РОСЭНЕРГОАТОМ
ВНИИАЭС
Центр компетенций по кибербезопасности

Анализ безопасности энергоблока АЭС, обусловленный воздействием компьютерных атак на АСУ ТП АЭС. Подход и основные аспекты

Докладчик: Начальник отдела нормативно-технического обеспечения кибербезопасности

Бабаев Денис Игоревич

Общая информация о центре компетенций

Лицензии РОСТЕХНАДЗОР

- 5 сотрудников центра являются экспертами МЭК ТК 45А
- Сотрудники проходят регулярное обучение и повышение квалификации по программам согласованным с ФСТЭК России.
- Сотрудники на регулярной основе участвуют в международных конференциях и семинарах ВАНО, МАГАТЭ и МЭК.

Лицензии ФСТЭК и ФСБ

Партнеры и сотрудничество - Организовано взаимодействие с МИФИ, МФТИ, ГНИИ ПТЗИ ФСТЭК России и разработчиками средств защиты информации

Актуальность

«….невозможно техногенный инцидент идентифицировать как следствия кибератаки или иного компьютерного инцидента, что в дальнейшем приводит к отсутствию проблемы кибербезопасности как таковой в нормативном поле».
[Материалы круглого стола «Кибербезопасность в условиях цифровой трансформации энергетики».

Федеральный закон от 26.07.2017 № 187

«О безопасности критической информационной инфраструктуры» и подзаконные ему акты:

- **Приказ ФСТЭК от 21 декабря 2017 г. № 235**
  «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»;
- **Приказ ФСТЭК от 25 декабря 2017 № 239**
  «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации».

Приказ ФСТЭК От 14 марта 2014 г. № 31

«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

В настоящее время отсутствуют достаточно формализованные методы, позволяющие оценить влияние нарушений свойств безопасности информации, обрабатываемой в АСУ ТП, на технологические процессы.

Некоторые методы анализа безопасности промышленных объектов

Анализ "дерева событий", Event Tree Analysis – ETA	ГОСТ Р 51901.1-2005
Анализ видов и последствий отказов (FMEA), а также Анализ видов, последствий и критичности отказов (FMECA)	ГОСТ Р 51901.12-2006, МЭК 60812
Анализ дерева неисправностей (отказов), Fault Tree Analysis - FTA	ГОСТ Р 51901.13-2005, МЭК 61025
Исследование опасности и связанных с ней проблем, Hazard and operability studies - HAZOP	ГОСТ Р 51901.11-2005, МЭК 61812:2001
Анализ влияния человеческого фактора, Human Risk Assessment - HRA	ГОСТ Р 51901.1-2005
Предварительный анализ опасности, PreliminaryHazard Analysis- PHA	ГОСТ Р 51901.11-2005, МЭК 61812:2001
Анализ человеко-машинного интерфейса (ЧМИ – HMI)	ГОСТ Р МЭК 61226 – 2011 (IEC 61226-2009), МЭК 61839
Детерминистический анализ безопасности (ДАБ)- оценка безопасности АЭС	НП-006-16
Вероятностный анализ безопасности (ВАБ), Probabilistic risk assessment (PRA)	МЭК 61839, НП-095-15

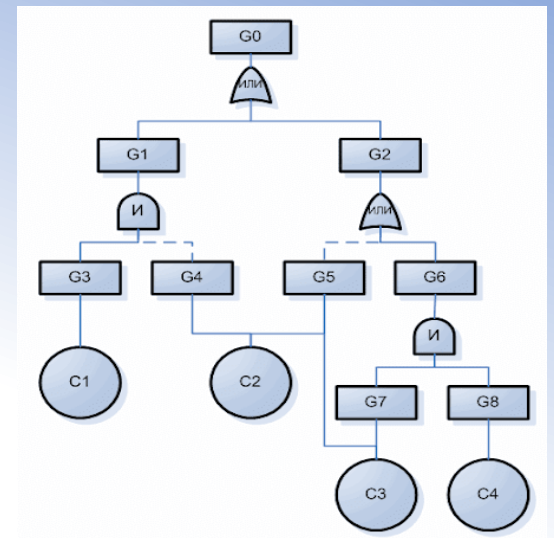
Недостатки

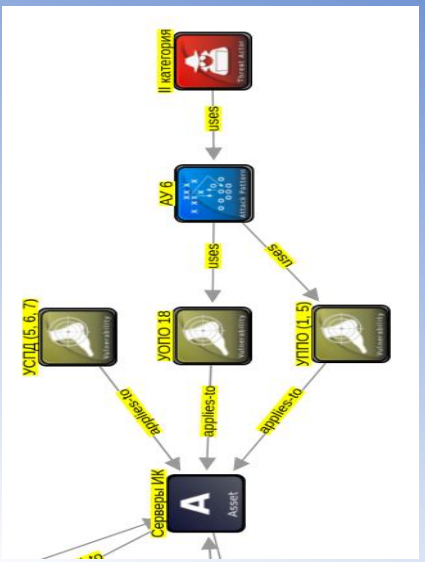
- **Не рассматриваются факторы антропогенных угроз**
- **Не адаптированы к сценариям (изменению состояния системы во времени), постулируются единовременные отказы**
- **Системы рассматриваются как относительно независимые от других систем и среды**

Источник: http://www.proatom.ru/modules.php?name=News&file=article&sid=3334

Некоторые методы анализа защищенности

- **Методики определения актуальных угроз ФСТЭК России**
- **Граф сценария компьютерной атаки**
- **Дерево компьютерной атаки**
- **Тесты на проникновения**





Недостатки

- **Не включают в себя аппарат оценки последствий от реализации компьютерных атак для безопасности сложных технологических систем, при этом некоторые методы предполагают такую оценку исключительно экспертно и без применения какого-либо аналитического механизма**
- **Высокая степень неопределённости при моделировании действий потенциального нарушителя**

Источник: Andrew P. Moore, Robert J. Ellison, Richard C. Linger. Attack Modeling for Information Security and Survivability
https://github.com/idaholab/STIG

Цели и задачи подхода

Обозначается необходимость в разработке подходов, позволяющих оценить последствия воздействия компьютерных атак на АСУ ТП АЭС и безопасность энергоблока АЭС в целом. Такие подходы должны основываться на лучшем опыте в части анализа безопасности АЭС и современных методах моделирования угроз, а также минимизировать неопределенность, связанную с моделированием сценариев КА.

Цель

Подготовка решений, направленных на повышение безопасности энергоблока АЭС

Задачи

- **Оценка возможности получения исходного события аварии на энергоблоке АЭС посредством проведения КА на компоненты АСУ ТП АЭС;**
- **Анализ возможности нарушения реализованных барьеров ЯРБ посредством КА на компоненты АСУ ТП АЭС;**
- **Выявление дефицитов безопасности* в проекте АЭС в целом, а также дефицитов безопасности, обусловленных применением программно-технических средств в составе АСУ ТП АЭС.**

*необеспеченность объекта использования атомной энергии какой-либо функцией безопасности в объеме, определяемом требованиями действующих норм и правил в области использования атомной энергии.

Нормативные основы

ГОСТ Р МЭК 61508-2-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью.

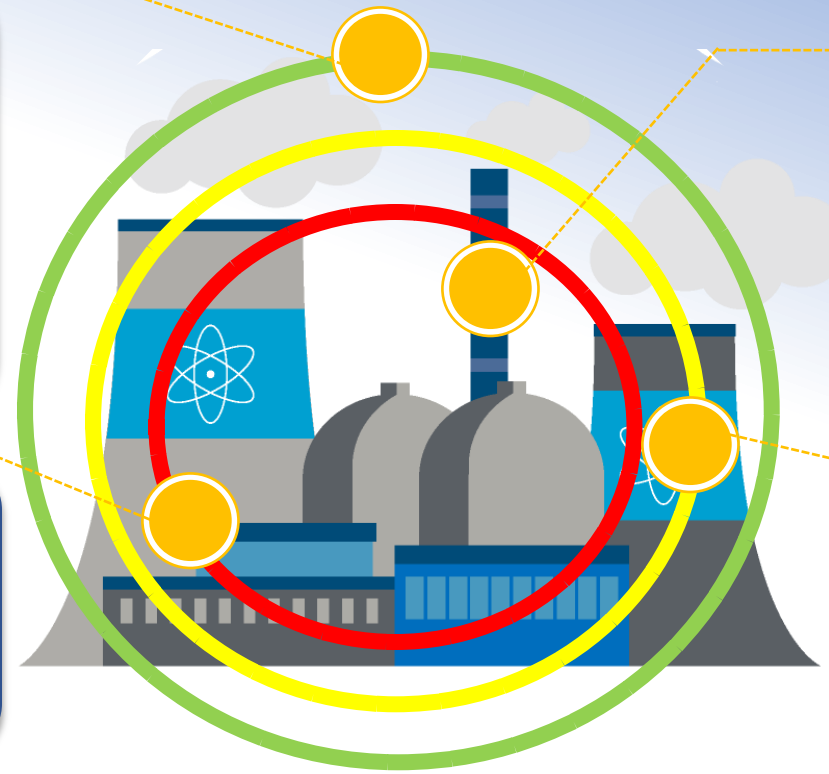
РБ-100-15 Руководство по безопасности при использовании атомной энергии "Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций»

Методические документы ФСТЭК России, Разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

Характеристики объекта управления в задачах безопасности

Источники угроз вне помещения:
поражение молнией; сильный дождь или снегопад, наводнение; буря (ураган), торнадо, ветровая нагрузка; землетрясение; низкая температура, замерзание; высокая температура; воздушная ударная волна; падающие, летящие предметы; обледенение; неравномерность осадки фундамента.

Человеческий фактор:
неправильное выполнение технологических операций (в том числе при выполнении переключений, воздействие на элементы защиты, автоматики; преднамеренное вмешательство в работу автоматики; нарушение политик кибербезопасности и других документов; нарушение технологии ремонта; и др.



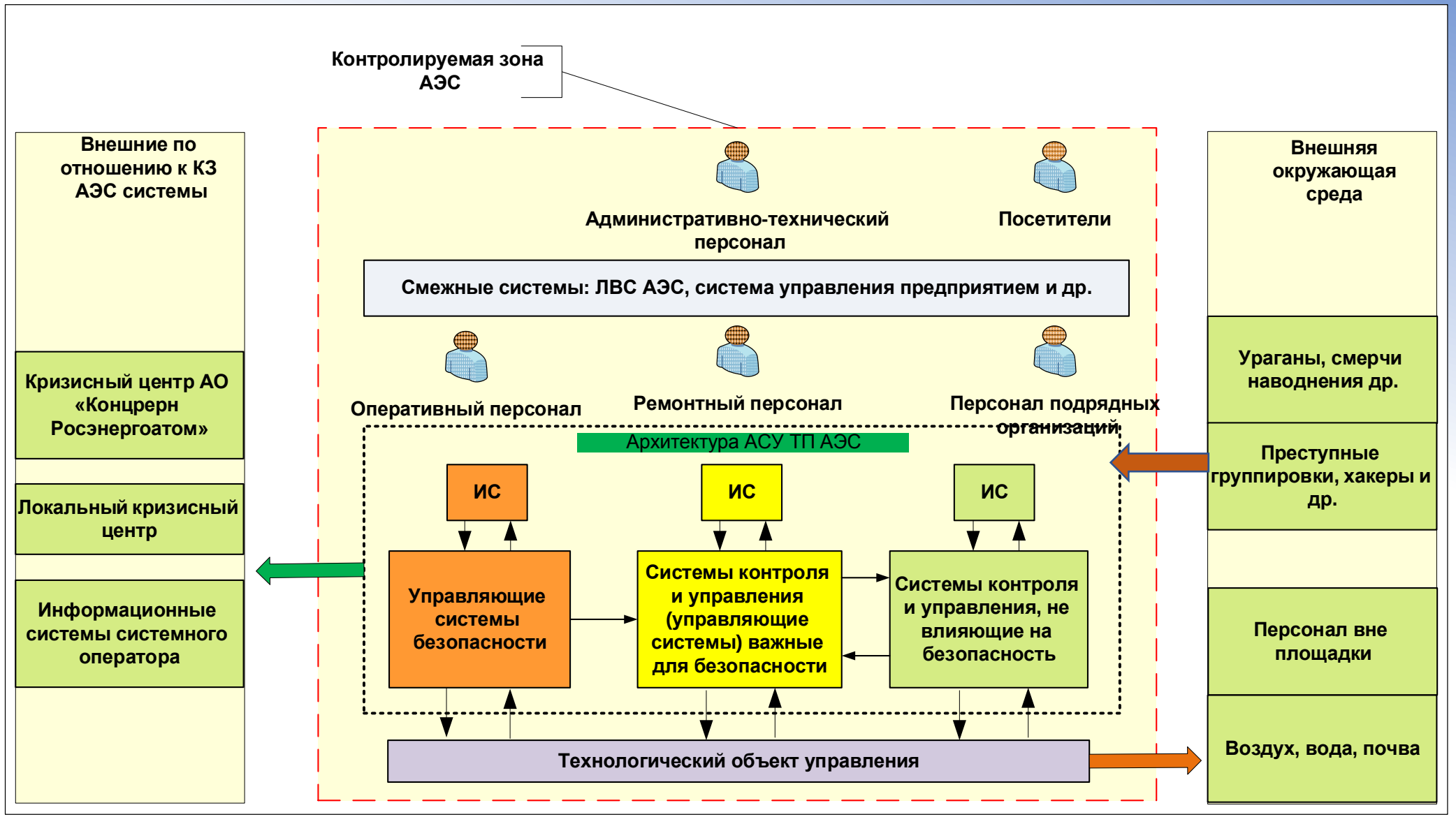
Источники угроз в АСУ ТП:
отказы и неисправности аппаратных средств; ошибки проектирования и конструирования; программно-аппаратные закладки; вредоносные программы, некачественное выполнение функций.

Источники угроз в помещениях:
изменения температуры; изменения давления; изменения влажности; затопление помещения; замерзание; облучение узлов (элементов); задымление; взрыв.

Наблюдаемость – свойство, заключающееся в возможности оценки значений координат (параметров), определяющих состояние ТОУ по измеренным значениям координат в условиях заданных ограничений;
Управляемость – свойство заключающееся в том, что существуют управляющие воздействия (команды), способные обеспечить достижение цели управления в условиях заданных ограничений;
Безопасность – свойство, заключающиеся в поддержании пределов и условий безопасной эксплуатации.

Модель АСУ ТП АЭС

«Организм и среда образуют целое и их следует рассматривать как таковое» Э.Г. Старлинг



Основные угрозы безопасности АСУ ТП АЭС

Несанкционированное вмешательство в управление технологическими процессами.

Нарушение функционирования (сбои, отказы) АСУ ТП АЭС и ее отдельных компонентов.

Несанкционированный доступ к технологической или иной информации.

В результате реализации угроз могут быть нарушены:

свойства энергоблока (ТОУ):

- наблюдаемость;
- управляемость;
- безопасность.

свойства функций АСУ ТП АЭС:

- устойчивость (сбои, отказы);
- качество (несвоевременное выполнение, задержки в выполнении).

свойства информации:

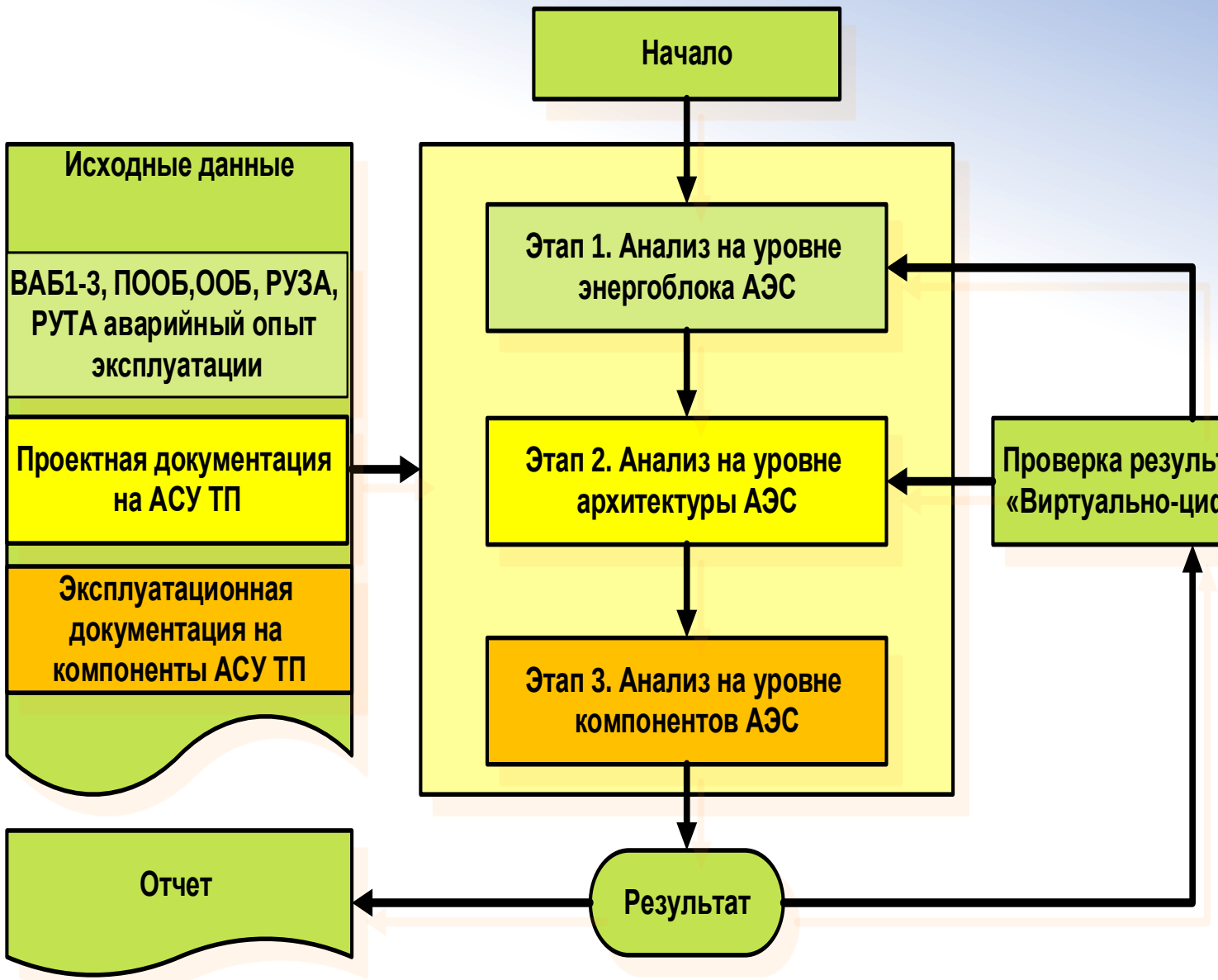
- доступность;
- целостность
- конфиденциальность .

Влияние на компоненты АСУ ТП **Влияние на функции АСУ ТП** **Влияние на энергоблок**

Виды компьютерных атак в задачах анализа

Тип КА	Описание компьютерной атаки	Нарушаемые свойства:		
		энергоблока (ТОУ)	функций СКУ	информации
I	КА, направленная реализацию отказа отдельных подсистем АСУ ТП. В результате может быть полный или частичный отказ подсистемы, характеризующейся нештатным выполнением отдельных ее функций.	Управляемость Наблюдаемость	Устойчивость Качество	Доступность
II	КА, направленная на нарушение в работе отдельного технологического оборудования энергоблока АЭС (например, насосов и (или) задвижек). Атака проводится математическое обеспечение (логику управления ТОУ) в АСУ ТП.	Управляемость	Устойчивость	Целостность Доступность
IIII	КА, направленная на нарушение информационных функции АСУ ТП, которая приводит к принятию ошибочных или несвоевременных решений по управлению энергоблоком АЭС.	Наблюдаемость	Качество	Целостность
IV	**Целенаправленная компьютерная атака (ЦКА),** направленная на **достижение исходного события аварии** – нарушение пределов и условий нормальной эксплуатации. В общем случае атака носит комбинированный характер.	Безопасность	Устойчивость	Целостность Доступность

Порядок проведения анализа



Процедура анализа

Технологи

Специалисты по АСУ ТП

Специалисты по ИБ

Специалисты по мат. моделированию

Объект: Система управления (АСУ ТП+ОУ)

Мероприятия

- Идентификация аварии (нарушения) и возможного ущерба
- Определение результирующего события нарушения ТП
- Идентификация основных технологических систем (элементов)
- Идентификация взаимодействующих систем

Этап 1

Объект: Управляющая система (АСУ ТП).

Мероприятия

- Выделяются функции (функции безопасности, ТЗиБ, контроля, регулирования и управления
- определяются подсистемы АСУ ТП, задействованные в реализации соответствующих функций;
- Определяются условия (сочетания отказов), необходимые для достижения события

Этап 2

Объект: Компоненты АСУ ТП .

Мероприятия

- Выделение и группировка компонентов АСУ ТП/ построение структурной схемы компонентов;
- Определение и описание состава ПТС;
- Определение событий порождающих отказ
- моделирование сценария компьютерной атаки.

Этап 3

Объект: Система управления, мат. обеспечение.

Мероприятия

- Проверка (верификация) реализации сценария нарушения ТП
- Корректировка сценариев нарушения ТП
- Получение характеристик энергоблока АЭС;
- Получение оценок ущерба от реализации КА

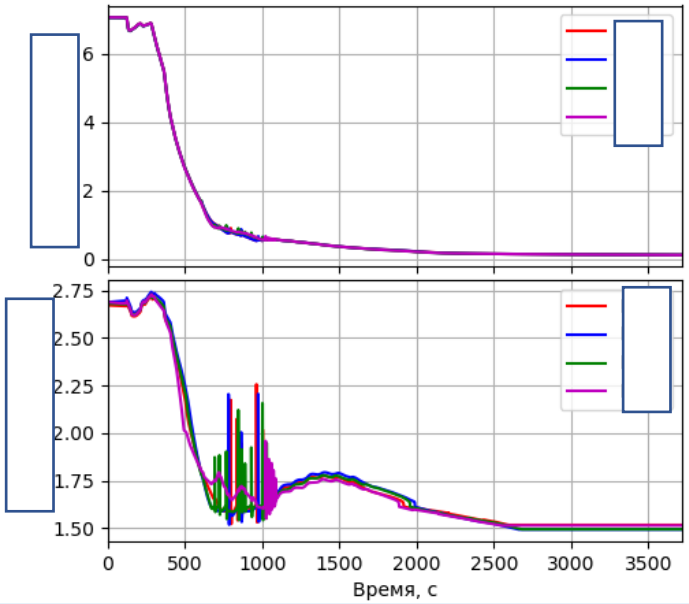
Этап 4

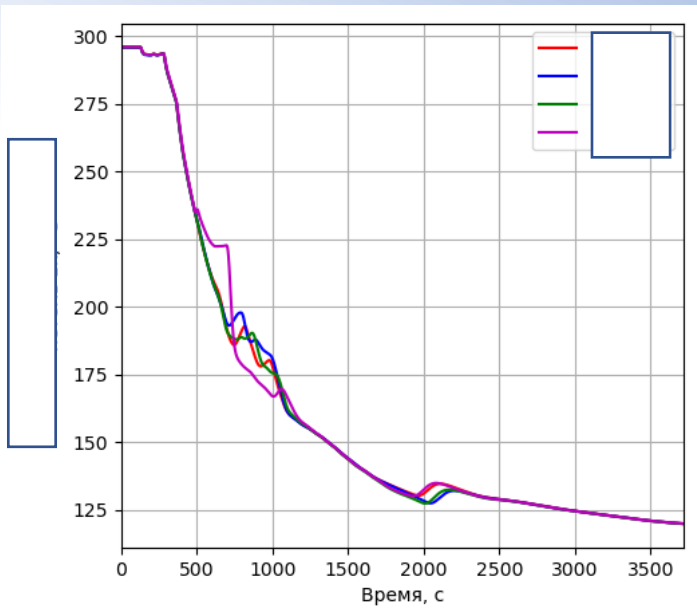
Процедура анализа. Пример результатов анализа

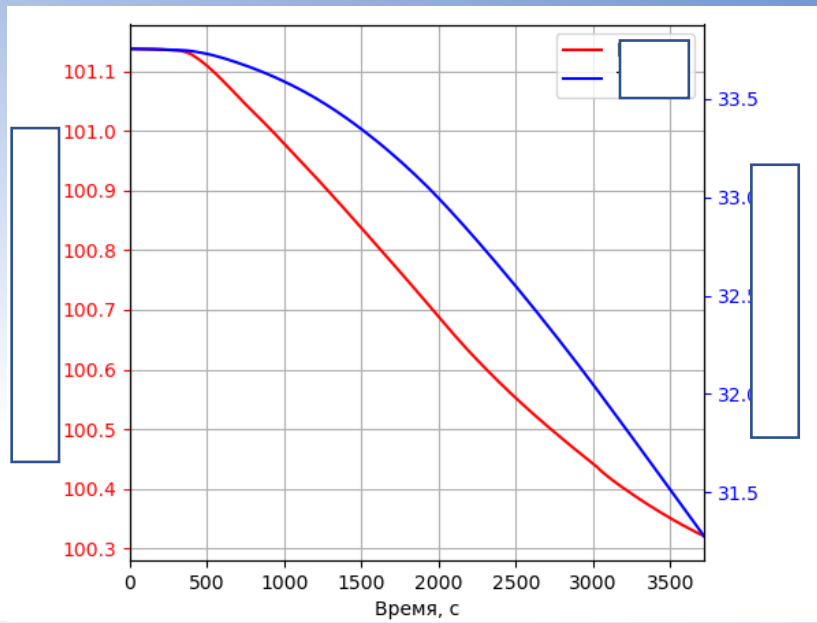
Системы (элементы) энергоблока АЭС, участвующие в нарушении	Предусмотренные защиты и блокировки (функции безопасности), функции контроля и управления, задействованные в реализации сценария	Подсистемы АСУ ТП АЭС, в которых реализованы функции контроля и управления, функции безопасности	Функциональные компоненты
Этап 1		**Этап 2**	**Этап 3**
Система или элемент	• Функция Безопасности 1	Подсистема А	Компонент 1, ИС
	– Закрытие клапана (1, 2). При давлении в паропроводе менее	Подсистема Б	Компонент 2, ИС

Моделирование на ПТК «Виртуально-цифровая АЭС»

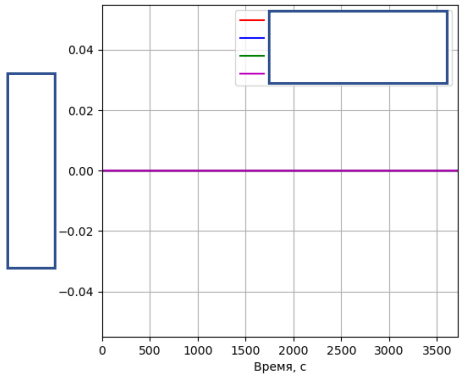
Состояние основных технологических систем

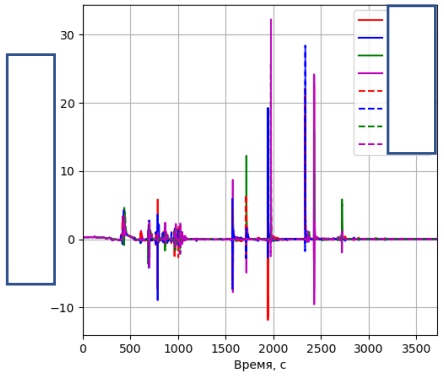




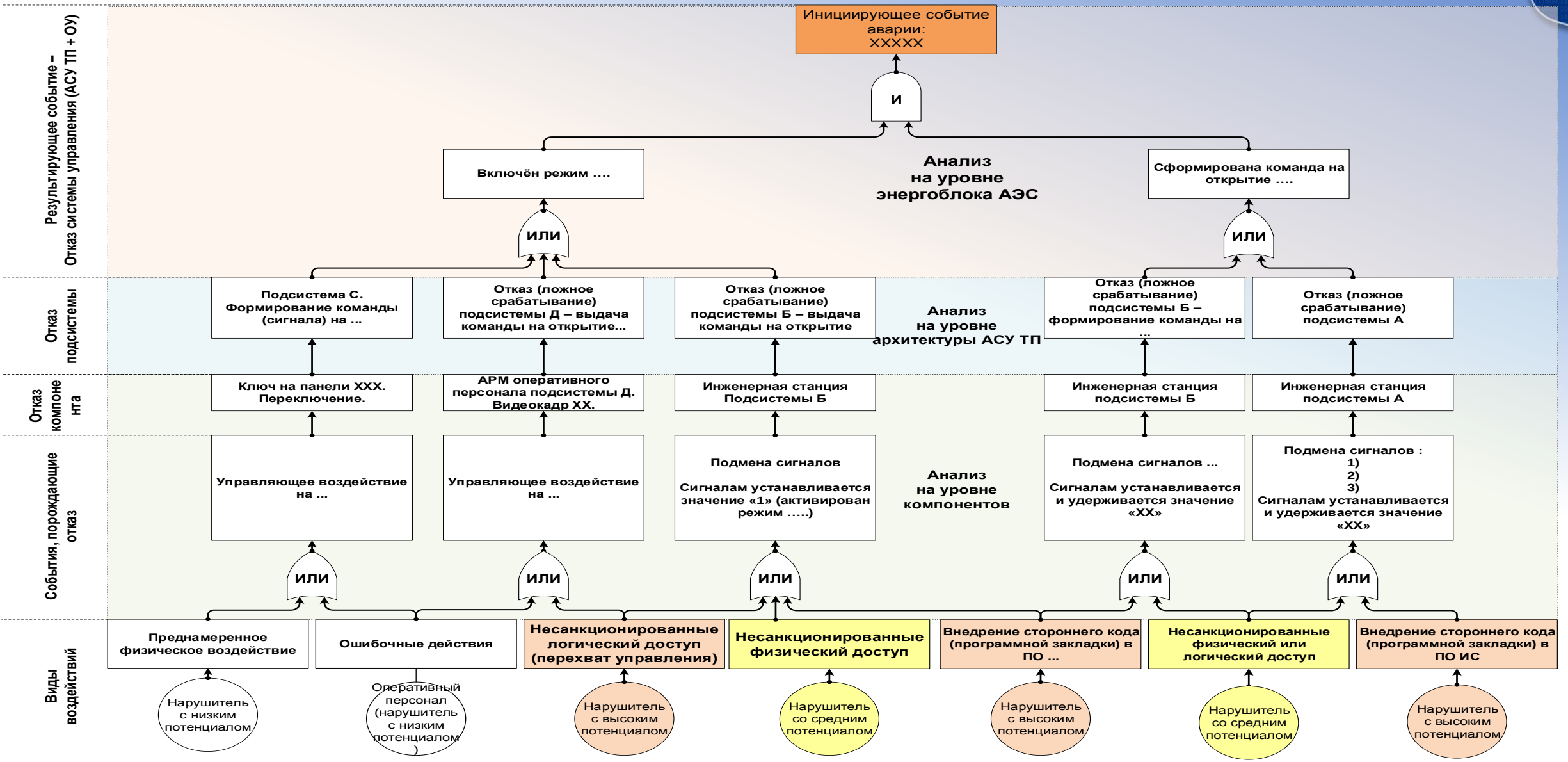


Состояние смежных технологических систем





Модель дерева компьютерной атаки



Анализ результатов

- ✓ **Дефициты безопасности энергоблока**
- ✓ **Сценарии нарушения**
- ✓ **Скомпрометированные технологические системы**
- ✓ **Скомпрометированные подсистемы АСУ ТП**
- ✓ **Скомпрометированные функции**
- ✓ **Скомпрометированные компоненты**
- ✓ **Угрозы, уязвимости, нарушители**

Технический отчет, включающий полные результаты анализа

Рекомендации по улучшению уровня безопасности:

- Защиты и блокировки, компенсирующие мероприятия
- Меры защиты информации

Сводные листы

№ п/п	Наименование элемента	Описание элемента
1.	ID сценария	AB-001
1.	Наименование	
1.	Тип	Целенаправленная компьютерная атака
1.	Описание сценария	
1.	Системы (элементы) энергоблока АЭС, участвующие в сценарии	
1.	Предусмотренные защиты и блокировки (функции безопасности), функции контроля и управления	
1.	Режим работы / состояние объекта исследования	Энергоблок на номинальной мощности
1.	Инициирующие условия	
1.	Начальное состояние	
1.	Конечное состояние	

Каталог (БД)

В стадии исследований

ML

- **Расследование инцидентов**
- **Выявление недостатков и дефицитов**
- **Определение компенсирующих мероприятий**

СПАСИБО ЗА ВНИМАНИЕ!
ВАШИ ВОПРОСЫ!

Приложение. Шкала ущерба ядерных аварий

Уровень по шкале INES	Пример события на АЭС
Уровень 7. Крупная авария	• Авария на Чернобыльской АЭС, СССР, 1986 год • Авария на АЭСФукусима-1, Япония, 2011 год
Уровень 6. Серьёзная авария	
Уровень 5.Авария с широкими последствиями	• Авария на АЭС Три-Майл-Айленд, США, 1979 год • Авария в Уиндскейле, Великобритания, 1957 год
Уровень 4.Авария с локальными последствиями	
Уровень 3. Серьёзный инцидент	• Пожар на АЭС Вандельос, Испания, 1989 год
Уровень 2. Инцидент	• Многочисленные события
Уровень 1. Аномальная ситуация	• Многочисленные события
Уровень 0. Событие с отклонением ниже шкалы	• Многочисленные события