Московский межотраслевой форум 2013

ПРОГНОЗИРОВАНИЕ АВАРИЙ И ЧС НА ОСОБО ОПАСНЫХ ОБЪЕКТАХ ЭКОНОМИКИ, ВЫЗВАННЫХ НАРУШЕНИЕМ ШТАТНОГО РЕЖИМА ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ В РЕЗУЛЬТАТЕ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ.

Докладчик:

Я.Д.Вишняков

Заслуженный деятель науки РФ,
профессор, д.т.н., ГУУ
Вице-президент национальной технологической палаты

Москва, 2013 г.

Сопоставление и совместный анализ динамики подготовки и характера угроз несанкционированных воздействия на объекты экономики дает основание для разработки современного и достаточно специального концептуального подхода к пониманию динамики и ситуационной обусловленности несанкционированных воздействий на большие информационно-коммуникационные и управляющие системы

Возможности прогнозирования и предупреждения ЧС, вызванных нарушениями штатного режима эксплуатации больших информационно-коммуникационных и управляющих систем (ИКУС) в результате несанкционированных воздействий на эти системы

Нарушение штатного режима больших информационно- коммуникационных и управляющих систем (ИКУС) способно послужить причиной аварий, катастроф и ЧС на особо опасных и критически важных объектах экономики

Основные типы нарушения штатного режима указанных систем:

- Непрогнозируемый отказ системы, работающей в одном из режимов специализированной ИТ. Внезапно и полностью прекращается управление и регулирование ответственных (в том числе пожаро- и взрывоопасных) технологических процессов, энергетических агрегатов, обладающих высокой удельной концентрацией энергии и т.п. Это прямой путь к возникновению ЧС, по масштабу близкого к ситуации на Чернобыльской АЭС.

- **Внезапный переход информационно-коммуникационной системы на режим искажения информационного потока. Особенно опасно в системах с диспетчерским управлением, в которых реагирование на искажение информации будет запаздывать в силу влияния человеческого фактора (ЧФ).**

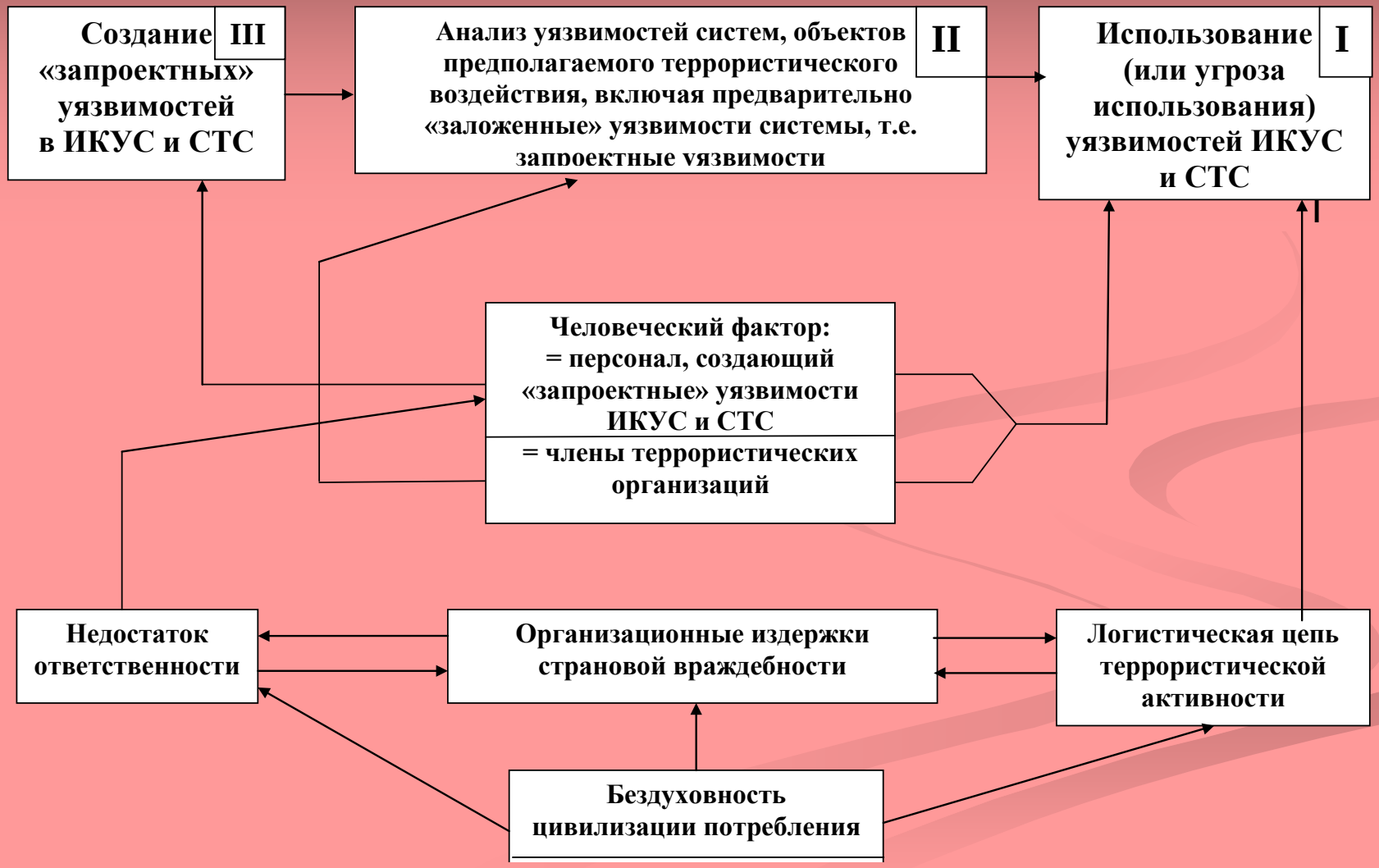
- **Существуют и другие нарушения штатного режима ИКУС, чреватые возникновением ЧС.**

Уязвимость больших ИКУС возрастает пропорционально увеличению масштабов этих систем, а также

использованию в этих системах импортных элементов и блоков систем, а также импортных информационных технологий.

Особого внимания требует интернационализация деятельности по прогнозированию и предупреждению ЧС, вызванных нарушением штатного режима эксплуатации больших информационно-коммуникационных и управляющих систем в результате несанкционированных воздействий.

Этапы развития процедур технологического и информационного терроризма



Несвоевременная оценка и недостаточное внимание к человеческому фактору является важнейшим стратегическим риском в области регулирования эксплуатации больших информационно-коммуникационных и управляющих систем в результате несанкционированных воздействий на эти системы

Противодействие террористическим воздействиям на СТС это комплексная задача, включающая необходимость решения социально-политических, этических, экономических, организационных и технико-технологических проблем.

- **Во-первых, это социально-политические и этические проблемы, носящие международный характер. Их реальное разрешение требует появления особой ответственности государственных структур как за последствия подготовки диверсионных актов на СТС, так и за особо тщательную охрану собственной документации с целью предотвращения доступа к ней террористов.**

- **Во-вторых, это проблемы экономического, организационного и технико-технологического характера. Их целесообразно решать совместным международными усислиями, так как они носят общий характер и могут решаться вне зависимости от решения проблем первой группы.**

- **Необходимо понимание того, что в виде ИКУС с предварительно «заложенными» уязвимостями террористы получают мощное орудие воздействия на правительство и административные органы того государства или региона, где террористы планируют решать свои задачи, чаще всего, кратковременного характера: добиться освобождения из тюрьмы сообщников, получить достаточно большую сумму денег и т.п.**

vishnyakov1@yandex.ru