Тенденции развития угроз безопасности информации в АСУ ТП

Алексей Енютин, ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Темы

Статистика уязвимостей

Вендоры, типы ошибок, характеристики уязвимостей, уязвимости конфигурации и архитектуры

Развитие угроз

Инциденты, типовые сценарии, перспективные технологии, новые угрозы, последствия атак, перспективные средства защиты

Защита АСУ ТП

Перспективные меры защиты, первоочередные практические шаги

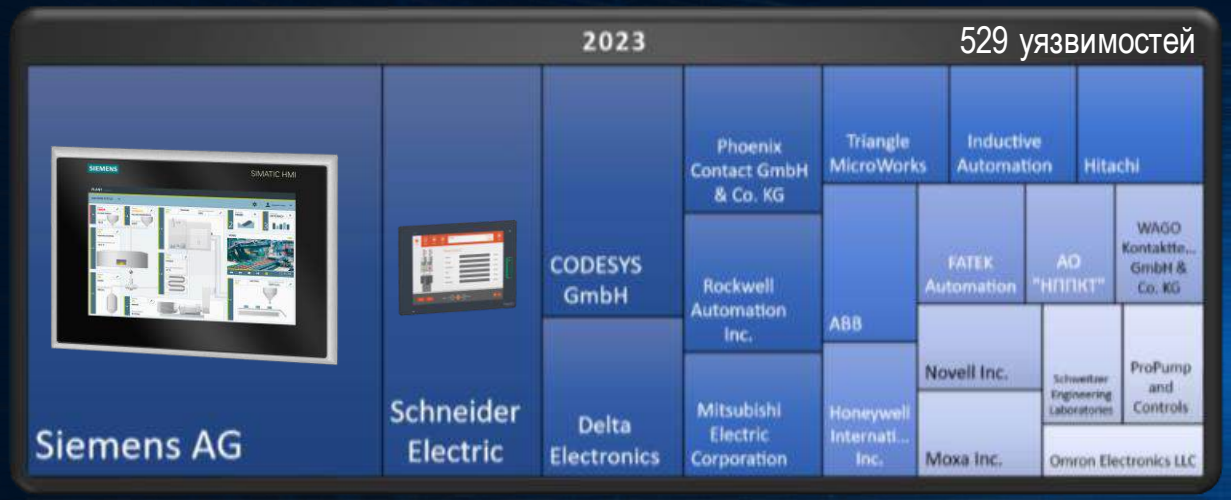
Статистика уязвимостей

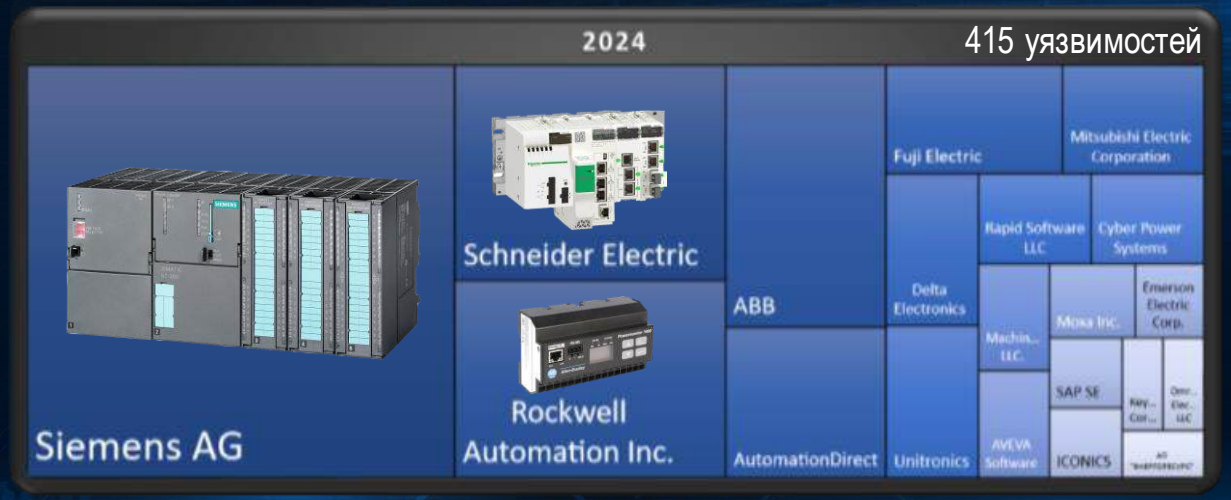
Вендоры

Уязвимости ПАС АСУ ТП

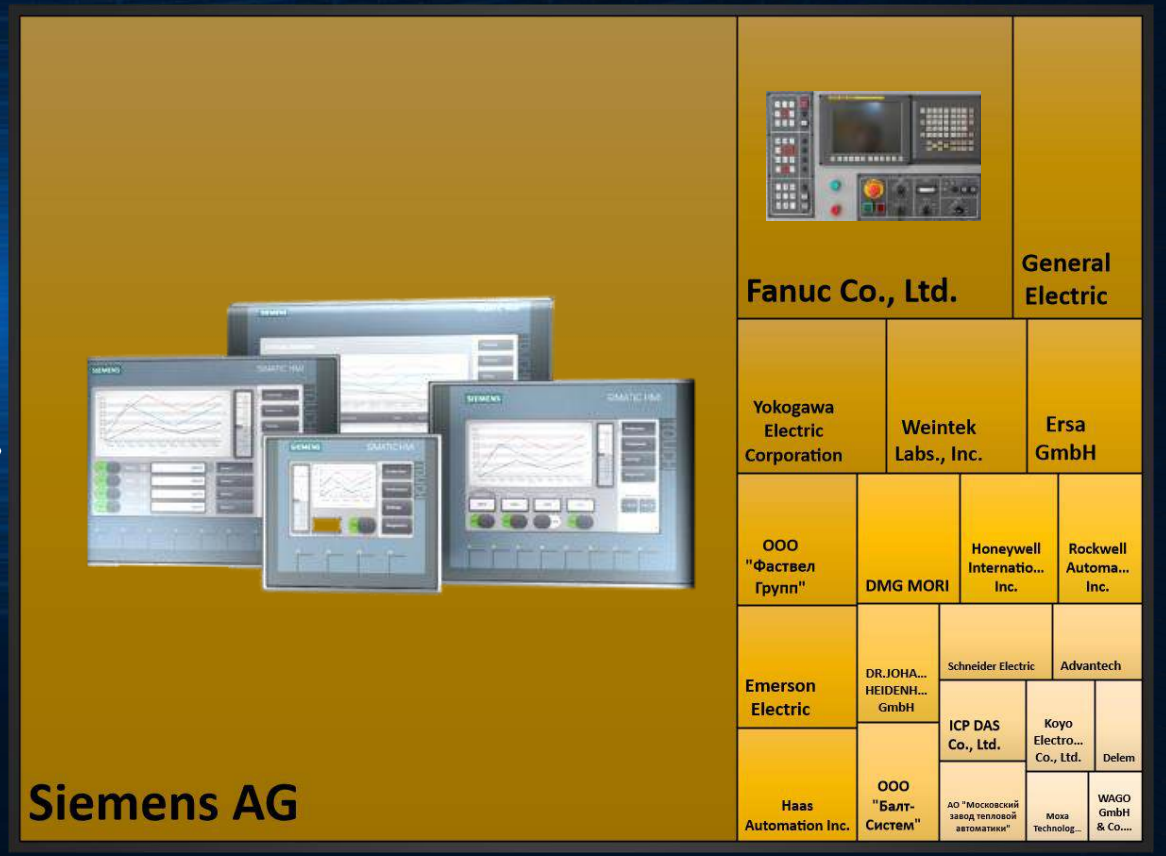
БДУ ФСТЭК России

БДУ АСУ ТП





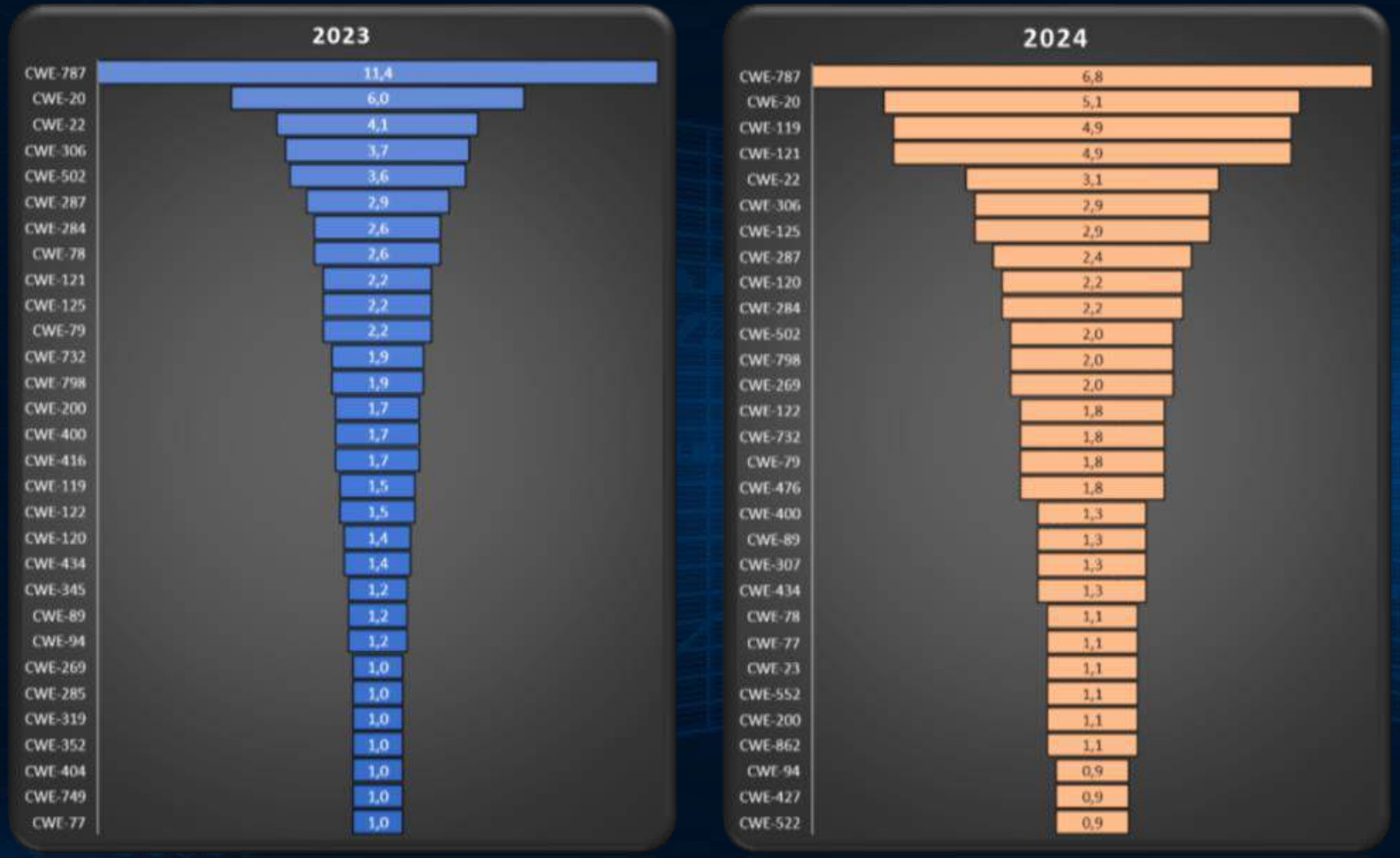
Соотношение вендоров на объектах КИИ



Статистика уязвимостей

Типы ошибок

Ошибки



Топ ошибок

- **Запись вне буфера (~ 9%)**
- **Некорректная проверка входных данных (~ 6%)**
- **Некорректные операции в пределах буфера памяти (~ 5%)**
- **Переполнение буфера на основе стека (~ 5%)**
- **Отсутствие аутентификации для критических функций (~ 4%)**
- **Некорректное ограничение пути к каталогу с ограниченным доступом (~ 4%)**

БДУ АСУ ТП → Бюллетени безопасности

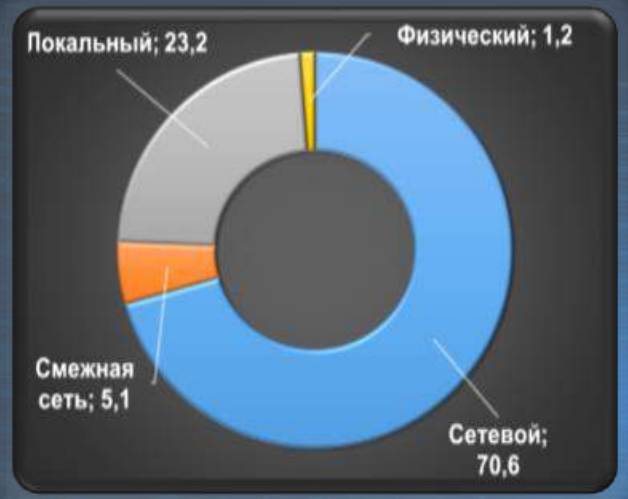
⚠ Более 30% уязвимостей

Статистика уязвимостей

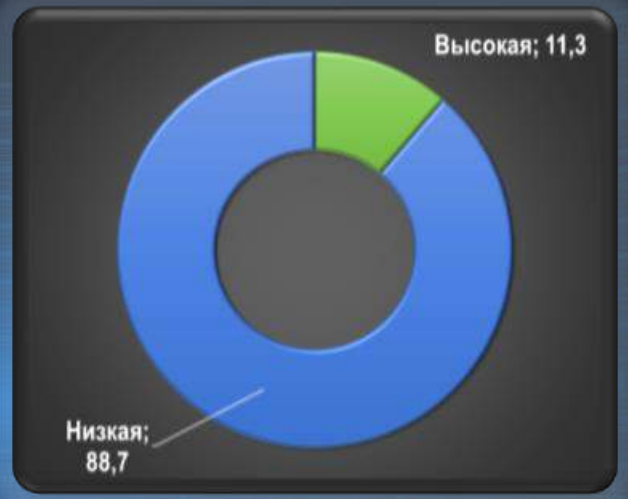
Характеристики уязвимостей АСУ ТП

3,4%	28,7%	47,4%	20,4%
Низкий уровень опасности	Средний уровень опасности	Высокий уровень опасности	Критический уровень опасности

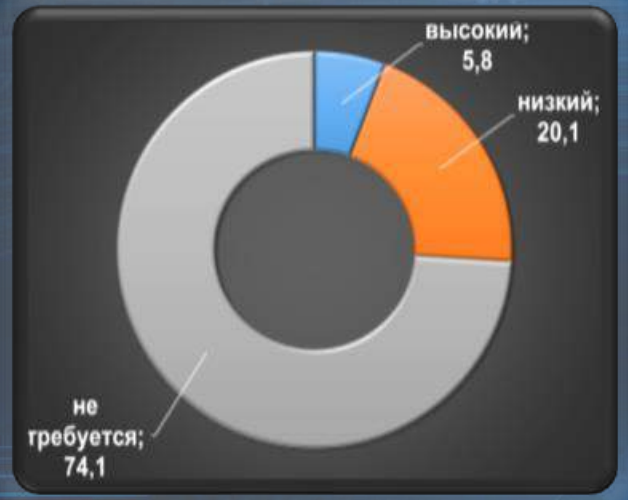
Вектор атаки



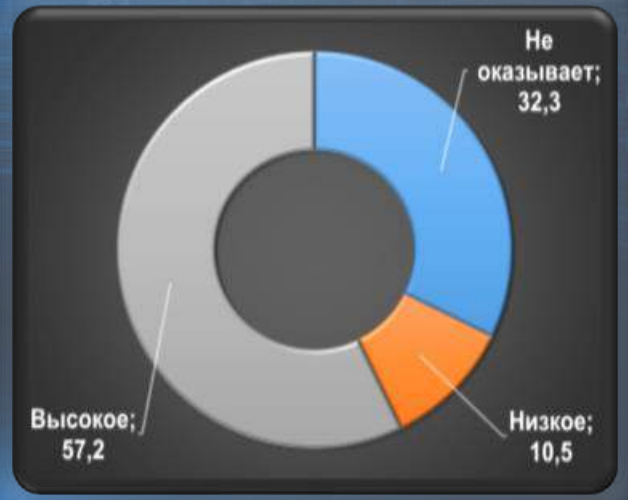
Сложность атаки



Уровень привилегий



Влияние на целостность



Статистика уязвимостей

Уязвимости конфигурации и архитектуры

БДУ
АСУ ТП

Основные уязвимости конфигурации

- Использование одной учетной записи для разных пользователей
- Использование нестойких к перебору паролей
- Использование паролей по умолчанию
- Открытые порты и сервисы
- Наделение пользователей избыточными полномочиями

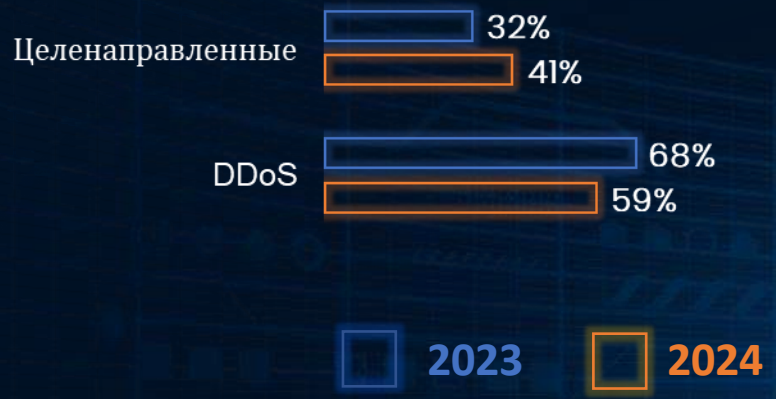
Основные уязвимости архитектуры

- Выход линий связи за пределы контролируемых зон
- Подключение компонентов АСУ ТП к Интернет
- Незащищенное (неучтенное) подключение АСУ ТП к корпоративной сети
- Открытые для доступа общие сетевые ресурсы

Развитие угроз

Инциденты

Виды атак



Виды объектов

Зафиксировано упоминаний об инцидентах: **389** (2023 год), **405** (2024 год)

Атакуемые отрасли

Развитие угроз

Типовые сценарии

Первоначальный доступ к корпоративной сети

- Социальная инженерия
- Фишинг
- Доступ через открытые сетевые ресурсы (корпоративные сайты)

Закрепление, повышение привилегий

- Эксплуатация уязвимостей
- Недостатки разграничения доступа
- Подбор аутентификационных данных
- Скомпрометированные учетные записи

Получение НСД к компоненту АСУ ТП

- Сканирование сети
- Изучение информации о системе
- Эксплуатация уязвимостей
- Использование недостатков разграничения доступа

Несанкционированные действия

- Модификация значений параметров блокировок
- Модификация прикладных программ управления
- Модификация уставок управления
- Отказ в обслуживании компонента

БДУ АСУ ТП

>70 типовых сценариев

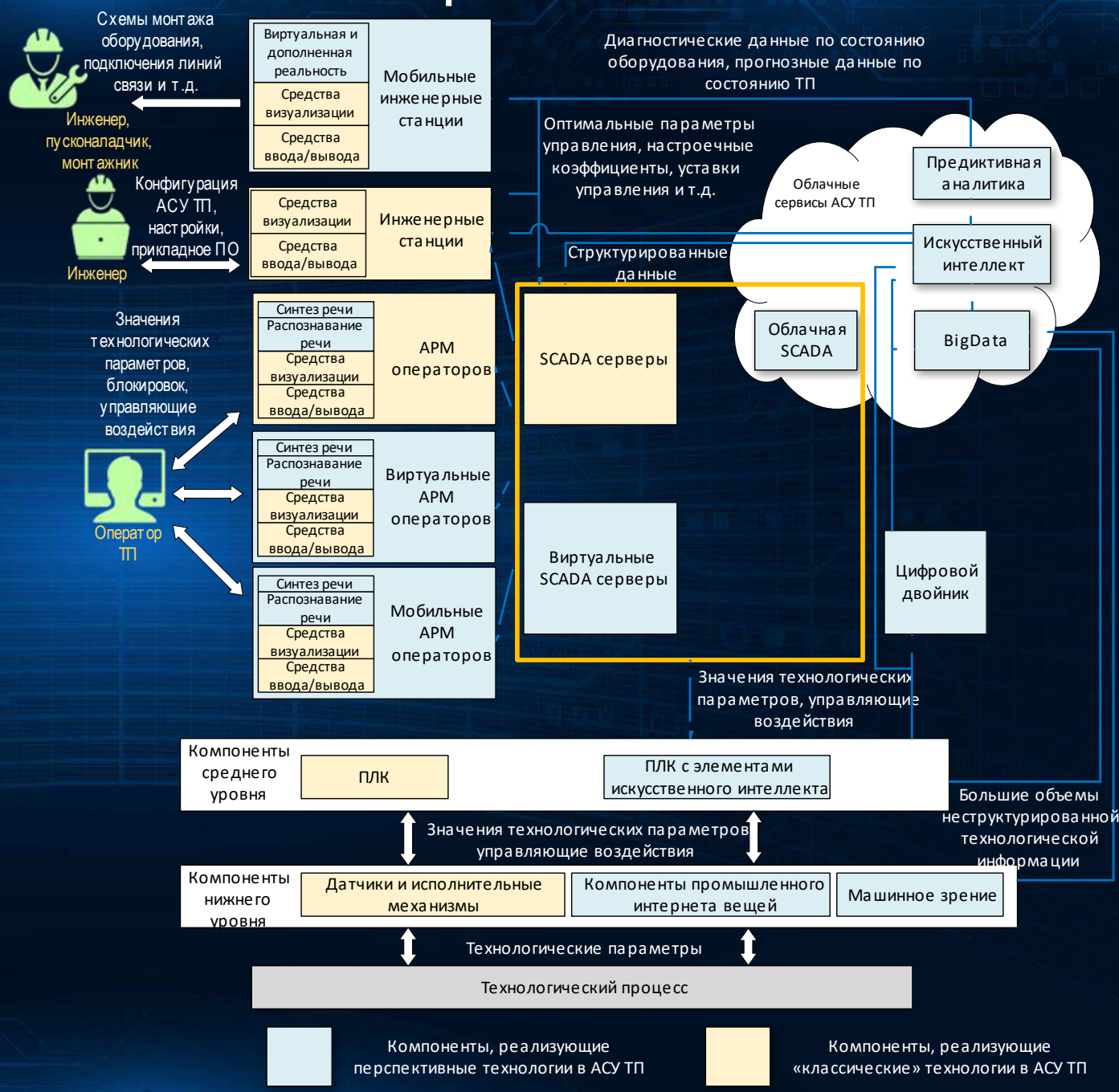
Развитие угроз

Перспективные технологии в АСУ ТП

- Виртуализация
- Облачные вычисления
- IIoT
- Цифровые двойники
- Виртуальная и дополненная реальность
- Предиктивная аналитика
- Большие данные
- Искусственный интеллект

НОВЫЕ УГРОЗЫ

Перспективная АСУ ТП



Развитие угроз

Новые угрозы перспективным технологиям

Новые угрозы	Недопустимые события
Атаки на модели машинного обучения	Некорректные прогнозы работы оборудования и хода ТП
Вредоносное ПО на нижнем уровне АСУ ТП (ИМ и ПЛК)	Некорректные измерения и управляющие воздействия
Атаки на виртуальную инфраструктуру	Нарушение функционирования одновременно всех компонентов АСУ ТП
Подмена моделей цифровых двойников	Неверные управляющие решения СУУ ТП. Некорректные прогнозы
Атаки на облачные SCADA	Отказ в обслуживании системы диспетчерского контроля. Подмена управляющих воздействий

Развитие угроз

Негативные последствия атак

Время наступления ущерба

Компьютерная атака

Информационная система

- Прекращение выполнения функций — **мгновенно**
- Потеря данных (шифрование) — **5 мин – 1 час** (для средних шифровальщиков)
- Хищение данных — **1 мин – 1 час** (для больших баз данных)

АСУ ТП

- Останов ТП — **До 5 мин** (для сложных технологических линий)
- Снижение качества/количества продукции — **До 5 мин** (для медленных переходных процессов)
- Авария — **До нескольких дней**

БДУ АСУ ТП

>300 Негативных последствий

Развитие угроз

Негативные последствия атак

Модификация

АСУ ТП

Алгоритмы управления

Параметры регуляторов

Нарушение устойчивости АСУ*

Отложенный ущерб

Авария развивается в условиях, когда атака уже завершена и ликвидированы следы взлома

*** УСТОЙЧИВОСТЬ является критически важным фактором для обеспечения безопасности объектов управления**

Меры предотвращения

- **Создание адаптивных систем поддержки принятия решений**
- **Внедрение многокритериального анализа состояния системы**
- **Регулярный мониторинг и контроль параметров**
- **Оперативное реагирование на отклонения**

Защита АСУ ТП

Перспективные средства защиты

Существующие системы

Система ПАЗ

- Реагирование на фактическое начало развития аварии
- Реагирование приводит к останову ТП

SIEM

- Обнаружение сетевых аномалий, отклонений от нормального поведения систем верхнего уровня
- Аномалии могут не быть причиной аварий

Перспективные средства

Цифровые двойники

- Прогнозирование сценариев развития аварийных ситуаций
- Обучение ИИ сочетаниям потенциально опасных комбинаций входных воздействий

Перспективная система ПАЗ

- Сигнализация о нарушении устойчивости
- Сигнализация о потенциальном развитии аварии

Перспективная SIEM АСУ ТП

- Обнаружение аномалий в алгоритмах управления
- Обнаружение аномалий команд управления

Защита АСУ ТП

Меры защиты

Первоочередные практические шаги

Аудит структуры АСУ ТП

- Определение ВСЕХ компонентов (ПО и ПАС) и их взаимосвязей
- Определение ВСЕХ подключений к внешним системам
- Определение ВСЕХ точек ввода/вывода информации (от персонала, через съемные носители, удаленно)
- Выявление беспроводных точек подключения

Анализ угроз и уязвимостей

- Определение уязвимостей и их устранение (обновления, компенсирующие меры)
- Актуализация перечня угроз и анализ достаточности мер по их блокированию

Защита периметра АСУ ТП

- Межсетевые экраны на периметре
- По возможности однонаправленная передача данных из АСУ ТП
- Защита физического доступа к линиям и устройствам, расположенным за пределами КЗ
- Управление съемными носителями информации

Защита доступа к компонентам АСУ ТП

- Управление физическим доступом
- Наделение пользователей минимальными необходимыми полномочиями
- Управление паролями и учетными записями
- Ограничение удаленного доступа

БДУ АСУ ТП

Рекомендации по мерам защиты АСУ ТП и перспективных технологий

«Методика оценки показателя состояния ТЗИ и обеспечения безопасности значимых объектов КИИ Российской Федерации» (утверждена ФСТЭК России 2 мая 2024 г.)

Организационные меры и документы

- ОРД по ИБ
- Правила и процедуры защиты и действий при возникновении инцидентов
- Инструкции персонала по ИБ

Спасибо за внимание !