РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Кибербезопасность АСУ ТП – вызовы времени

АО «РАСУ»

Юлия Черникова

Коммерческий директор направлений «Информационная безопасность» и «Доверенные цифровые решения»

Деятельность АО «РАСУ» в области ИБ АСУ ТП

Зарубежные проекты
- Венгрия, Пакш-2
- Турция, Аккую
- Египет, Эль-Дабаа
- Бангладеш, Руппур
- Белорусская АЭС
- Индия, Куданкулам

Проекты РФ
- Калининская АЭС
- Ростовская АЭС
- Курская АЭС-2
- Нововоронежская АЭС
- Ленинградская АЭС-2
- Белоярская АЭС

Взаимодействие с комитетами и регуляторами в России
- ТК 362 «Защита информации» на базе ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
- ТК 167 «Программно-аппаратные комплексы для критической информационной инфраструктуры и программное обеспечение для них»
- Совет по информационной безопасности в Госкорпорации «Росатом» и ее организациях

Международная деятельность (WANO, IAEA)
- Разработка руководств и рекомендаций по компьютерной безопасности
- Участие в рабочих группах по компьютерной безопасности

Участие в экспертном совете разработки ядра Linux

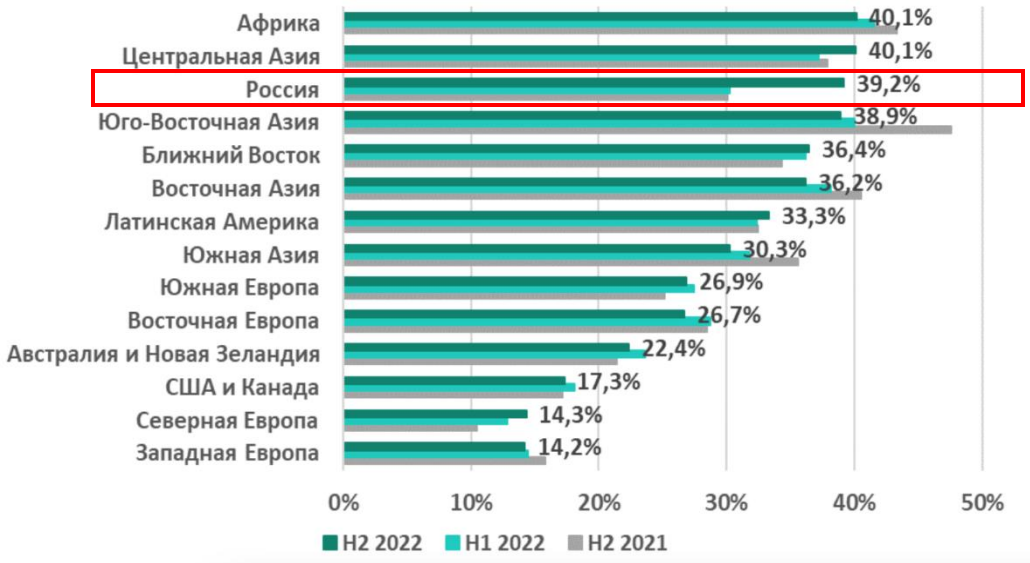
Рост роли кибератак в военных конфликтах

«Я это говорил в Запорожье, я это говорил в Киеве, я это сейчас говорю в Калининграде: такие объекты, как АЭС, никогда не могут быть легитимной целью в вооруженном конфликте»

Рафаэль Гросси, Генеральный директор МАГАТЭ

420 млн **кибератак на объекты КИИ по всему миру произошло в 2023 году (на 30% больше, чем в 2022)***

Динамика роста атак на АСУ ТП в России и мире**



* по данным исследования KnowBe4
**по данным исследований Kaspersky Lab

Вызовы времени

РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Кибератаки на критическую инфраструктуру стали одним из ключевых аспектов в современных политических и военных конфликтах

Цели нападения на объекты КИИ

- Усиление уязвимости
- Инфраструктурный хаос
- Экономические потери
- Эскалация конфликта
- Усиление внутриполитической напряженности
- Психологическое давление на население

Примеры кибератак на объекты КИИ

Зарубежные примеры кибератак

- **2014 год** – атака хакерской группы Kimsuky на две АЭС в Южной Корее: Кори и Вольсон
- **2014 год** – заражение вирусом компьютеров АЭС Мондзю, Япония
- **2019 год** – массированная хакерская атака на автоматическую систему контроля ГЭС Эль-Гури, Венесуэла
- **2024 год** – таргетированная кибератака на нефтегазовую отрасль через цепочку поставок TetraSoft

Примеров множество, и все они показывают, что объектом кибератаки сегодня может стать любое предприятие

* Источники: www.infowatch.ru, www.sibmeda.ru, www.rbc.ru, www.tadviser.ru, Lenta.ru

Проблемы обеспечения кибербезопасности на промышленных объектах

РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

1. Зависимость от импорта
2. Непроверенное ПО и производители
3. Устаревшее ПО и ПАК
4. Дефицит квалифицированного персонала
5. Беспечное отношение руководства
6. Несоответствие требованиям регуляторов

Только организационные и компенсирующие меры не эффективны

РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

ИБ должна быть обеспечена в соответствии с требованиями регуляторов, но:

- компенсирующие меры закрывают не более 30-40% требований
- не исключают основных угроз
- наиболее серьезные и дорогостоящие риски не компенсируются

Ответственность и последствия

Последствия отказа от комплексных мер влекут за собой масштабные кумулятивные риски и последствия:

- репутационные потери
- экономический ущерб
- риск техногенной катастрофы
- персональная ответственность

Подход Росатома: безопасность – высочайший приоритет

РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

«Безопасность как таковая, безопасность ядерная, экологическая безопасность в коде атомщиков — это и цель нашей деятельности, это и абсолютный приоритет»

Алексей Лихачев,
Генеральный директор ГК Росатом

- АО РАСУ – центр компетенций ИБ АСУ ТП
- Превентивный подход
- Системы обнаружения и мониторинга угроз
- Технические меры

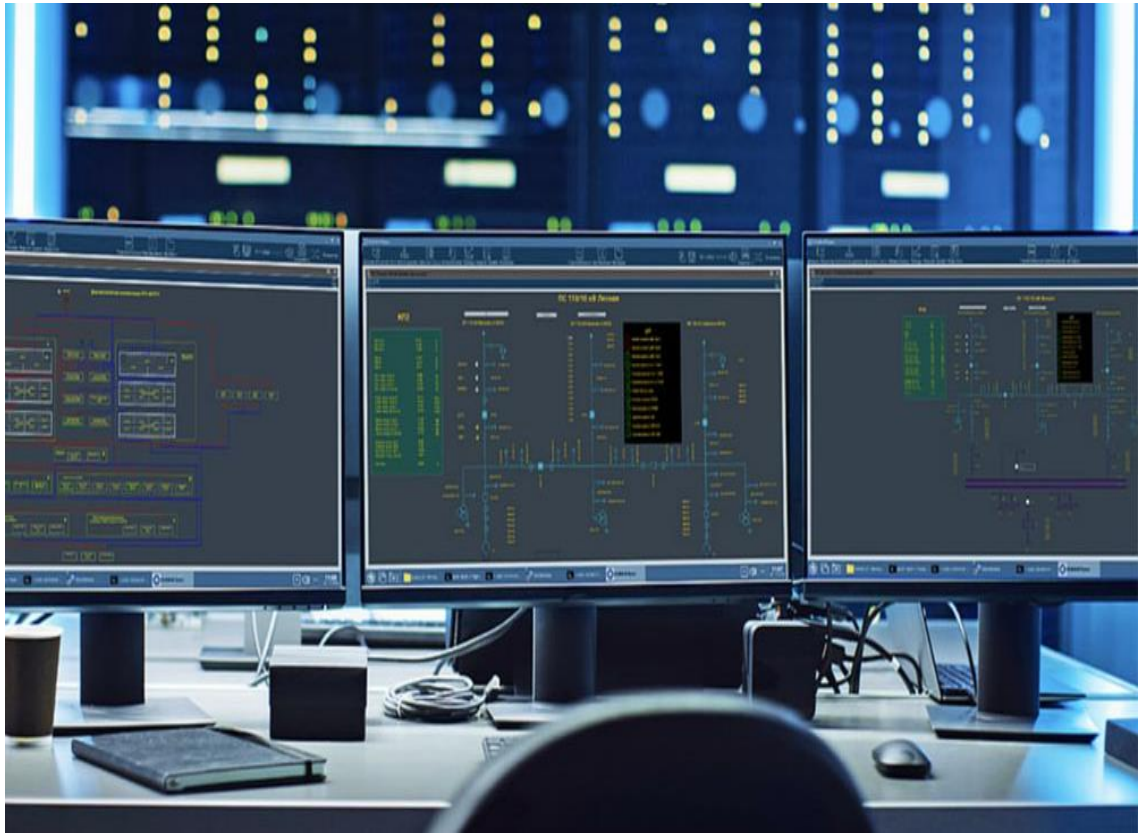
В основе политики Росатома лежат принципы ядерной безопасности – мы стремимся к исключению и предотвращению рисков

СОИБ РАСУ: функционал

РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Соответствует нормативным требованиям по обеспечению ИБ для объектов КИИ до 1-го класса защищенности

1. Выявление и предотвращение компьютерных атак на АСУ ТП
2. Автоматическое сопоставление событий ИБ для выявления компьютерных инцидентов
3. Сбор и хранение информации о событиях ИБ от сетевых устройств АСУ ТП
4. Передача информации о компьютерных инцидентах в отраслевой центр ГосСОПКА



СОИБ РАСУ: компоненты

РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Полноценные технические и организационные меры для обеспечения информационной безопасности АСУ ТП

- Система обнаружения вторжений
- Система управления событиями безопасности
- Систем контроля защищённости
- Средства анализа защищённости
- Средства антивирусной защиты, в том числе портативные
- Специализированные средства и системы для промышленности
- АРМ проверки носителей информации

РАСУ – центр компетенции ГК Росатом по ИБ АСУ ТП

РОСАТОМ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

АО «РАСУ» обладает необходимыми лицензиями и сертификатам и может работать с объектами КИИ до 1-ой категории значимости

- Проектирование систем обеспечения информационной безопасности АСУ ТП
- Разработка документации: ИТТ, модели угроз, ТЗ, ТП, РД, ЭД в части информационной безопасности
- Настройка оборудования АСУ ТП в соответствии с требованиями ИБ
- Проведение испытаний подсистем АСУ ТП на соответствие требованиям ИБ
- Тестирование СЗИ, ПО, ПАК на полигоне АО «РАСУ»
- Анализ уязвимостей в АСУ ТП и тестирование рисков проникновения
- Проведение аудитов поставщиков части реализации процессов безопасной разработки ППО
- Проверка ППО на соответствие требованиям ИБ (проведение статического, динамического тестирования, фаззинг-тестирования, тестирование рисков проникновения)

Безопасность – наивысший приоритет на всех предприятиях ГК Росатом!

115230, Москва, Каширское шоссе, 3, с2, ст16,
Бизнес Центр «Сириус Парк»

+7 495 933 43 40

info@rasu.ru