ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТЭК ОТ КИБЕРУГРОЗ

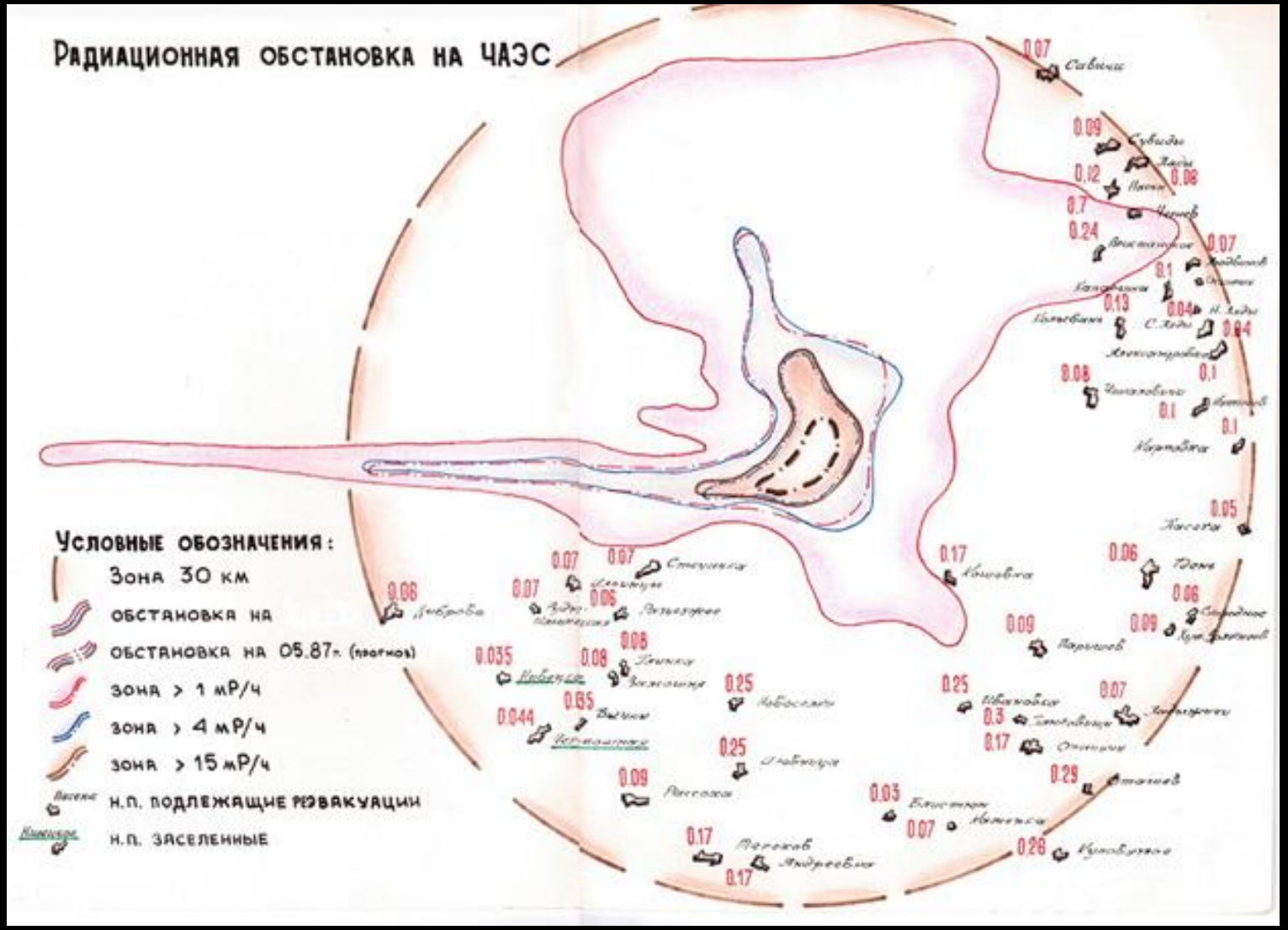
Профессор, доктор технических наук
Минзов Анатолий Степанович
MinzovAS@mpei.ru

Моё участие в ликвидации последствий аварии на ЧАЭС

1. В период с 17 декабря 1986 по 18 января 1987 года в составе Оперативной группы НХВ МО СССР Героя Советского Союза генерал-полковника В.К.Пикалова.

2. В период с 10 по 17 марта 1987 года для решения организационных вопросов по прохождению учебной практики слушателей ВАХЗ.

Фрагмент документа о радиационной обстановке в 30 км зоне



Резюме

1. Общая численность личного состава, принимавшего участие в ликвидации последствий аварии на ЧАЭС, составила не менее 500 000 чел.
2. В первые недели после аварии дозиметрический контроль не был организован. Допустимой считалась доза излучения 50 БЭР (0,5 Зв). В конце 1986 она составляла 25 БЭР (0,25 Зв).
3. Катастрофа показала общую неготовность к подобным авариям как специалистов ХВ и ГО, так и промышленности.

Прошло 30 лет...

Какие выводы можно сделать сегодня ?

Создание нового укрытия для
4 энергоблока ЧАЭС

Некоторые выводы из анализа причин и сценариев развития аварий и катастроф на объектах ТЭК

1. Причиной аварий и катастроф чаще всего являлся человеческий фактор и пренебрежение персоналом технологиями безопасного управления объектами ТЭК.
2. Характерно, что развитие аварий и тяжесть последствий чаще всего связана с плохой организацией системы информационной безопасности АСУТП.
3. Развитие систем связи и информационных технологий приводит к появлению новых угроз на объектах ТЭК – киберугроз. Это может нарушить работу объектов ТЭК и привести к авариям и разрушениям регионального, государственного или международного масштаба.
4. Использование импортных технологий и технических систем создаёт недоверенную среду, которая может привести к реализации концепции управляемых катастроф.

Сетевой червь *Stuxnet*

- Использует уязвимость программного обеспечения микроконтроллеров Simens (WinCC/PCS 7).
- Атакует только контроллеры, к которым подключены приводы переменной частоты.
- Заменяет микропрограмму контроллера.
- Изменяет частоту вращения привода в широком диапазоне, что приводит к выводу из строя привод.
- Дальнейшее развитие вредоносного кода – это *Duqu, Flame (2011), Regin (2014)*

Меры противодействия авариям и катастрофам ТЭК

1. Разработка и принятия нормативно-правовых актов в сфере обеспечения информационной безопасности АСУТП ТЭК, создающих механизмы регулирования в сфере информационной безопасности объектовТЭК и решающих, в том числе, проблему ответственности собственников за безопасность объектов ТЭК.
2. Разработка технологий малоресурсной криптографии для промышленных сетей.
3. Совершенствование технологий разработки АСУТП в SCADA-системах за счёт включения новых функций, создающих доверенную среду.

Меры противодействия авариям и катастрофам ТЭК

3. Научная проработка создания мета-информационных систем, практически исключающих аварии и катастрофы на объектах ТЭК за счет одновременного контроля:
   - **состояния технологических процессов;**
   - **управляющих параметров в АСУТП;**
   - **показателей систем управления информационной безопасностью;**
   - **действий персонала.**

4. Введение в образовательный процесс НИУ МЭИ на кафедре ИЭБ нового профиля обучения «Безопасность АСУТП».

Заключение

Реализация этих мер потребуют совместных действий и усилий Министерства энергетики РФ, РАН, МЧС, Национальных исследовательских университетов РФ и других научных организаций в этой сфере деятельности.

Вопросы ?