kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Денис Бабаев

Начальник отдела нормативно-технического обеспечения кибербезопасности АСУ ТП, ВНИИАЭС

#KasperskyICS

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

РОСЭНЕРГОАТОМ
ВНИИАЭС
Центр компетенций по кибербезопасности

Рабочая встреча ВАО АЭС на тему: «Информационная безопасность»

Опыт проведения аудитов кибербезопасности АСУ ТП действующих АЭС

Докладчик: Начальник отдела нормативно-технического обеспечения кибербезопасности АСУ ТП АЭС

Бабаев Денис Игоревич

г. Прага, 25-28 ноября 2019 г

Обзор нормативной базы по кибербезопасности АСУ ТП АЭС и безопасности КИИ

Безопасность КИИ

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».*

Безопасность КВО

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»

IEC 62645:2014 «Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems»

IEC 62859:2016 «Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity »

IAEA International Atomic Energy Agency

IAEA Nuclear Security Series No. 17 «Computer Security at Nuclear Facilities» («Компьютерная безопасность на ядерных установках»)

IAEA Nuclear Security Series No. 33-T. Computer Security of Instrumentation and Control Systems at Nuclear Facilities. Technical Guidance

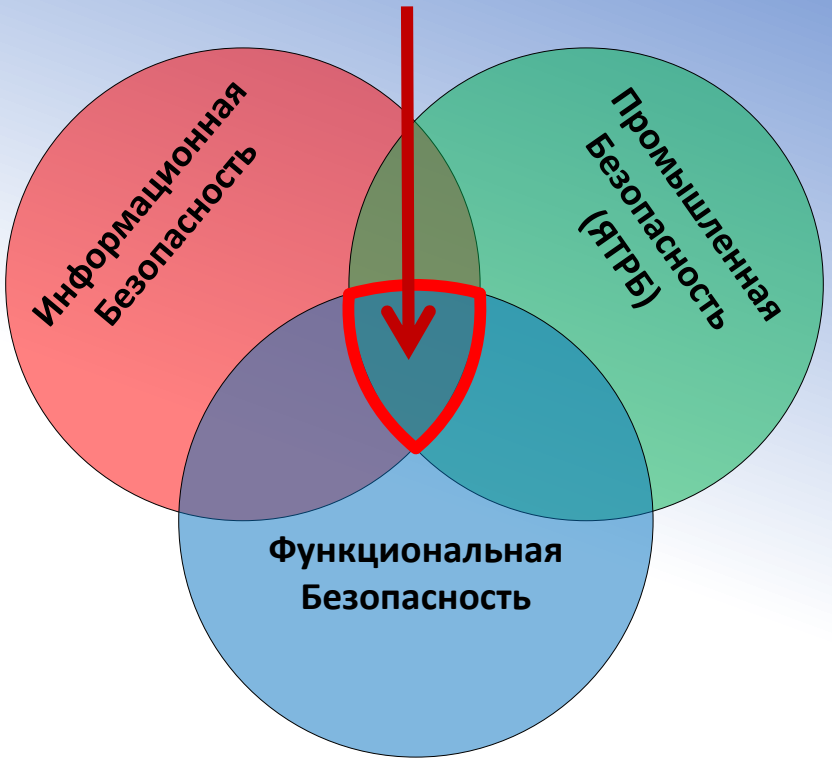
Кибербезопасность АСУ ТП АЭС

Кибербезопасность АСУ ТП АЭС - состояние АСУ ТП АЭС, при котором риски нарушения технологического процесса из-за кибератак на АСУ ТП АЭС минимизированы.
[СТО 1.1.1.06.1186-2016]

»**Цель** обеспечения кибербезопасности АСУ ТП АЭС – сохранение устойчивого функционирования АСУ ТП в условиях воздействия различного вида угроз, в том числе компьютерных атак, и, соответственно сохранение безопасности и эффективности технологических процессов АЭС.

Фундаментальные принципы обеспечения кибербезопасности АСУ ТП:
»**БЕЗУСЛОВНЫЙ ПРИОРИТЕТ ЯДЕРНОЙ, РАДИАЦИОНОЙ БЕЗОПАСНОСТИ!** ***[170-ФЗ, IAEA NSS 033-Т]***
»**Дифференцированный подход** ***[IEC 62645, IEC 62859, IAEA NSS 033-Т, Приказы ФСТЭК России № 13,239]***

Кибербезопасность АСУ ТП

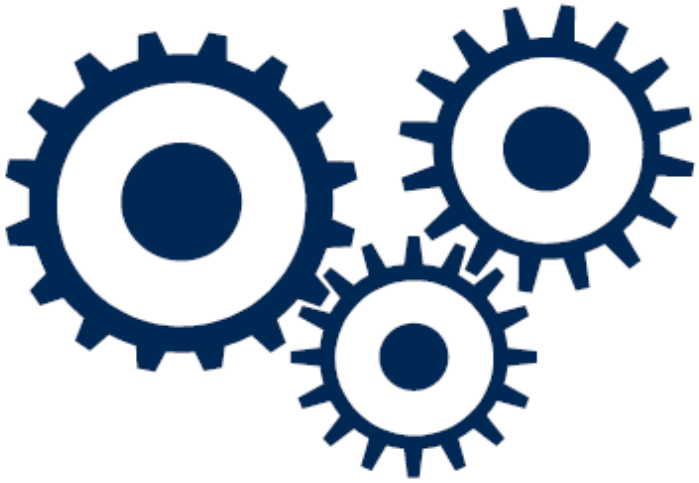


Специфичным в кибербезопасности АСУ ТП АЭС является:с
- **Верное целеполагание при создании системы обеспечения кибербезопасности АСУ ТП.**
- **Учет рисков, связанных с ядерной и радиационной безопасностью.**

Центр компетенций по кибербезопасности АСУ ТП АЭС на базе АО «ВНИИАЭС»

РОСЭНЕРГОАТОМ
ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ ДИВИЗИОН РОСАТОМА

»Центр компетенции АО «Концерн Росэнергоатом» по кибербезопасности АСУ ТП АЭС (Приказ КРЭА № 9/464-П от 10.04.2017)



- Организует научно-методическое обеспечение и координацию всех видов работ по обеспечению кибербезопасности АСУ ТП на АЭС.
- Формирует промышленную и научно-техническую политику по кибербезопасности АСУ ТП АЭС.
- Формирует концепцию кибербезопасности АСУ ТП АЭС в обеспечение эффективности, надежности и безопасности эксплуатации АЭС.
- Организует и проводит экспертизу проектной и эксплуатационной документации АСУ ТП АЭС на соответствие требованиям кибербезопасности.
- Организует и проводит аудиты кибербезопасности АСУ ТП АЭС.
- И др. функции и задачи в соответствии с Положением о Центре Компетенций.

Общая информация о центре компетенций

Лицензии РОСТЕХНАДЗОР

- 5 сотрудников центра являются экспертами МЭК ТК 45А
- Все 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

Перечень выполняемых работ Центром компетенций

- Аудит кибербезопасности АСУ ТП АЭС (включая тесты на проникновение)
- Моделирование угроз
- Проектирование систем обеспечения кибербезопасности АСУ ТП (включая разработку документации: Политик, процедур, регламентов, требований)
- Поставка сертифицированных средств защиты информации.
- Обучение и подготовка персонала.

Аудит кибербезопасности АСУ ТП действующих АЭС

Аудит – систематический, независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения критериев аудита. [ИСО/ МЭК 19011]

Вводные положения

Заказчик – Центральный аппарат АО «Концерн Росэнергоатом»

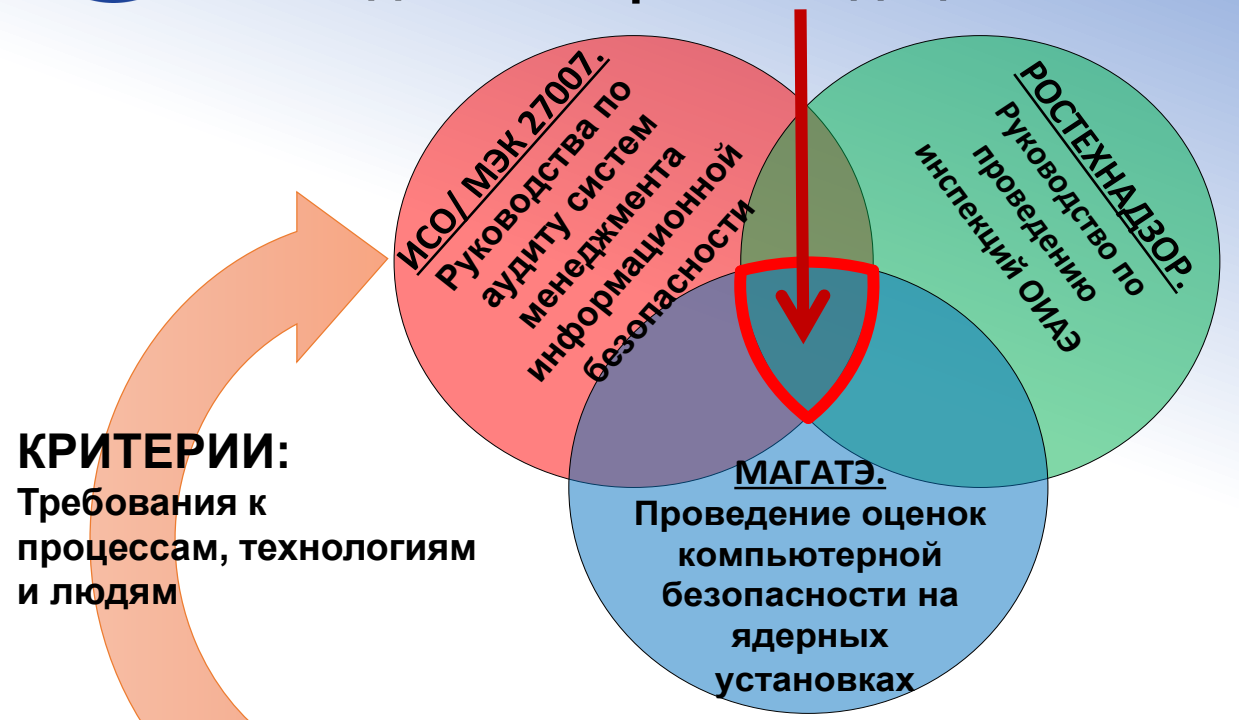
Новоронежская АЭС э/б №4,5,6
Июль 2019

Кольская АЭС э/б № 1,2,3,4
Август 2019

Ленинградская АЭС э/б № 2, 3,4,5
Сентябрь 2019

Калининская АЭС э/б № 1,2,3,4
Октябрь 2019

Руководство по проведению аудитов безопасности информации АСУ ТП. Методические рекомендации



КРИТЕРИИ:
Требования к процессам, технологиям и людям

Требования по обеспечению безопасности КИИ

Принципы проведения аудита

Приоритет ядерной, радиационной безопасности.

Независимость аудиторов.

Ответственность и конфиденциальность аудиторов.

Беспристрастность аудиторов.

Дифференцированный подход к выбору объемов и типов аудита.

Типы и виды аудитов

Этапы аудита

Этап 1. Планирование работ

- границы проведения аудита;
- ответственных руководителей подразделений со стороны АЭС за обеспечение условий для проведения аудита и выдачу исходных данных;
- подготовка Исполнителем программы проведения аудита
- разработка опросных листов
- согласование с Заказчиком программы аудита.

Этап 2. Подготовка к аудиту

- Сбор и анализ исходных данных

Этап 3. Проведение аудита

- анализ ОРД;
- проверка реализованных мер защиты на соответствие требованиям нормативных документов;
- анализ результатов анкетирования и интервьюирования;
- проведение интервью с персоналом;

Этап 4. Формирование отчета

- формирование аналитического отчета;
- согласование аналитического отчета с Заказчиком;

2 месяца

1 месяц

4 месяца (14 дней на каждой АЭС)

2 месяца

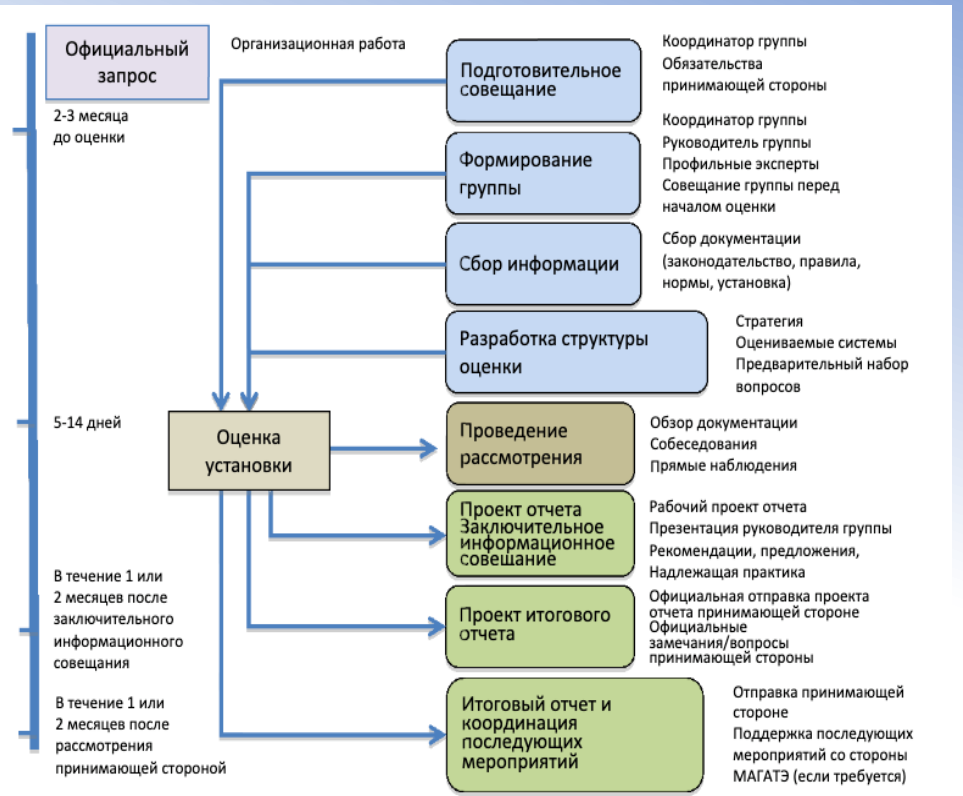


РИС. 1. Этапы и сроки оценки. Сроки могут быть скорректированы в соответствии с имеющимися ресурсами и временными ограничениями.

Источник: IAEA-TDL-006

Рабочая программа аудита

Акционерное общество
«Всероссийский научно-исследовательский институт
по эксплуатации атомных электростанций»
(АО «ВНИИАЭС»)

РОСЭНЕРГОАТОМ
ВНИИАЭС
Центр компетенций по кибербезопасности

ЦЕНТР КОМПЕТЕНЦИЙ АО «КОНЦЕРН РОСЭНЕРГОАТОМ» ПО КИБЕРБЕЗОПАСНОСТИ АСУ ТП АЭС

УТВЕРЖДАЮ

Заместитель генерального директора –
директор по производству и эксплуатации
АЭС АО «Концерн Росэнергоатом»

_____А.А. Дементьев
"____" _____ 2019

ПРОГРАММА
аудита кибербезопасности АСУ ТП
Филиала АО «Концерн Росэнергоатом» «Ленинградская АЭС»

Наименование объекта, подлежащего проверке:
АСУ ТП энергоблоков №2, 3, 4, 5

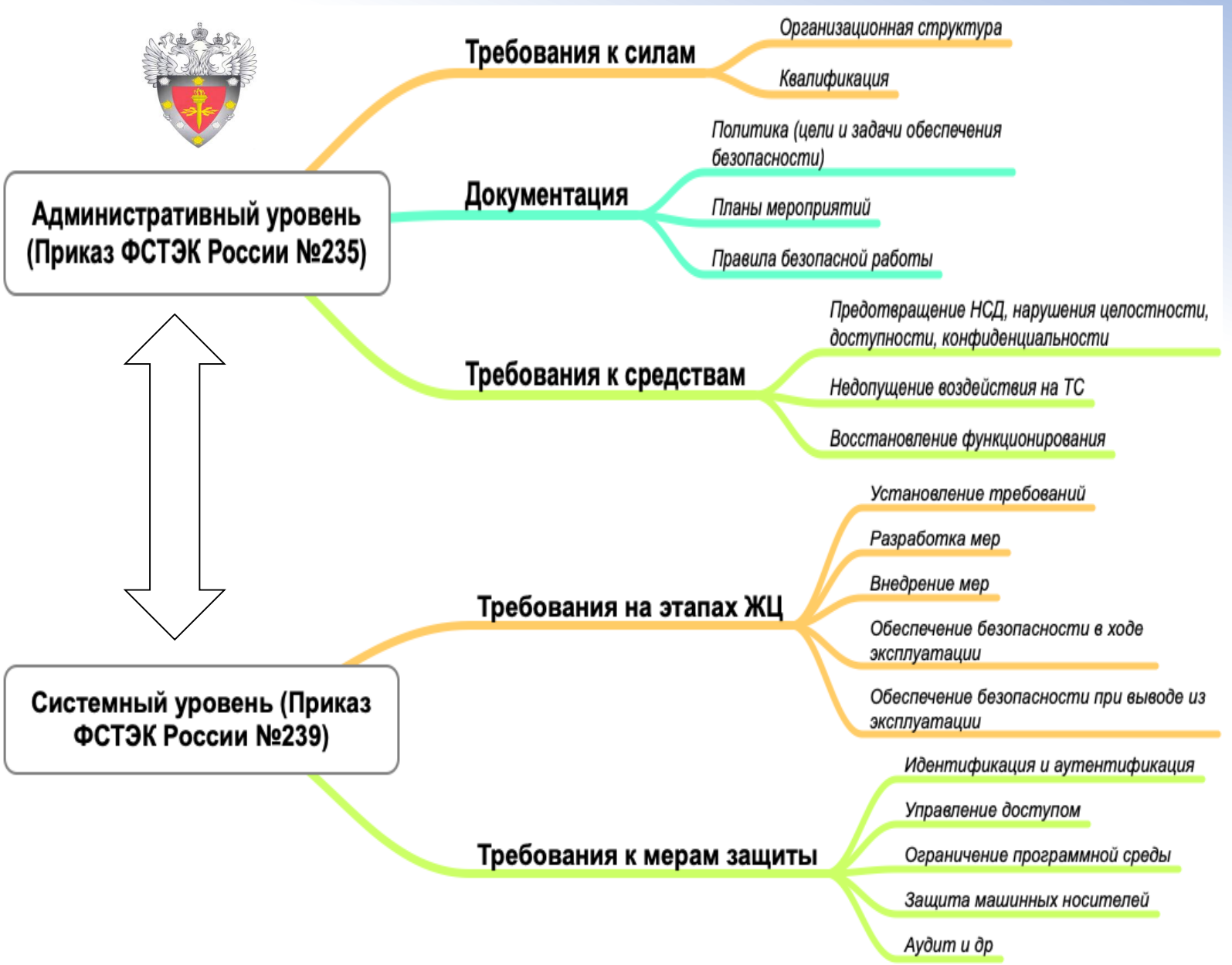
Состав комиссии организации проводящей аудит

№ п/п	Роль	Функции
1	**Руководитель комиссии**	Общее руководство процессом аудита. Контроль выполнение плана аудита.
2	**Заместитель руководителя комиссии**	Разработка плана аудита и формирование дневных программ аудита на площадке АС. Контроль выполнения работ. Координация работ Комиссии.
3	**Технический писатель**	Ведение детальных записей по аудиту. Анализ технических записок; Подготовка аналитического отчета по аудиту. Разработка опросных листов.
4	**Член комиссии**	Ведение детальных записей по аудиту. Подготовка аналитического отчета по аудиту. Проведение анализа исходных данных; Проведение интервьюирования персонала АС; Проведение осмотра объекта.
5	**Член комиссии**	Ведение детальных записей по аудиту. Подготовка аналитического отчета по аудиту. Проведение анализа исходных данных; Проведение интервьюирования персонала АС; Проведение осмотра объекта.

Исходные данные

- Организационная структура
- Отчет по обоснованию безопасности.
- Технические условия /Технические задания на подсистемы и комплексы АСУ ТП.
- Эксплуатационная документация на подсистемы и комплексы АСУ ТП.
- Организационно-распорядительная документация на систему защиты АСУ ТП АЭС.
- Модели угроз подсистем и комплексов АСУ ТП.
- Эксплуатационная документация на средства защиты.
- Результаты ранее проведенных аудитов.
- Виртуальные образы компонентов АСУ ТП и конфигурационные файлы средств защиты.

Рассматриваемые вопросы



- **Проверка общей ОРД по кибербезопасности АСУ ТП**
- **Проверка уровня квалификации персонала**
- **Проверка готовности персонала к реагированию на инциденты**
- **Проверка реализации мер защиты**
- **Оценка реализации СОКБ АСУ ТП**

ОЦЕНКА АДЕКВАТНОСТИ ДОКУМЕНТОВ → **ОЦЕНКА ТОГО, КАК НА САМОМ ДЕЛЕ**

Проверка реализации мер

№ п/п	Наименование группы мер	Наименование меры в группе	Вес меры в группе
1	2	3	4
1	I. Идентификация и аутентификация (ИАФ)	Разработка политики идентификации и аутентификации	100
2	I. Идентификация и аутентификация (ИАФ)	Идентификация и аутентификация пользователей и инициируемых ими процессов	30
3	I. Идентификация и аутентификация (ИАФ)	Идентификация и аутентификация устройств	19
4	I. Идентификация и аутентификация (ИАФ)	Управление идентификаторами	10
5	I. Идентификация и аутентификация (ИАФ)	Управление средствами аутентификации	10
6	I. Идентификация и аутентификация (ИАФ)	Идентификация и аутентификация внешних пользователей	22
7	I. Идентификация и аутентификация (ИАФ)	Двусторонняя аутентификация	5
8	I. Идентификация и аутентификация (ИАФ)	Защита аутентификационной информации при передаче	4
9	II. Управление доступом (УПД)	Разработка политики управления доступом	100
10	II. Управление доступом (УПД)	Управление учетными записями пользователей	11
11	II. Управление доступом (УПД)	Реализация политик управления доступом	12

Оценивается уровень реализации защитных мер в проверяемых подсистемах АСУ ТП. Для оценки уровня реализации защитных мер сформирован набор метрик на основе перечня защитных мер, приведенных в нормативных документах ФСТЭК России. В свою очередь меры сгруппированы по категориям в соответствии с направленностью защитных мер.

Каждой мере в группе присваивается вес по по значимости для защиты.

Инструментальный контроль защищенности. Основные положения

Инструментальный аудит не должен оказывать отрицательного влияния на технологический процесс.

Инструментальный аудит должен проводиться только в ППР или в период внеплановых остановов.

Средства инструментального аудита должны быть сертифицированными.

Запрещается применение средств инструментального аудита в управляющих системах безопасности.

Рекомендуется организация тестовых сред в достаточной мере повторяющих функционал, состав подсистем и комплексов АСУ ТП для проведения инструментального аудита.

Инструментальный контроль защищенности. Методы проведения

«черный», «серый» и «белый» ящик»

Виртуальная среда

Виртуальные образы компонентов АСУ ТП (АРМ, Серверы)

Конфигурационные файлы межсетевых экранов

Средства анализа защищенности (Kali Linux)

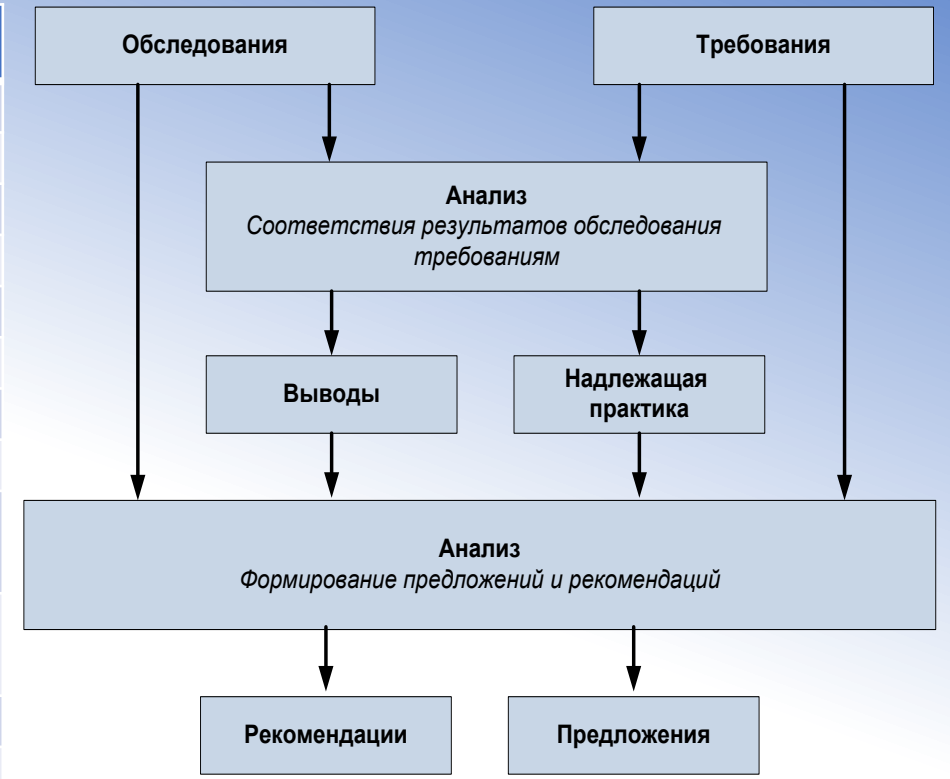
Сканер-ВС
анализ защищенности

Ручной анализ конфигураций компонентов АСУ ТП (журналов (log-файлов), конфигураций МЭ и др.)

Существуют ограничения: Некоторые компоненты АСУ ТП не поддерживают виртуализацию. Такие компоненты проверяются в рамках целевого аудита в период ППР.

Структура аналитического отчета

№	Наименование раздела/подраздела
-	Титульный лист
-	Краткий обзор проведенных работ
-	Сокращения
1	Введение
1.1	Сведения об организации проводящей аудит
1.2	Сведения о проверяемом объекте
1.3	Сведения о заказчике
1.4	Цели и объем аудита кибербезопасности АСУ ТП АС
1.5	Критерии и материалы, используемые для проведения аудита
1.5.1	Требования, взятые за основу для проведения аудита кибербезопасности АСУ ТП
1.5.2	Рассмотренная информация (исходные данные)
1.6	Процесс аудита
1.7	Содержание отчета
2	Основные выводы и рекомендации по результатам проведения аудита
2.1	Общий вывод
2.2	Перечень и краткое описание проверяемых вопросов и систем, подсистем и комплексов АСУ ТП
2.3	Непосредственные наблюдения на площадке АС
2.4	Специальные рекомендации, предложения, комментарии



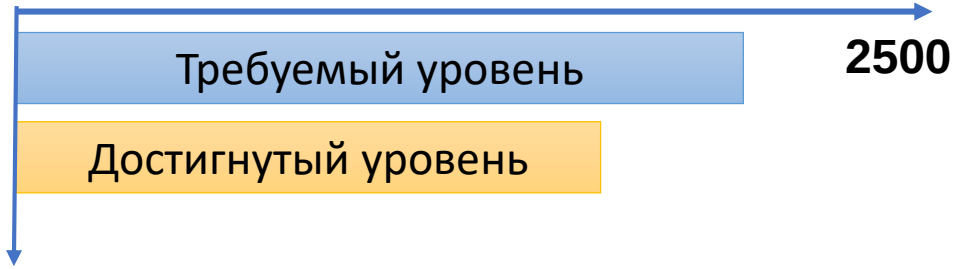
Структура аналитического отчета (основная часть)

Рассматриваемый вопрос

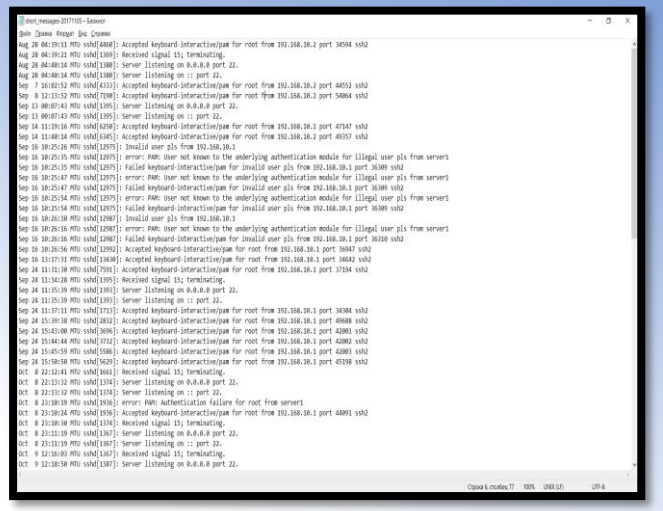
Критерий	Свидетельство	Анализ	Оценка

Область/ Вопросы аудита	Нерезультативно – требуются срочные меры	Недостаточно результативно – требуются улучшения	Достаточно результативно – возможны улучшения	Результативно – высокий уровень
Рассматриваемый вопрос			X	

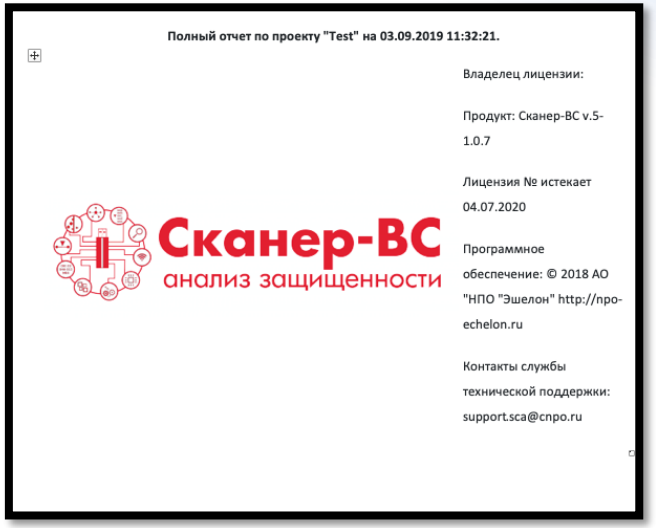
Уровень защищенности



Отчет об анализе конфигураций



Отчет об уязвимостях



Вместо результатов аудита – перечень известных компьютерных инцидентов на ОИАЭ

Месяц/Год	Наименование объекта	Страна	Описание	Тип инцидента
Июнь 2010	Завод по обогащению урана в Нетензе (Natanz Nuclear Facility)	Иран	Вирус **Stuxnet**, предназначенный для уничтожения центрифуг	Намеренный
Апрель 2011	Национальная лаборатория Ок-Ридж (Oak Ridge National Laboratory)	США	Кража данных с помощью целенаправленного фишинга (spear-phishing)	Намеренный
Сентябрь 2011	Areva	Франция	Сетевые атаки (сетевое проникновение)	Неизвестно
Октябрь 2011	Завод по обогащению урана в Нетензе (Natanz Nuclear Facility)	Иран	Вирус **Duqu**, используемый для проведения шпионажа	Намеренный
Май 2012	Завод по обогащению урана в Нетензе (Natanz Nuclear Facility)	Иран	Вирус **Flame**, используемый для проведения шпионажа	Намеренный
Ноябрь 2012	АЭС Саскуэханна (Susquehanna Nuclear Power Plant)	США	Технический сбой	Случайный/ Неумышленный
Январь 2014	АЭС Мондзю (Monju Nuclear Power Plant)	Япония	Публикация (разглашение, утечка) данных	Неизвестно
Декабрь 2014	KHNP (Korea Hydro and Nuclear Power Company)	Южная Корея	Кража и публикация (разглашение, утечка) данных	Намеренный
Февраль 2015	Японский центр контроля ядерных материалов (Japanese Nuclear Material Control Center)	Япония	Ядерный объект использовался в качестве промежуточной точки в компьютерной атаке	Неизвестно
Февраль 2016	NRC (Nuclear Regulatory Commission/U.S. Department of Energy)	США	Сотрудник пытался заразить правительственные компьютеры вирусами, целенаправленно распространяемыми по электронной почте (spear-phishing emails)	Намеренный
Апрель 2016	АЭС Гундреммингen (Gundremmingen Nuclear Power Plant)	Германия	Два вируса проникли в систему мониторинга топливных стержней (ТВЭЛов) станции	Неизвестно
Июнь 2016	Университет Тояма, Исследовательский центр по исследованию изотопов водорода (University of Toyama, Hydrogen Isotope Research Center)	Япония	Кража данных с помощью целенаправленного фишинга (spear-phishing)	Намеренный

СПАСИБО ЗА ВНИМАНИЕ!
ВАШИ ВОПРОСЫ!