РАСУ
РОСАТОМ

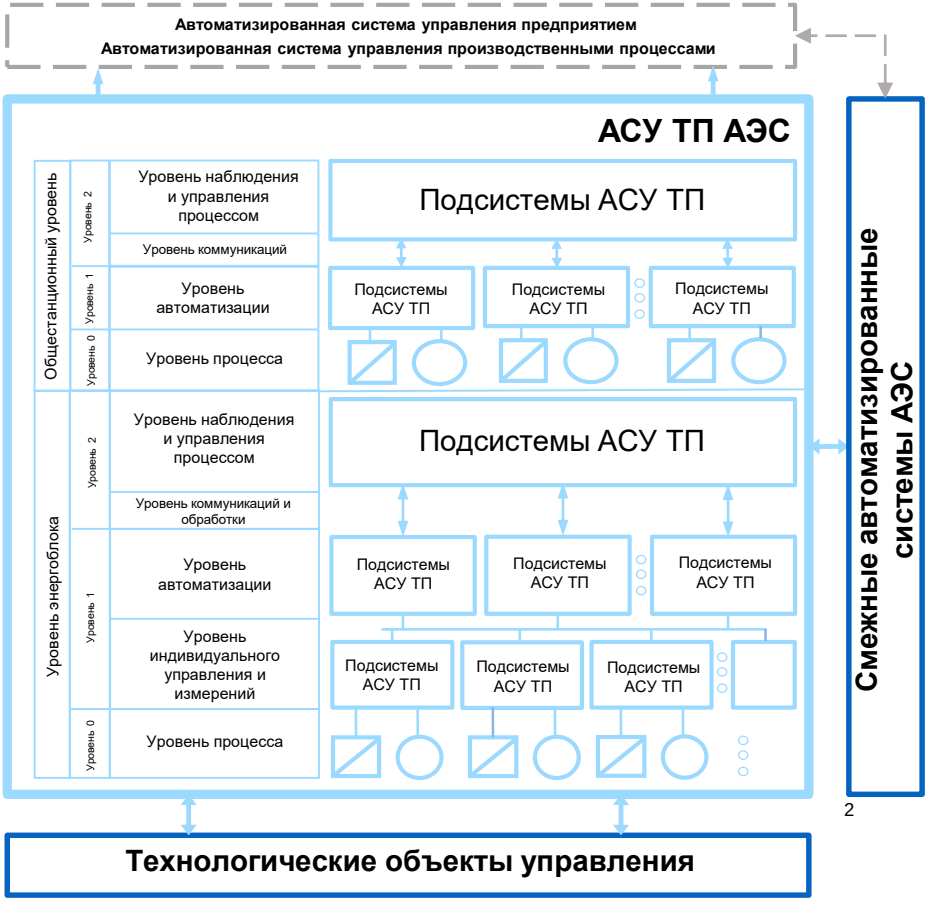
Безопасность АСУ ТП АЭС
Применение встроенных и наложенных СЗИ
Опыт внедрения

Код ИБ| INDUSTRIAL 2023

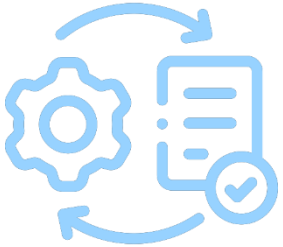
Застылова Людмила Юрьевна
Руководитель обособленного подразделения АО «РАСУ» в г. Екатеринбурге

АСУ ТП АЭС

* Представлена упрощенная схема взаимодействия систем между собой. Существую взаимосвязи между подсистемами АСУ ТП и внешними системами, которые также должны контролироваться и защищаться



Факторы, влияющие на обеспечение ИБ



Приоритет ядерной и радиационной безопасности

Отсутствие **значимого** негативного влияние на технологические процессы АСУ ТП

Взаимодействие АСУ ТП (подсистем АСУ ТП) со смежными и внешними автоматизированными системами

Разные изготовители подсистем АСУ ТП/ систем АСУ ТП/ ПТК и оборудования

Разные используемые принципы и алгоритмы

Ограниченный выбор средств защиты информации

Программное обеспечение собственной разработки

Проприетарные протоколы передачи данных

Ограничение на использование «основных» (технологических) каналов связи (ограничения на прямую передачу «вспомогательных» данных (диагностика, траффик, сислоги и т.д.)

Одна и та же подсистема АСУ ТП

↓

Разные проекты (АЭС)

↓

Разные генпроектировщики

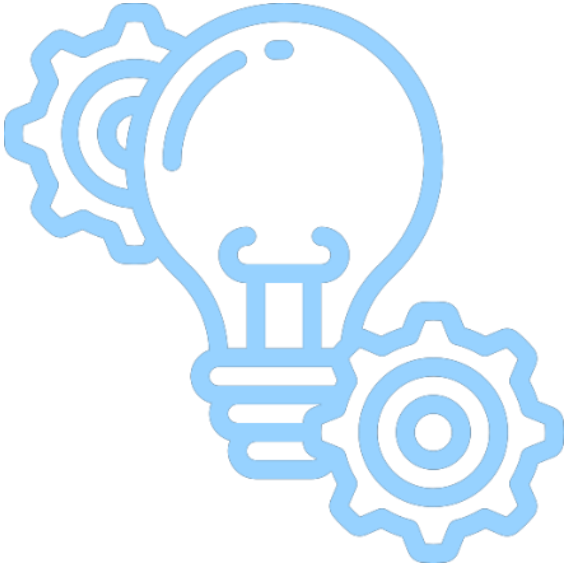
↓

Разные изготовители

↓

Разные принципы и линейки оборудования

Концептуальные подходы к обеспечению ИБ АСУ ТП АЭС



Вариант №1. Внедрение мер ИБ:

- на уровне подсистем АСУ ТП
- на уровне АСУ ТП **в целом**

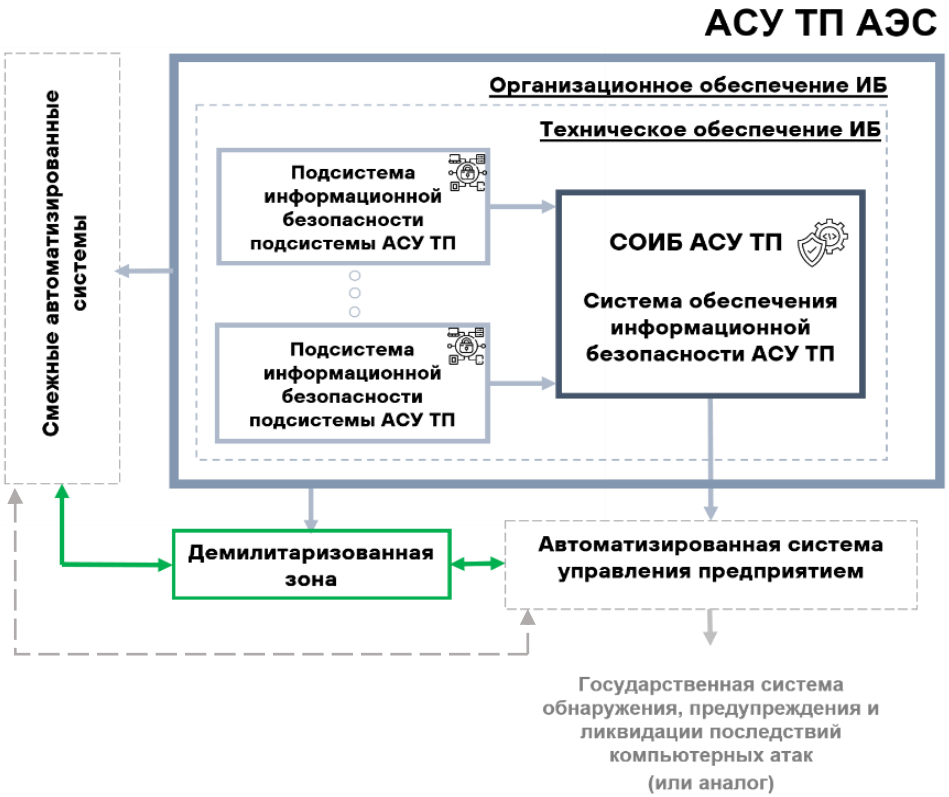
Вариант №2. Внедрение мер ИБ:

- на уровне подсистем АСУ ТП

Вариант №3. Внедрение мер ИБ:

- в **отдельных** подсистемах АСУ ТП

Вариант №1. Комплексный



Превентивный подход

Детективный подход

Подсистема информационной безопасности

представляет из себя совокупность организационных и технических мер по обеспечению информационной безопасности, принятых в соответствии с присвоенной подсистеме АСУ ТП категорией значимости / степенью безопасности / классу защищенности

СОИБ АСУ ТП АЭС

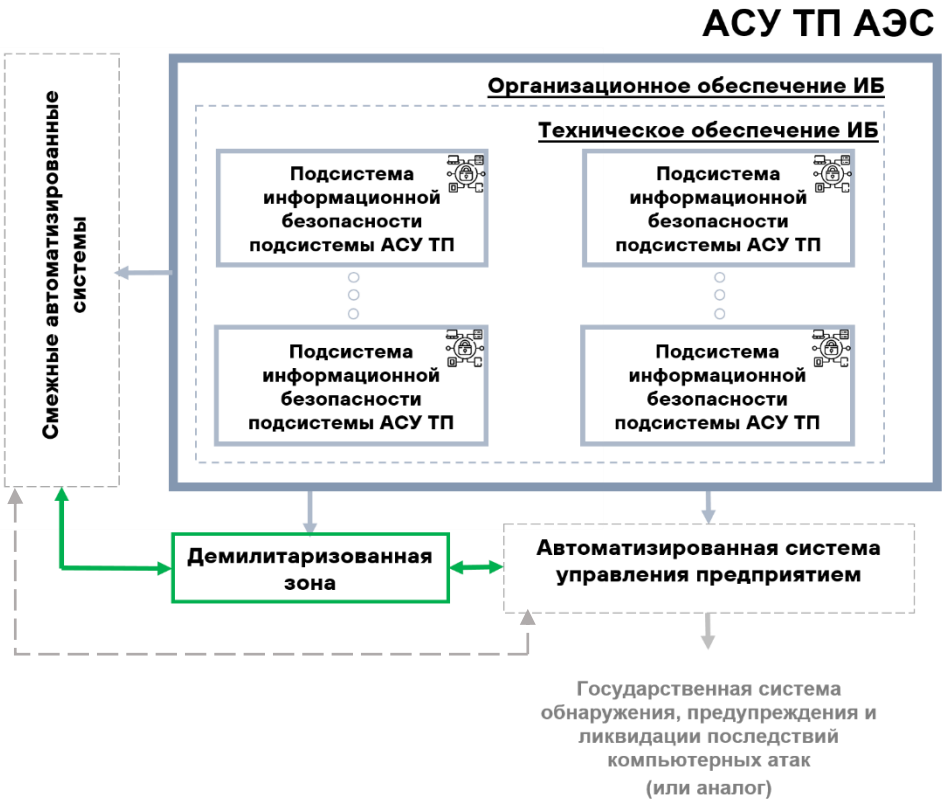
подсистема АСУ ТП основной задачей которой является обнаружение нарушения состояния ИБ АСУ ТП АЭС **путем сбора и анализа данных от и об подсистемах АСУ ТП** (сетевой траффик, журналы событий, сведения об уязвимостях компонентов подсистем) с последующим информированием ответственных лиц

Организационное обеспечение ИБ

представляют из себя совокупность регламентирующих правил и процедур обеспечения ИБ, изложенных в ОРД АЭС и Процедурах реализации мер ИБ на подсистемы АСУ ТП

Подсистема информационной безопасности = Подсистема безопасности (приказ ФСТЭК России №239)

Вариант №2



Превентивный подход

Подсистема информационной безопасности

представляет из себя совокупность организационных и технических мер по обеспечению информационной безопасности, принятых в соответствии с присвоенной подсистеме АСУ ТП категорией значимости / степенью безопасности / классу защищенности

Организационное обеспечение ИБ

представляют из себя совокупность регламентирующих правил и процедур обеспечения ИБ, изложенных в ОРД АЭС и Процедурах реализации мер ИБ на подсистемы АСУ ТП

Вариант №2 уместен в случае отсутствия размещения СОИБ АСУ ТП на действующих объектах

Вариант №2. Переходный

Превентивный подход

Детективный подход

Подсистема информационной безопасности

представляет из себя совокупность организационных и технических мер по обеспечению информационной безопасности, принятых в соответствии с присвоенной подсистеме АСУ ТП категорией значимости / степенью безопасности / классу защищенности

Мини - СОИБ АСУ ТП АЭС

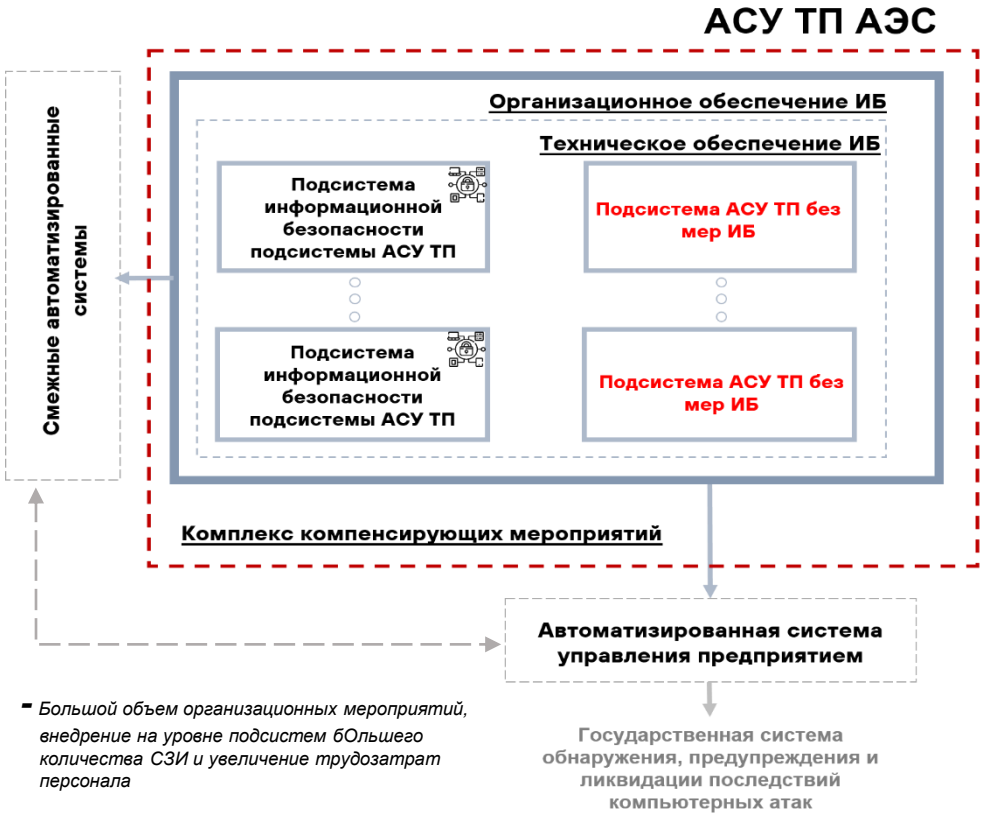
частичная реализации СОИБ АСУ ТП. Определение подсистем, в которых возможна частичная реализация компонентов СОИБ и их внедрения при модернизации. В других подсистемах – проведение подготовки при модернизациях к дальнейшему переходу на Вариант №1

Организационное обеспечение ИБ

представляют из себя совокупность регламентирующих правил и процедур обеспечения ИБ, изложенных в ОРД АЭС и Процедурах реализации мер ИБ на подсистемы АСУ ТП

Вариант №2. Переходный уместен в случае плановой поэтапной модернизации систем

Вариант №3. Компенсирующий



- *Большой объем организационных мероприятий, внедрение на уровне подсистем бОльшего количества СЗИ и увеличение трудозатрат персонала*

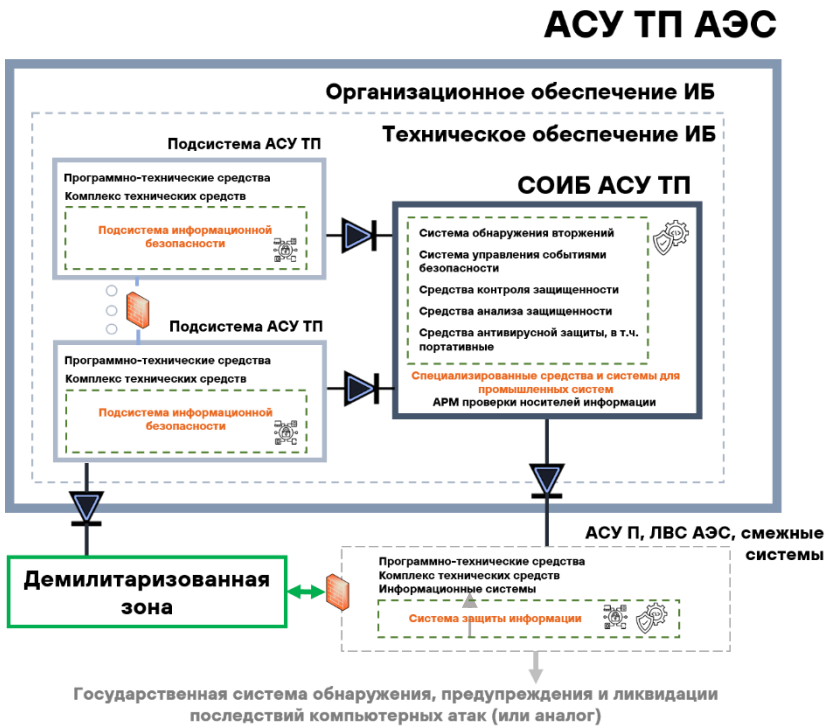
Превентивный подход
и компенсирующие мероприятия

Подсистема информационной безопасности
представляет из себя совокупность организационных и технических мер по обеспечению информационной безопасности, принятых в соответствии с присвоенной подсистеме АСУ ТП категорией значимости / степенью безопасности / классу защищенности

Организационное обеспечение ИБ
представляют из себя совокупность регламентирующих правил и процедур обеспечения ИБ, изложенных в ОРД АЭС и Процедурах реализации мер ИБ на подсистемы АСУ ТП

Вариант №3 уместен в случае отсутствия размещения СОИБ АСУ ТП на действующих объектах и плановой поэтапной модернизации подсистем АСУ ТП и без возможности в ближайшую волну модернизации внедрить СОИБ АСУ ТП

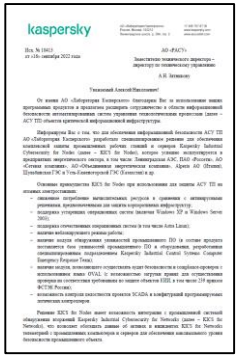
Вариант №1. Реализация



- ✓ В каждой подсистеме АСУ ТП должна быть спроектирована и внедрена **подсистема информационной безопасности**
- ✓ Организуются **демилитаризованные зоны** для однонаправленной передачи данных из подсистем АСУ ТП в АСУ П / ЛВС АЭС /смежные (есть исключения) и/или внешние системы при выполнении требований информационной безопасности

- ✓ В состав **СОИБ АСУ ТП** входят:
- специализированные средства и системы для промышленных систем
- **портативные средства антивирусной защиты** для проведения периодической антивирусной проверки в подсистемах АСУ ТП, в которых по объективным причинам невозможна установка «стационарного» средства антивирусной защиты
- анализаторы Wi-Fi сетей
- специализированные средства для проведения анализа защищенности
- специализированные средства для контроля защищенности
- АРМ проверки носителей информации

Вариант №1. Проблемные вопросы



С сентября 2022 г. KES не может применяться в АСУ ТП

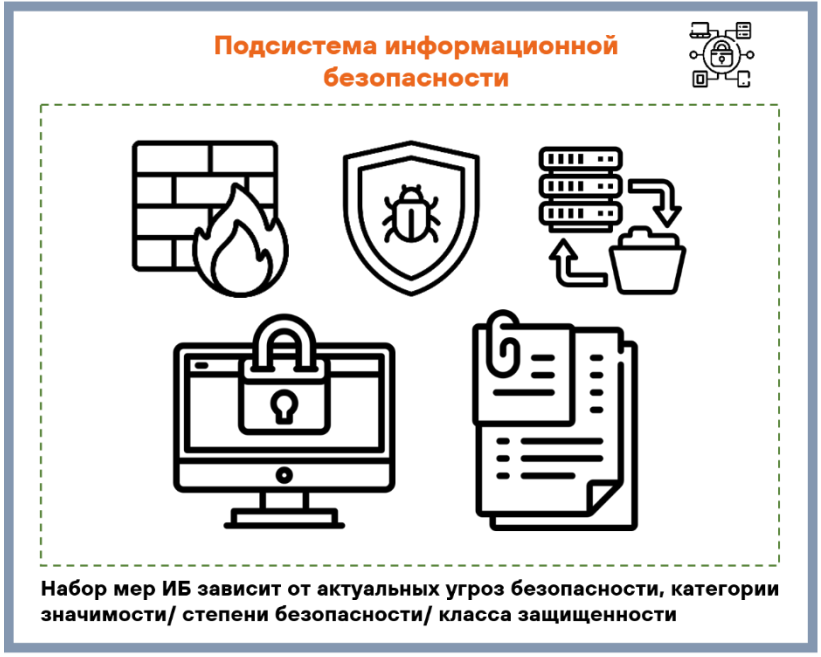
Пример выявленной при испытаниях проблемы корпоративных САВЗ:

при отсутствии компонента «центр обновления», утилита для офлайн обновлений есть только по ОС Windows. Для ОС семейства Linux процесс заключается в скачивании сигнатурных баз из сети общего пользования Интернет с помощью утилиты под ОС Windows и копирование их в папку САВЗ. При этом обновление баз не отображается и не подтверждается самим САВЗ

- ✓ Ограниченный выбор средств защиты информации
- ✓ Влияние СЗИ (настроек СЗИ), обновлений СЗИ и ПО на штатное функционирование подсистемы АСУ ТП
- ✓ Несоответствие заявляемого функционала фактическому состоянию (фактор «отечественных аналогов»)
- ✓ **Межсетевое экранирование**
  - Невозможность установки аппаратного МЭ на границах подсистемы АСУ ТП (серийно выпускаемые КТС, дополнительная точка отказа, влияние на надежность системы, проектные сроки – изменение РКД, повторные квалификационные испытания)
  - Встроенные в ОС средства межсетевого экранирования не сертифицированы и не могут применяться в качестве МЭ
- ✓ Отсутствие встроенных средств защиты информации в прикладном программном ПО (собственная разработка Поставщиков)
- ✓ **Средства антивирусной защиты**
  - Ограниченный выбор сертифицированных САВЗ, возможных к применению в АСУ ТП
  - Влияние САВЗ на технологический процесс
  - Ограничение применения корпоративных решений (САВЗ) в промышленных системах
  - Стоимость специализированных САВЗ
- ✓ Совместимость SIEM-систем на уровне АСУ ТП и АСУ П
- ✓ Разбор проприетарных протоколов
- ✓ Режим работы СОИБ АСУ ТП при проведение ППР
- ✓ Ограничение на количество персонала, обеспечивающего ИБ АСУ ТП
- ✓ …

Вариант №1. Пути решения (укрупненно)

Подсистема АСУ ТП АЭС



КОНТРОЛЬ ПЕРИМЕТРА. Обеспечение ИБ при взаимодействии как со смежными подсистемами АСУ ТП, так и со смежными АС АЭС и внешними АС

*Применение **АПМДЗ или ПМДЗ** на АРМ в подсистемах АСУ ТП отдельных случаях при актуальных угрозах и способах реализации*

- ✓ **Программное обеспечение собственной разработки**
  - Установка требований по наличию ВСЗИ через моделирование угроз
  - Внедрение процессов безопасной разработки ПО
  - Аудит внедрения процессов безопасной разработки ПО
- ✓ **Межсетевое экранирование**
  - Включение в конструктив КТС на ранних этапах проектирования подсистем АСУ ТП
  - Настройка netfilter в ОС Linux, как одной из компенсирующих мер, и дополнительное тестирование на этапе предварительных испытаний
  - Тестирование и оценка влияния программных МЭ на технологический процесс
- ✓ **Средства антивирусной защиты**
  - Использование САВЗ для промышленных систем
  - Тестирование влияния САВЗ на технологический процесс до этапа испытаний (макет, испытательный стенд)
  - «Тонкая» настройка САВЗ, отключение модуля активной защиты, ограничение потребления ресурсов и т.д.)
  - Использование портативного САВЗ в отдельных случаях
- ✓ **Встроенные средства защиты в ПТС**: ИАФ, УПД, АУД и прочие меры ИБ
- ✓ **Организационные меры обеспечения ИБ** – унифицированный подход

Непрерывный процесс:

тестирования СЗИ российского производства (ПО, ПАК);
тестирования ПТС с ВСЗИ российского производства;
взаимодействия с отечественными вендорами

Вариант №1. СОИБ АСУ ТП АЭС

СОИБ АСУ ТП

Система обнаружения вторжений

Система управления событиями безопасности

Средства контроля защищенности

Средства анализа защищенности

Средства антивирусной защиты, в т.ч. портативные

Специализированные средства и системы для промышленных систем

АРМ проверки носителей информации

При тестировании диодов разных производителей выявлены несоответствия в заявляемых функциях и сложности при реализации взаимодействия между системами

- **SIEM**
- Средство мониторинга событий информационной безопасности. Информация о состоянии работы и событиях передаётся посредством протокола Syslog или протокола SNMP в режиме реального времени.
- **СОВ**
- Средство для обнаружения вторжений. Для его работы используется копия сетевого трафика, полученного с помощью технологии зеркалирования.
- **АВЗ**
- Средство антивирусной защиты. Используется активный режим работы, который предполагает не инвазивные методы защиты. Подозрительный файл не удаляется и не помещается в карантин, но оператор информируется о угрозе.
- Дополнительные вспомогательные программные средства

SIEM Классический SIEM

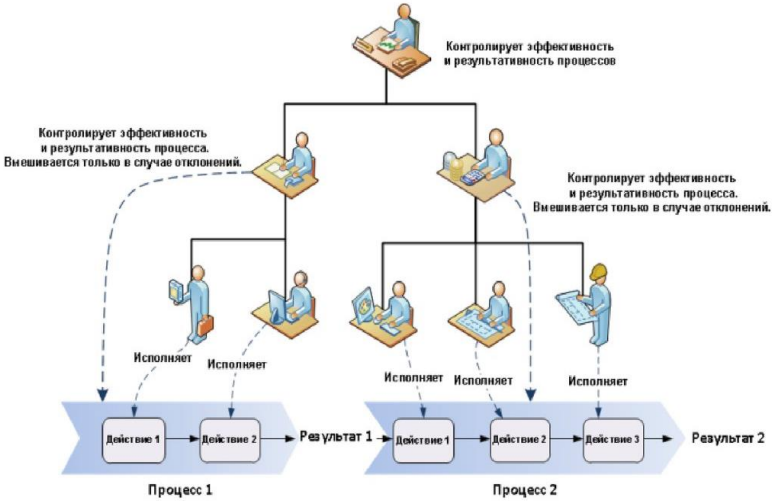
SIEM SIEM с «особыми» режимами

SIEM SIEM с доп. реализацией функционала для оперативного персонала

SIEM Дополнительные уникальные правила корреляции (пакеты экспертизы)

Вариант №1. СОИБ АСУ ТП АЭС. Оргобвязка

№ п/п	Наименование документа
	ПОРЯДКИ
1	Порядок по обеспечению информационной безопасности АСУ ТП
	ПРИКАЗЫ
2	Приказ об определении ответственных лиц за выполнение требований по обеспечению информационной безопасности
3	Приказ о разделении ответственности за функционирование подсистем АСУ ТП АЭС
	ПЛАНЫ
4	План обеспечения и контроля информационной безопасности АСУ ТП, в составе
4.1	План мероприятий по анализу уязвимостей
4.2	План проведения мониторинга событий информационной безопасности
4.3	План проведения внутренних аудитов
4.4	План проведения внешних аудитов
4.5	План проведения контроля целостности информации и программного обеспечения
4.6	План проведения контроля доступности технических средств
4.7	План проведения резервного копирования информации и программного обеспечения
4.8	План проведения инвентаризации и контроля конфигурации
4.9	План проведения информирования и обучения персонала
	РЕГЛАМЕНТЫ
5	Регламент обеспечения и контроля информационной безопасности АСУ ТП, в составе
5.1	Регламент управления идентификаторами и средствами аутентификации
5.2	Регламент управления доступом
5.3	Регламент по ограничению программной среды
5.4	Регламент по порядку учета, хранения, обращения и уничтожения машинных носителей информации
5.5	Регламент проведения мероприятий по анализу и устранению уязвимостей
5.6	Регламент проведения мониторинга событий информационной безопасности



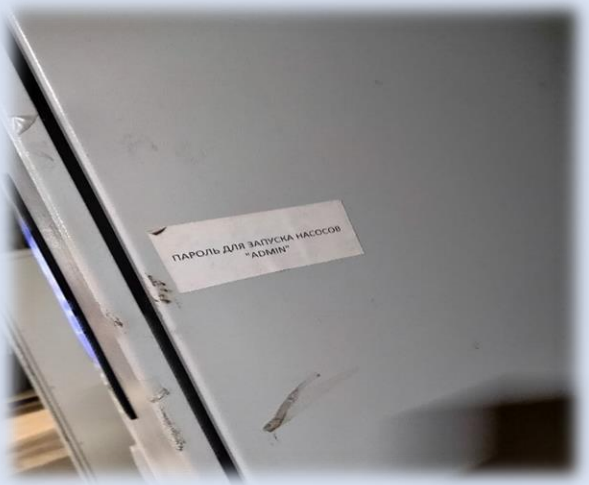
РЕГЛАМЕНТ ПО РЕАГИРОВАНИЮ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

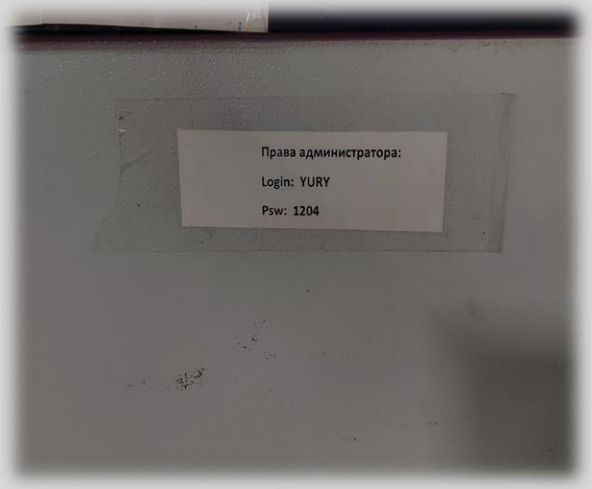
5.7	Регламент проведения аудита безопасности
5.8	Регламент проведения антивирусной защиты
5.9	Регламент контроля целостности информации и программного обеспечения
5.10	Регламент проведения контроля доступности технических средств
5.11	Регламент проведения резервного копирования и восстановления информации и программного обеспечения
5.12	Регламент по организации хранения и использования средств восстановления информации и программного обеспечения
5.13	Регламент защиты информационной (автоматизированной) системы и ее компонентов
5.14	Регламент по проведению инвентаризации и контроля конфигурации
5.15	Регламент управления обновлениями программного обеспечения

Напоследок

РАСУ РОСАТОМ

Примеры выявленных в ходе сбора исходных данных нарушений базовых требований ИБ





Спасибо за внимание

Застылова Людмила Юрьевна
Руководитель обособленного подразделения АО «РАСУ» в г. Екатеринбурге

Тел.: +7 (495) 933-43-40 доб. 20702
E-mail: LyYZastylova@rasu.ru
www.rasu.ru

12.07.2023