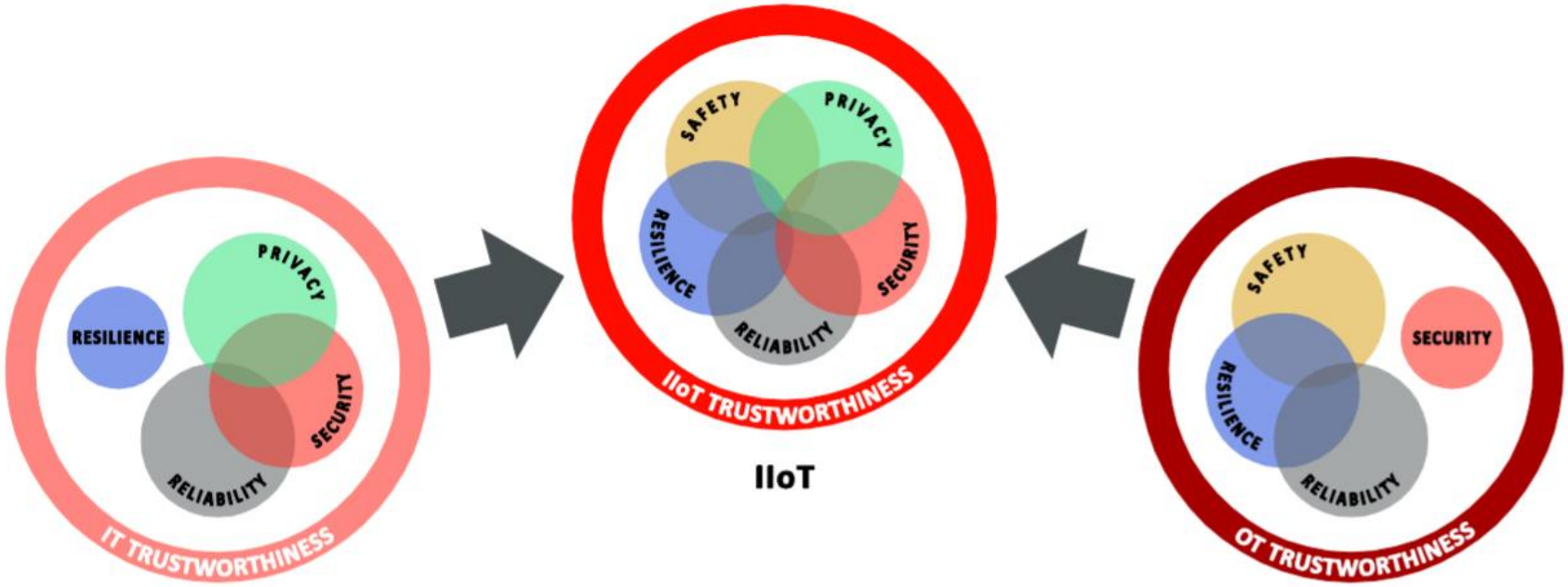
к.т.н. Руководитель отдела кибербезопасности АСУ ТП

+7 915 221 15 96

Ростелеком

Солар

Комплексность требований для развития АСУ ТП и IIoT



Ростелеком
Солар

Развитие методической базы

Киберфизическая система: взаимосвязанная совокупность физического (первичного) оборудования, информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей, согласованно выполняющая определенную функцию.

Кибербезопасность в общем: все аспекты, связанные с определением, достижением и поддержанием состояния защищенности киберфизической системы, при котором обеспечено ее устойчивое функционирование при проведении в отношении нее кибератак.

Кибербезопасность как состояние: состояние защищенности киберфизической системы, при котором обеспечено ее устойчивое функционирование в условиях проведения против нее кибератак.

Исследование Лаборатории Кибербезопасности АСУ ТП «Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса».

Ростелеком
Солар

Существующие методы оценки последствий на производстве

- Проведение анализа опасности и работоспособности (AOP/HAZOP) технологической части на стадии «П».
- Анализ опасности и работоспособности (AOP/HAZOP) контуров безопасности системы ПАЗ, назначение УПБ/SIL на стадии РД проекта технологической части.

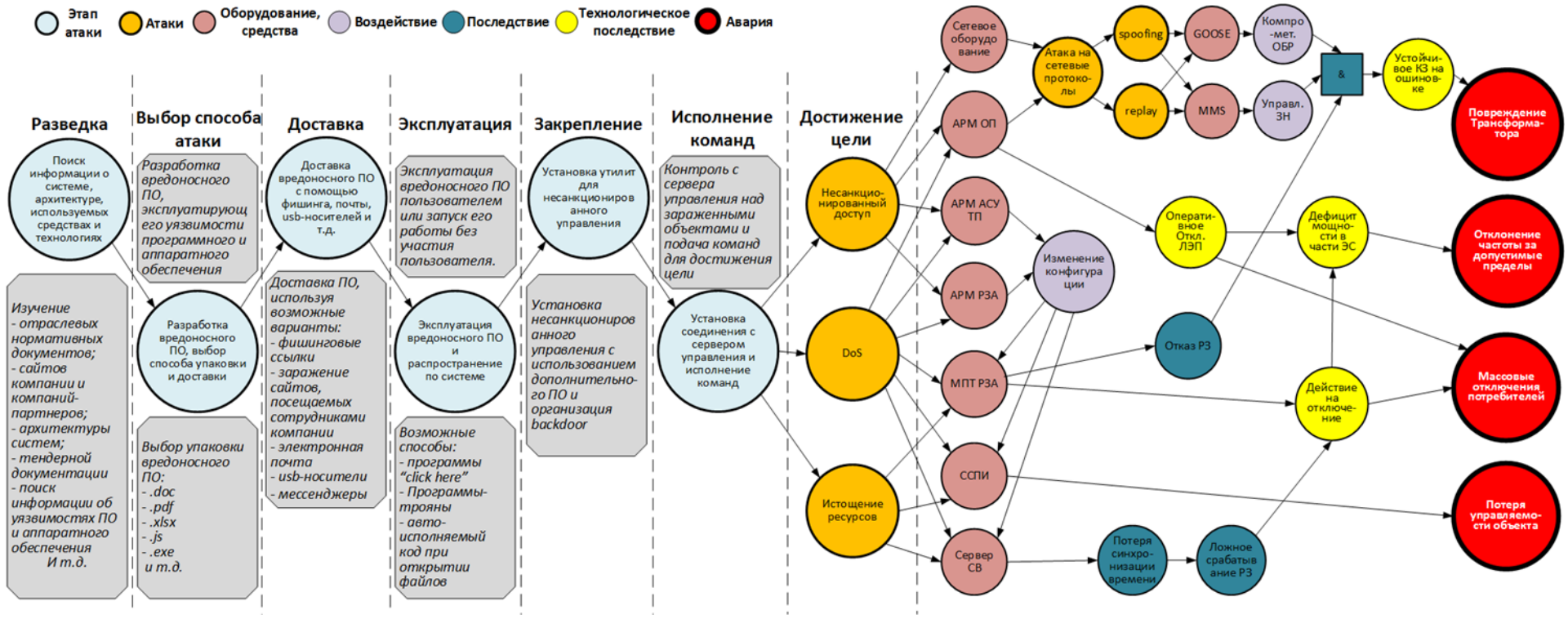
Обоснование безопасности ОПО – …сведения о результатах оценки риска аварии ОПО

Анализ опасностей и рисков – HAZARD & RISK analysis: HAZOP, FMEA, FTA, LOPA:

- анализ опасности и работоспособности HAZOP
- анализ вида и последствий отказов FMEA
- анализ «дерева отказов» FTA
- анализ «дерева событий» ETA
- анализ барьеров безопасности LOPA

Ростелеком
Солар

Результаты развития принципов моделирования угроз



Исследование Лаборатории кибербезопасности АСУ ТП «Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса».

Ростелеком
Солар

Виды тренировок и учений, существующие на данный момент

- Противоаварийные
- Противопожарные
- Аварийно-восстановительные тренировки
- Антитеррористические тренировки
- Учения по гражданской обороне и ликвидации чрезвычайных ситуаций

Киберучения – это новый вид тренировок, которые могут быть организованы и проведены как отдельно, так и в комплексе с существующими формами производственной деятельности, обеспечивающей поддержание необходимого профессионального образовательного уровня персонала для выполнения им производственных функций.

Виды киберучений

Теоретический этап:

- Штабные киберучения (**Table-top exercise)**

Практический этап:

- Гибридные киберучения (**Hybrid**)
- Полнофункциональные киберучения (**Full Live**)
  - Purple team
  - Red team

Ростелеком
Солар

Международный опыт – EU

- Ведущей организацией Евросоюза, ответственной за проведение киберучений, является Европейское агентство сетевой и информационной безопасности (European Network and Information Security Agency – ENISA, www.enisa.europa.eu), которое было учреждено в ноябре 2004 году и 1 сентября 2005 года приступило к работе в соответствии с регламентом ЕС № 460/2004.

- Начиная с 2010 года ENISA каждые два года организует и проводит киберучения Cyber Europe.

Ростелеком
Солар

Киберучения НАТО

- **Киберучения НАТО Locked Shields**

Организуются и проводятся Центром передового опыта по совместной защите от киберугроз с 2010 года.

- **Киберучения НАТО Cyber Coalition**

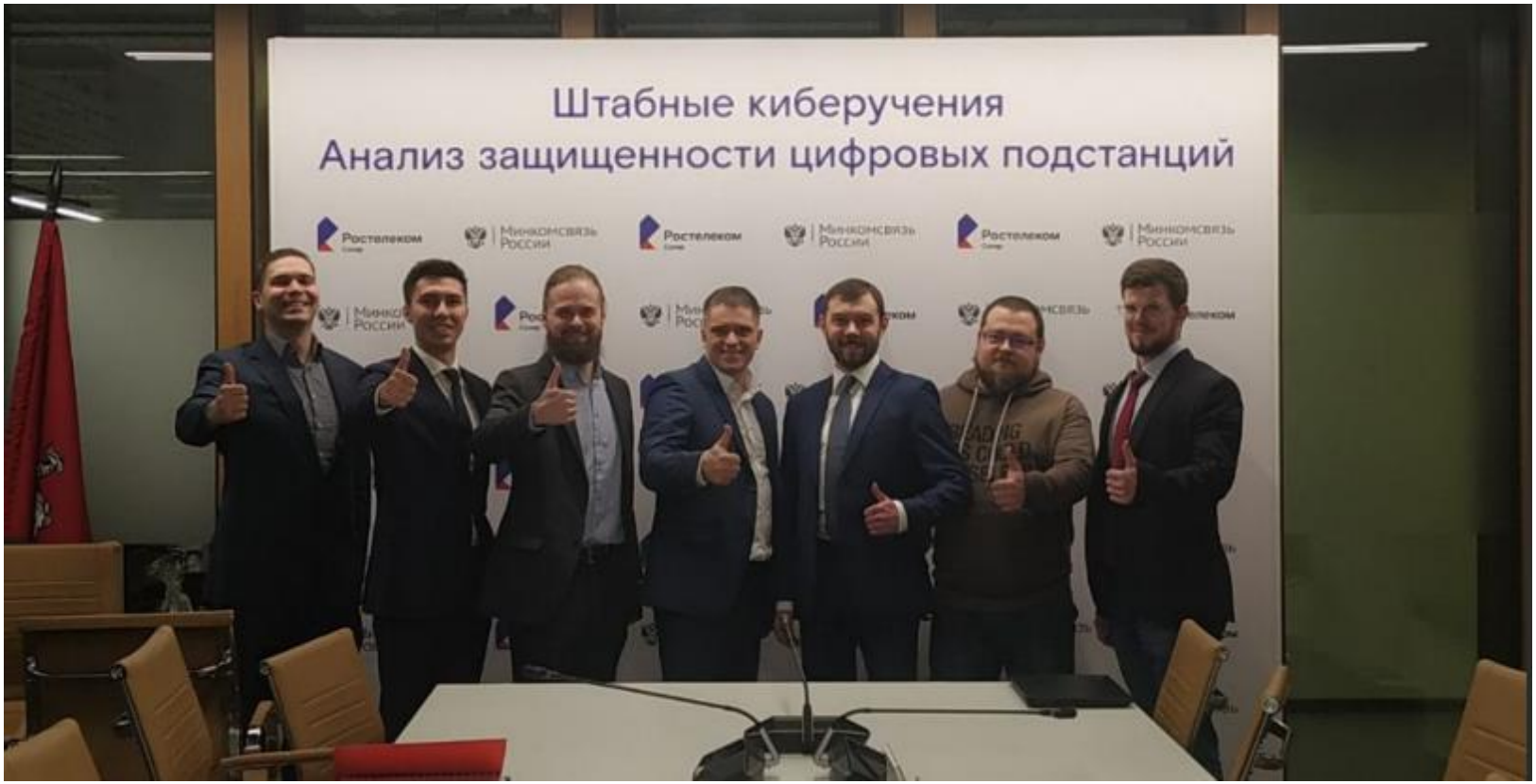
Организуются и проводятся Центром передового опыта по совместной защите от киберугроз (CCDCOE) с 2006 года.

В рамках киберучений имитируются сценарии массированных кибератак на объекты критической инфраструктуры государства или ряда государств:

- Системы водоочистки
- Электрические сети
- Электростанции

Ростелеком
Солар

Российский практический опыт



Сценарии штабных киберучений

- **Сценарий 1.** Нарушение управляемости и наблюдаемости энергорайона из-за воздействия вредоносного программного обеспечения на оборудование диспетчеризации цифрового РЭС.
- **Сценарий 2.** Несанкционированное удаленное управление или изменение конфигурации реклоузера 6-35 кВ.
- **Сценарий 3.** Несанкционированное удаленное управление коммутационным оборудованием ТП 10/0,4 кВ.
- **Сценарий 4.** Отключение межсистемной связи 500/330/220 кВ к системе со значительным дефицитом активной мощности.
- **Сценарий 5.** Нарушение динамической устойчивости энергосистемы вследствие деструктивного информационного воздействия, приведшего к КЗ недопустимой длительности на ЛЭП 500 кВ.

Цели проведения киберучений

- Повышение уровня обеспечения безопасности критической информационной инфраструктуры
- Повышение общего уровня компетенции участников киберучений по вопросам кибербезопасности
- Повышение общей культуры осведомленности участников киберучений по вопросам кибербезопасности
- Разработка актуальных моделей и методов противодействия современным кибератакам
- Приобретение практических навыков выявления, реагирования на компьютерные атаки

Киберучения как новая форма производственной деятельности, направленной на повышение защищенности и устойчивости функционирования систем промышленной автоматизации

Карантаев Владимир

К.т.н. руководитель отдела кибербезопасности АСУ ТП

+7 915 221 15 96

Ростелеком

Солар