УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ

КРИТИЧНОСТЬ АСУ ТП
Подходы к обоснованию

Татьяна Пермякова

Старший аналитик

Направления аудитов
и соответствия требованиям ИБ

USSC.RU

ТАРГЕТИРОВАННЫЕ АТАКИ

Space Pirates

Группировка действует как минимум с 2017 года.
В 2022 году атаковали по меньшей мере 5 организаций в России и еще несколько в других странах

Цель злоумышленников: госучреждения, авиационно-космическая и электроэнергетическая отрасль

APT41

За 2021 год группировка смогла получить доступ как минимум в 13 организаций по всему миру. Атакующие заинтересованы в кибершпионаже и финансовой выгоде

Цель злоумышленников: государственный сектор, промышленное производство, авиация и прочие отрасли

TA428

Китайскоязычная кибергруппировка совершает атаки, используя заранее подготовленные фишинговые письма. В ряде случаев атакующим удалось полностью захватить ИТ-инфраструктуру жертв

Цель злоумышленников: российские и зарубежные оборонные предприятия и госорганы

МАСШТАБЫ ВОЗМОЖНЫХ ПОТЕРЬ

Один из крупнейших мировых производителей авиационной техники стал жертвой вымогательского ПО и вынужден был **остановить работы заводов в 4 странах на неделю**.

Сумма убытков составила около
40 млн.$

Из-за успешной атаки на производителя деталей автомобилей деятельность компании была приостановлена. Вследствие чего произошел **останов производства** автомобилей на всех японских заводах ведущего автопроизводителя.

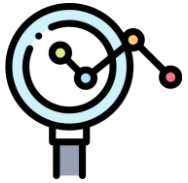
Другая кибератака на производителя привела к **потере секретной информации** и ущербу **более 37 млн.$**

АВТОМАТИЗАЦИЯ ПРОИЗВОДСТВА

МЕТОД ДОСТИЖЕНИЯ СТРАТЕГИЧЕСКИХ ЦЕЛЕЙ

Повышение объемов выпуска продукции

Снижение затрат на производство



Обеспечение качества продукции

Снижение бизнес-рисков, обусловленных человеческим фактором

ПОДХОДЫ К ОБОСНОВАНИЮ КРИТИЧНОСТИ

Законодательный

Анализ
производственного процесса

ПОДХОДЫ К ОБОСНОВАНИЮ КРИТИЧНОСТИ

Законодательный

Анализ
производственного процесса

ЗАКОНОДАТЕЛЬСТВО РФ

По аналогии с категорированием объектов КИИ

- Единый подход на всем предприятии
- Большая практика применения
- Ведущий каталог мер ИБ в РФ

Приказ ФСТЭК России №239

- Оценивается ущерб для государства
- Требует адаптации для бизнес-целей
- Может вызвать вопросы у ФСТЭК России

Постановление Правительства Российской Федерации от 08.02.2018 №127
«Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации,
а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

ЗАКОНОДАТЕЛЬСТВО РФ

Классификация АСУ ТП по Приказу ФСТЭК России №31

- ✓ Не противоречит КИИ
- ✓ Большая практика применения
- ✓ Широкий каталог мер ИБ
- ✗ Сложно обосновать бизнесу
- ✗ Отсутствуют четкие метрики классификации

ПОДХОДЫ К ОБОСНОВАНИЮ КРИТИЧНОСТИ

Законодательный

Анализ
производственного процесса

АНАЛИЗ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА

ЦЕЛЕВОЕ НАЗНАЧЕНИЕ

Основные	Вспомогательные	Обслуживающие	Контролирующие	Измерительные
превращения сырья и материалов в готовую продукцию, являющуюся основной, профильной продукцией для предприятия	направлены на изготовление продукции или выполнение услуг для обеспечения нормального протекания основных производственных процессов	обеспечивают создание нормальных условий для протекания основных и вспомогательных производственных процессов	процессы, задачей которых является постоянный или периодический контроль за безопасностью протекания прочих процессов, состоянием оборудования, качеством готовой продукции	процессы, задачей которых является учет ресурсов и готовой продукции

АНАЛИЗ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА

КРИТИЧНОСТЬ ПО ЦЕЛЕВОМУ НАЗНАЧЕНИЮ

Основные	Вспомогательные	Обслуживающие	Контролирующие	Измерительные
Высокая степень – прямое влияние на основной процесс и выпуск готовой продукции	**Низкая степень** – не оказывает влияния	Равна степени критичности обслуживаемого процесса	Равна степени влияния на основной процесс и условия, при которых оказывается влияние	**Средняя степень** – может снижать общую эффективность процессов при искажении измеряемых данных

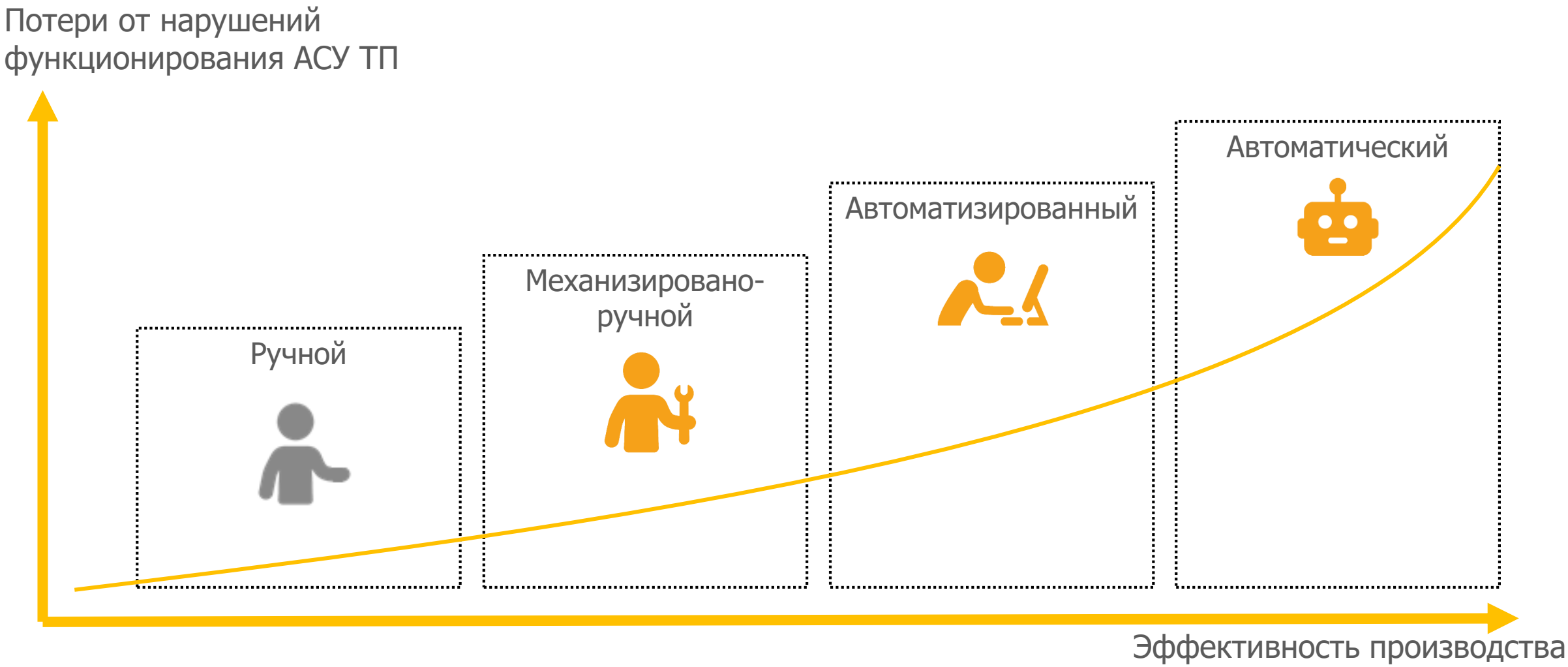
АНАЛИЗ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА

УРОВЕНЬ АВТОМАТИЗАЦИИ

- **Ручной** – реализуется за счет энергии человека
- **Механизировано-ручной** – применение энергии человека и машины
- **Автоматизированный** – участие человека и средств автоматизации
- **Автоматический** – без участия человека

АНАЛИЗ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА

УРОВЕНЬ АВТОМАТИЗАЦИИ



АНАЛИЗ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА

КРИТИЧНОСТЬ АСУ ТП

		Ручной	Уровень автоматизации		
			Механизировано-ручной	Автоматизированный	Автоматический
Критичность процесса	Низкая	-	Низкая	Низкая	Средняя
	Средняя	-	Низкая	Средняя	Высокая
	Высокая	-	Средняя	Высокая	Высокая

ЧТО ДАЛЬШЕ?

Критичность АСУ ТП

+

Моделирование угроз ИБ

Оценка рисков ИБ

Обработка рисков ИБ

Мониторинг

Уральский центр систем безопасности

- Аудит ИБ АСУ ТП
- Оценка рисков и моделирование угроз ИБ
- Разработка ОРД
  (стратегия, стандарты, регламенты, инструкции)
- Корпоративный центр ГосСОПКА
- Внедрение комплекса мониторинга
  и анализа состояния ИБ АСУ ТП CyberLympha DATAPK
- Проектирование и внедрение систем защиты

USSC.RU

Телефон
+7 (343) 379-98-34

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Татьяна Пермякова

Старший аналитик

Направления аудитов
и соответствия требованиям ИБ

tpermyakova@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU