РАСУ

РАСУ
РОСАТОМ

Обеспечение ИБ АСУ ТП при переходе от внешнего управления ИТ-инфраструктурой со стороны зарубежных компаний к российским владельцам. Проблематика и практика реализации

Застылова Людмила
Руководитель обособленного подразделения
АО «РАСУ»

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn’t lead to any obligations to RASU and its affiliated companies.
RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

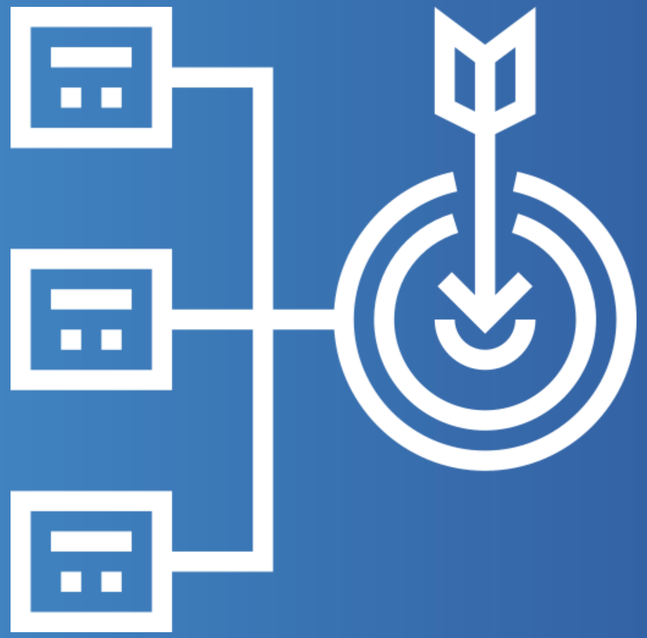
РАСУ

Основная проблематика

ПРОБЛЕМАТИКА

- Большое количество компаний на территории РФ в разных отраслях промышленности долгое время находилось под управлением зарубежных партнеров
- Уход с российского рынка зарубежных компаний, владеющих предприятиями, в состав которых входят потенциальные объекты КИИ РФ, и неготовность к безболезненному переходу на «новые рельсы»

РАСУ



Цели и задачи

ЦЕЛИ И ЗАДАЧИ

Цели:

Глобальная цель:

Сохранение стратегических для экономики страны отраслей промышленности при уходе иностранного капитала

Локальная цель:

Сохранение непрерывности производства для обеспечения стабильности бизнеса при переходе управления от зарубежного владельца в ведение российской компании

Задачи:

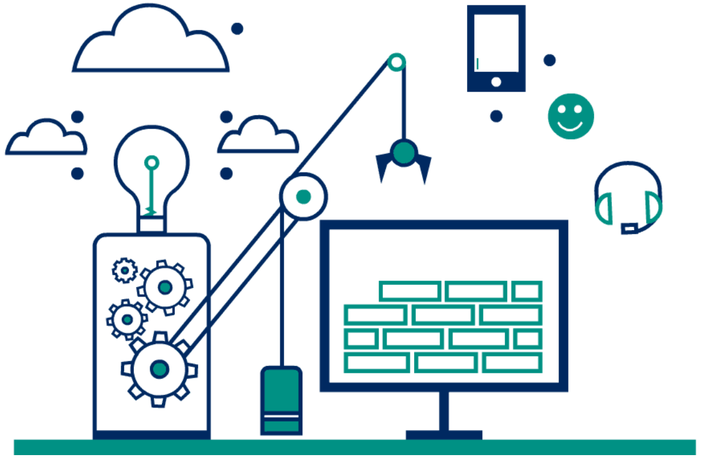
- ❑ Исключение останова производства после подписания договора купли-продажи предприятия
- ❑ Исключение возможного влияния «бывших» зарубежных владельцев на текущие производственные процессы предприятия
- ❑ Обеспечение ИБ технологического сегмента АСУ ТП предприятия

- ❑ Обеспечение заделов для последующего перехода на отечественное технологическое оборудование и российское программное обеспечение

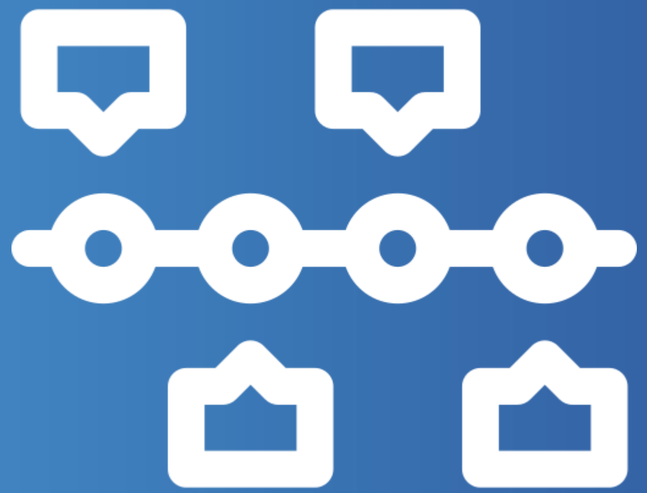
ОГРАНИЧИВАЮЩИЕ ФАКТОРЫ И РИСКИ

- **Простой производственного процесса более, чем на 30 минут способен вывести из строя технологическое оборудование предприятия (фактор непрерывности производства)**

- **Удаленное управление корпоративными и технологическими процессами предприятия, а, следовательно:**
  - Отсутствие возможности заранее проводить инвазивные подготовительные работы (удаленное отслеживание всей сетевой инфраструктуры зарубежным владельцем)
  - Угроза остановки технологического процесса вследствие отключения ПО АСУ ТП
  - Отсутствие собственной ИТ и ИБ службы на предприятии
  - Отсутствие у персонала предприятия документации на сетевую инфраструктуру, оборудование, ПО, резервных копий и прочих важных сведений



РАСУ



Этапность работ

ЭТАПНОСТЬ РАБОТ

1. Сбор и анализ исходных данных
2. Анализ уязвимостей
3. Реализация мер и процедур ИБ
4. Документирование результатов работ
5. Выдача рекомендаций

СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ

1 этап

Состав работ

Определение:

- Особенностей технологического процесса
- Типов и версий применяемого ПО
- Типов и версий применяемого оборудования
- Сведений для формирования схемы сетевой инфраструктуры

Методы и средства проведения работ

- Инвентаризация информационных ресурсов предприятия
- Опрос обсуживающего персонала
- Сбор данных сетевой инфраструктуры с помощью инструментальных средств

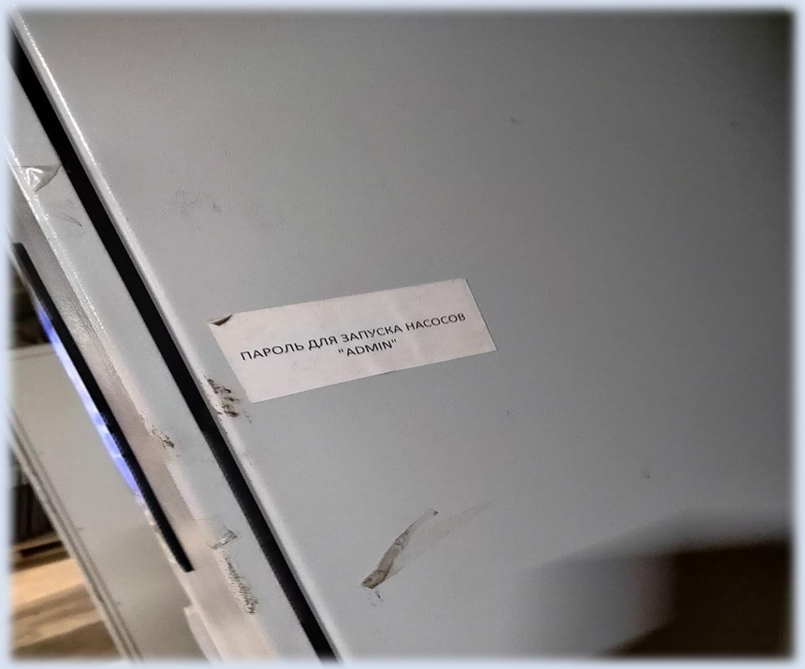
Результаты

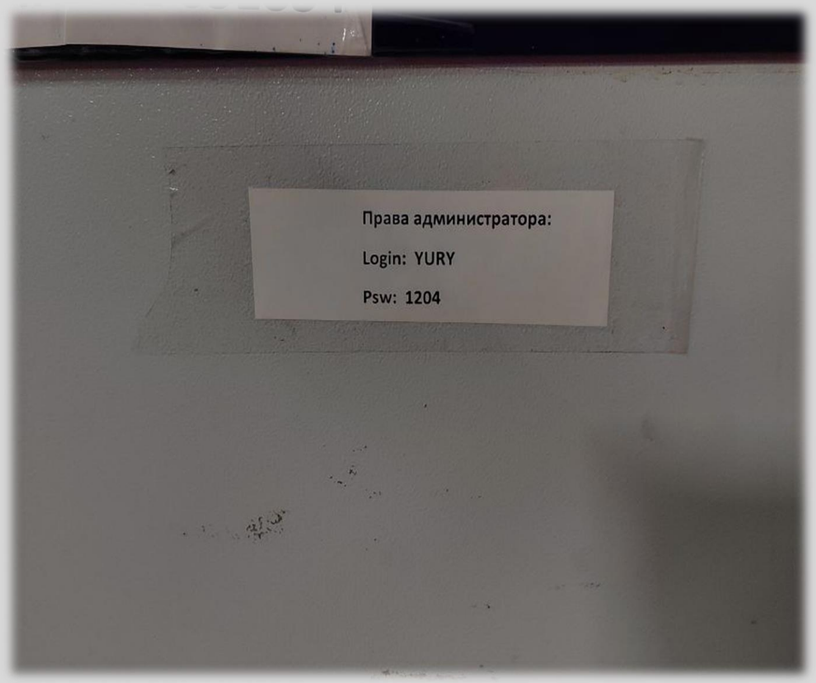
- Перечень используемых технических средств и ПО
- Схема сети предприятия
- Очевидные нарушения требований ИБ в производственных участках предприятия

СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ

1 этап

Примеры выявленных в ходе сбора исходных данных нарушений базовых требований ИБ





АНАЛИЗ УЯЗВИМОСТЕЙ

2 этап

Состав работ

- Проведение антивирусных проверок промышленных серверов и АРМ
- Сканирование инфраструктуры АСУ ТП на наличие беспроводных сетей и интерфейсов передачи данных
- Проведение проверки на наличие уязвимостей в АРМ и промышленных серверах

Методы и средства проведения работ

Для проведения перечисленных работ использовались мобильные технические средства (ноутбуки) с установленным ПО:

- средства антивирусной защиты
- средства для анализа
- клиентская программа для работы с сетевыми протоколами

Результаты

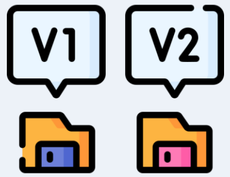
- Антивирусная проверка не выявила актуальных вирусных угроз на дату проведения проверки
- Сканирование выявило наличие беспроводных интерфейсов передачи данных и действующие Wi-Fi сети в сегменте АСУ ТП
- Проверка уязвимостей выявила критичные уязвимости в установленном ПО

АНАЛИЗ УЯЗВИМОСТЕЙ

2 этап

Выявлены критичные уязвимости:

ПО и ТС для удаленного администрирования



Уязвимые версии ПО и протоколов передачи данных

Устранены уязвимости:

- Исключены беспроводные технологии передачи данных в технологическом сегменте АСУ ТП
- Удалены агенты ПО для удаленного администрирования с промышленных серверов сегмента АСУ ТП

Следующие уязвимости не устранены на месте в связи с риском нарушения технологического процесса:

- Не произведено отключение модемов для предоставления удаленного доступа к технологическому оборудованию. Приняты компенсирующие меры по безопасному использованию данных каналов связи
- Не устранены уязвимости ПО, связанные с использованием устаревших версий. Приняты компенсирующие меры для нивелирования данных уязвимостей

РЕАЛИЗАЦИЯ МЕР И ПРОДЕДУР ИБ

3 этап

Состав работ

- Изолирование сегмента АСУ ТП от корпоративного сегмента предприятия и сети «Интернет»
- Настройка локальной синхронизации времени внутри технологического сегмента АСУ ТП
- Настройки функций ИБ в оборудовании
- Внедрение организационных мер обеспечения ИБ

Методы и средства проведения работ

- Проведение работ в технологическом сегменте с использованием мобильных технических средств
- Непосредственное взаимодействие с обслуживающим персоналом

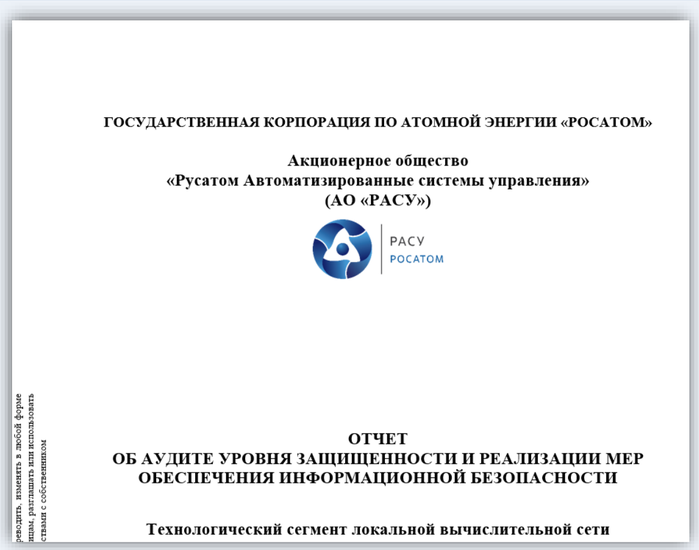
Результаты

- Удаление физических сетевых соединений с коммутаторами корпоративной сети, исключение доступа к технологическому сегменту из сети Интернет
- Удаление учетных записей предыдущих владельцев, настройка парольной политики и прочих функций ИБ
- Отключение общедоступных компьютерных розеток
- Настройка синхронизации времени в сегменте АСУ ТП
- Информирование персонала о требованиях ИБ

ФИНАЛЬНЫЕ ЭТАПЫ

Документирование и выдача рекомендаций

Документирование результатов выполненных работ



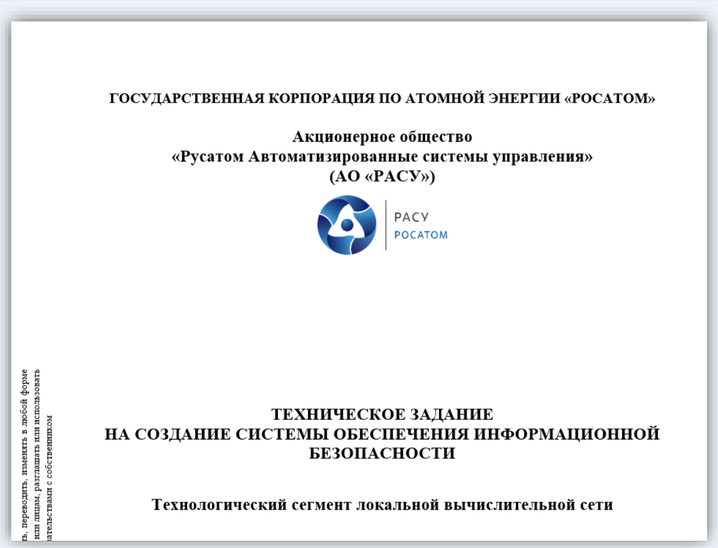
ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

Акционерное общество
«Русатом Автоматизированные системы управления»
(АО «РАСУ»)

РАСУ
РОСАТОМ

ОТЧЕТ
ОБ АУДИТЕ УРОВНЯ ЗАЩИЩЕННОСТИ И РЕАЛИЗАЦИИ МЕР ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Технологический сегмент локальной вычислительной сети



ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

Акционерное общество
«Русатом Автоматизированные системы управления»
(АО «РАСУ»)

РАСУ
РОСАТОМ

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА СОЗДАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Технологический сегмент локальной вычислительной сети

В качестве следующих шагов для развития ИБ АСУ ТП необходимо:

- ❑ Разработать план перехода на отечественную программную и аппаратную платформу или зарубежные аналоги из дружественных стран
- ❑ Выполнить категорирование объекта(ов) критической информационной инфраструктуры. Категорирование должно быть проведено в соответствии с действующими на момент проведения работ Постановлениями Правительства РФ и нормативными правовыми актами ФСТЭК России (Постановление Правительства РФ от 08.02.2018 №127, приказ ФСТЭК России от 22.12.2017 №236)
- ❑ Создать подразделение, ответственное за обеспечение ИБ АСУ ТП.
- ❑ Внедрение полноценной системы обеспечения информационной безопасности.

РАСУ

Итоги

ИТОГИ

Внедрение ИБ АСУ ТП

Опыт данного кейса показал нам, что не существует УНИВЕРСАЛЬНОГО ИДЕАЛЬНОГО подхода к реализации требований ИБ при подобных обстоятельствах. В таких случаях мы рекомендуем:

- ❑ Оценивать ограничения и риски, которые накладывает технологический процесс конкретного предприятия
- ❑ Анализировать каждый шаг и этап по внедрению функций ИБ, оценивать результат
- ❑ Осуществлять поэтапную интеграцию функций ИБ в технологический сегмент
- ❑ Учитывать, что обеспечить ИБ в полном объеме сразу невозможно, не бояться переходных периодов!

Внешние факторы

Геополитическая обстановка

Увеличение числа хакерских атак

Санкционный режим

Ограничения и риски

Негативное влияние на технологический процесс

Сокращение или останов производства

Технологическая безопасность

РАСУ

Вопрос-ответ

РАСУ

РАСУ
РОСАТОМ

115230, Москва, Каширское шоссе, д. 3, корп. 2, стр.16,
деловой квартал «Сириус Парк»
+7 495 933 43 40
info@rasu.ru

rasu.ru