udv|group

Обзор рынка защиты АСУ ТП

как заказчики реагируют на ИБ-угрозы

АЛЕКСЕЙ ШАНИН
Директор по продуктам
UDV Group

https://ru.wikipedia.org/wiki/Туман_войны

udv|group

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

БОЛЕЕ 10 ЛЕТ ЭКСПЕРТИЗЫ ИБ АСУ ТП

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

СОБСТВЕННЫЙ R&D И ЛАБОРАТОРИЯ КИБЕРБЕЗОПАСНОСТИ

ДЕЛОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРЫ

5 важнейших элементов управления кибербезопасностью АСУ ТП

Реагирование на инциденты, специфичные для АСУ ТП

Безопасный удаленный доступ

Сетевая архитектура защищенной системы управления

Видимость и мониторинг сети

Управление уязвимостями на основе рисков

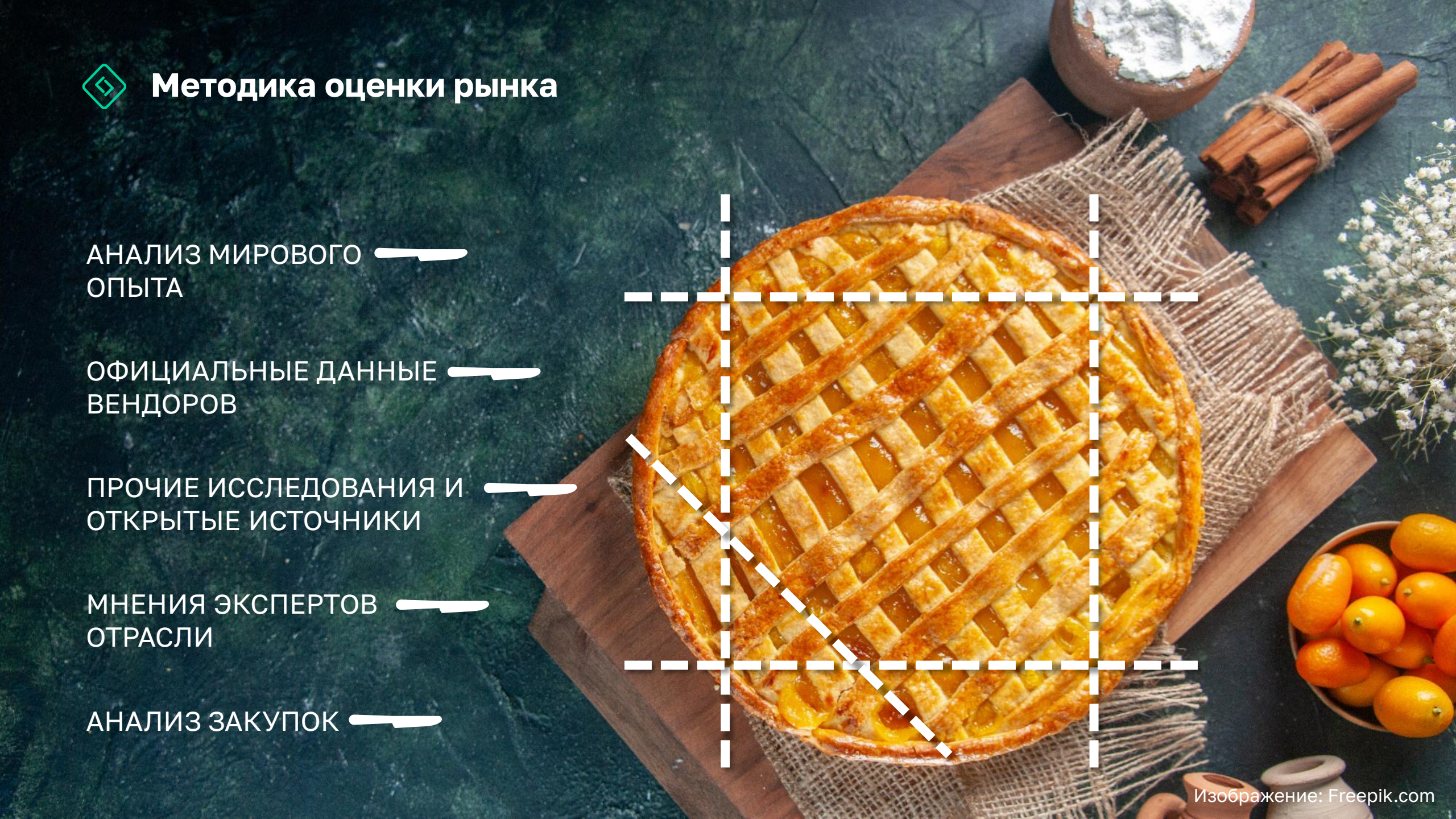
Источник: опрос «SANS ICS/OT Cybersecurity Survey: 2023’s Challenges and Tomorrow’s Defenses» в области кибербезопасности АСУ ТП (сентябрь 2023 г.). Данные на основе более 700 ответов.

Некоторые классы решений

КЛАСС РЕШЕНИЯ	НАЛИЧИЕ СПЕЦИФИЧНЫХ ДЛЯ АСУ ТП РЕШЕНИЙ
ПРОМЫШЛЕННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ	●
ШЛЮЗЫ ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ	●
СОВ В ПРОМЫШЛЕННОМ ИСПОЛНЕНИИ	●
ЗАЩИТА КОНЕЧНЫХ ТОЧЕК	●
ПРИМАНКИ И ЛОВУШКИ (DECEPTION)	● / ○
КОНТРОЛЬ КОНФИГУРАЦИЙ	● / ○
УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ	● / ○
МОНИТОРИНГ ФУНКЦИОНИРОВАНИЯ (ДОСТУПНОСТЬ, ПРОИЗВОДИТЕЛЬНОСТЬ)	● / ○
КОНТРОЛЬ ВЕРСИЙ ПРОЕКТОВ ПЛК	●
SIEM	● / ○
ПЛАТФОРМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ О КИБЕРУГРОЗАХ	● / ○
IRP/SOAR	● / ○
EDR/XDR	● / ○
SGRC	● / ○

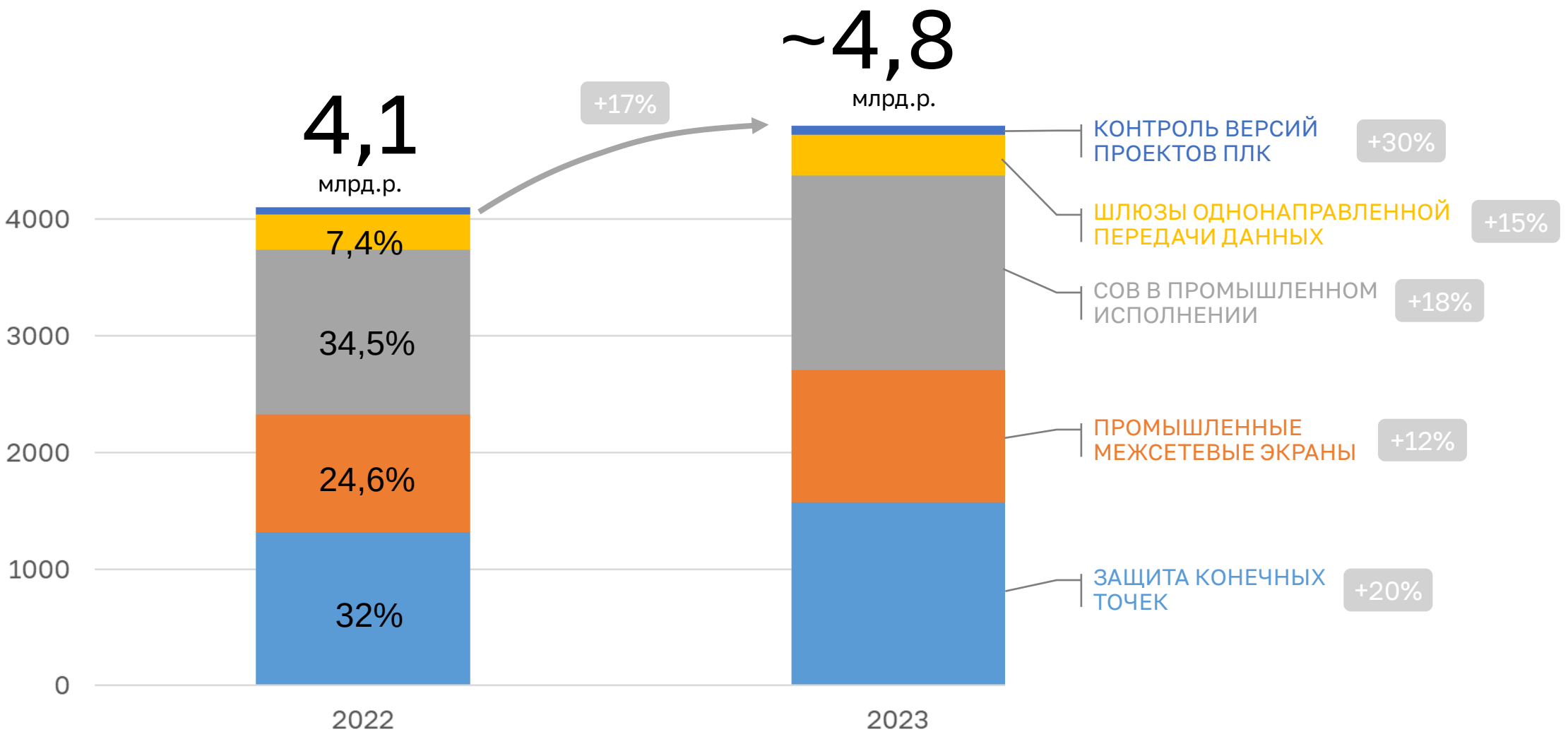
Методика оценки рынка

- АНАЛИЗ МИРОВОГО ОПЫТА
- ОФИЦИАЛЬНЫЕ ДАННЫЕ ВЕНДОРОВ
- ПРОЧИЕ ИССЛЕДОВАНИЯ И ОТКРЫТЫЕ ИСТОЧНИКИ
- МНЕНИЯ ЭКСПЕРТОВ ОТРАСЛИ
- АНАЛИЗ ЗАКУПОК

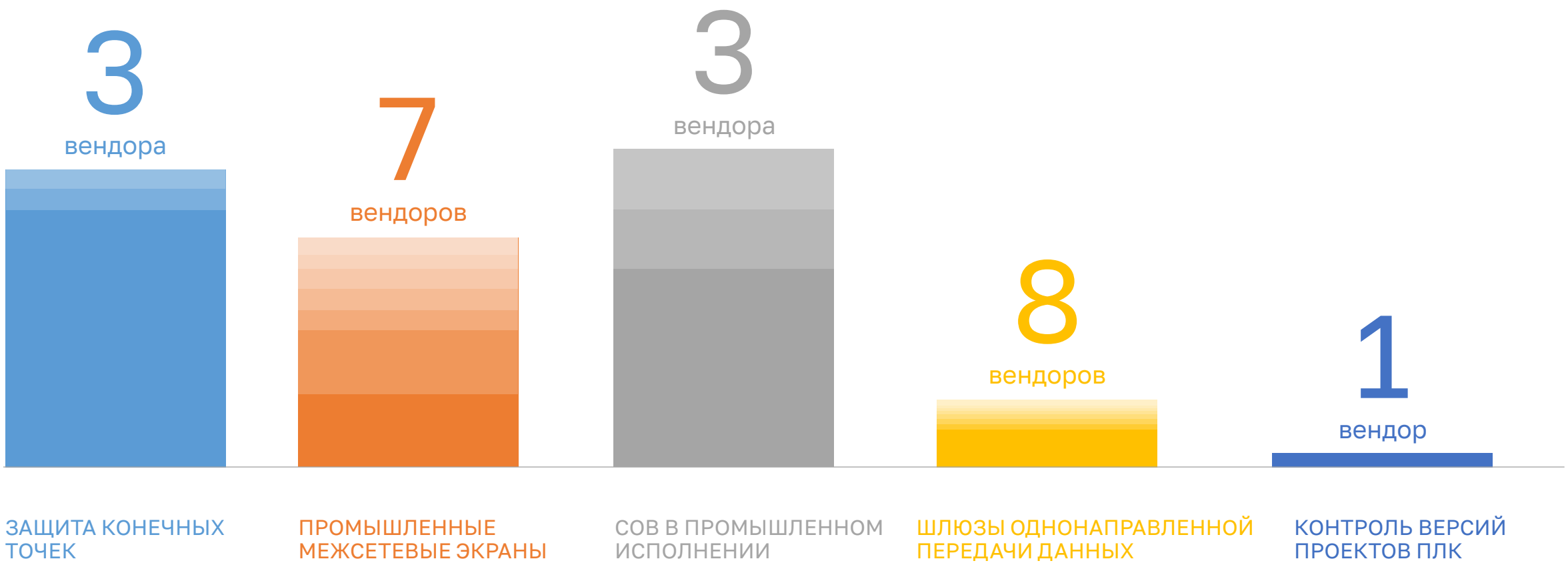


Изображение: Freepik.com

Ёмкость рынка обеспечения ИБ АСУ ТП в 2022-2023 г.г.



Количество решений для обеспечения ИБ АСУ ТП в 2023 году



Экосистемный подход от одного вендора

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК	ПРОМЫШЛЕННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ	СОВ В ПРОМЫШЛЕННОМ ИСПОЛНЕНИИ	ШЛЮЗЫ ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ	КОНТРОЛЬ ВЕРСИЙ ПРОЕКТОВ ПЛК
✗	✓	✓	✓	✓
✗	✗	✓	✗	✗
✓	✗	✓	✗	✗

Степень проникновения решений (усреднение)

КЛАСС РЕШЕНИЯ	До 2022	В 2022	2023+
ПРОМЫШЛЕННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ			
ШЛЮЗЫ ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ			
СОВ В ПРОМЫШЛЕННОМ ИСПОЛНЕНИИ			
ЗАЩИТА КОНЕЧНЫХ ТОЧЕК			
ПРИМАНКИ И ЛОВУШКИ (DECEPTION)			
КОНТРОЛЬ КОНФИГУРАЦИЙ			
УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ			
МОНИТОРИНГ ФУНКЦИОНИРОВАНИЯ (ДОСТУПНОСТЬ, ПРОИЗВОДИТЕЛЬНОСТЬ)			
КОНТРОЛЬ ВЕРСИЙ ПРОЕКТОВ ПЛК			
SIEM			
ПЛАТФОРМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ О КИБЕРУГРОЗАХ			
IRP/SOAR			
EDR/XDR			
SGRC			

Количество голосов респондентов: много средне мало

udv|group

Выводы по итогам общения с заказчиками

- От предприятия к предприятию ситуация сильно меняется
- Топ 3 наиболее часто применяемых классов решений: защита конечных точек, промышленные СОВ, управление уязвимостями
- Значимость неинвазивности снижается
- В подавляющем количестве предприятий процесс реагирования на инциденты ИБ задокументирован
- Службы ИБ и эксплуатации совместно решают задачи по обеспечению ИБ АСУ ТП

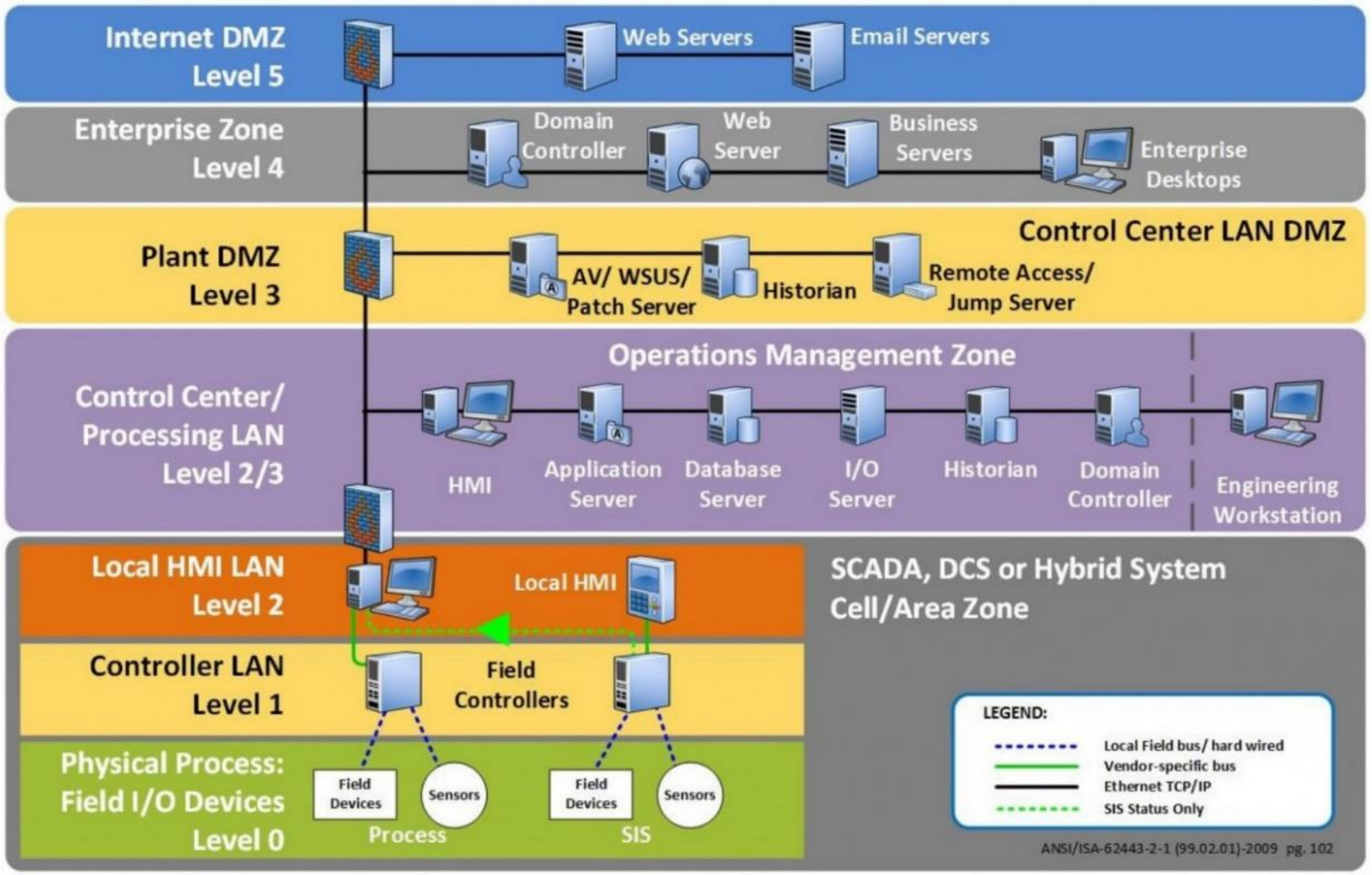
Облачные сервисы в АСУ ТП

Источник: опрос «SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses» в области кибербезопасности АСУ ТП (сентябрь 2023 г.). Данные на основе более 700 ответов.

Наиболее важные инициативы по повышению безопасности АСУ ТП в ближайшие 18 месяцев

Источник: опрос «SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses» в области кибербезопасности АСУ ТП (сентябрь 2023 г.). Данные на основе более 700 ответов.

The Purdue Model for Industrial Control Systems (ISA/IEC 62443)



УРОВЕНЬ 5:
ПОДКЛЮЧЕНИЕ ВНЕШНИХ СЕТЕЙ

УРОВЕНЬ 4:
УПРАВЛЕНИЕ ПРЕДПРИЯТИЕМ

УРОВЕНЬ DMZ:
БАРЬЕР МЕЖДУ IT & OT

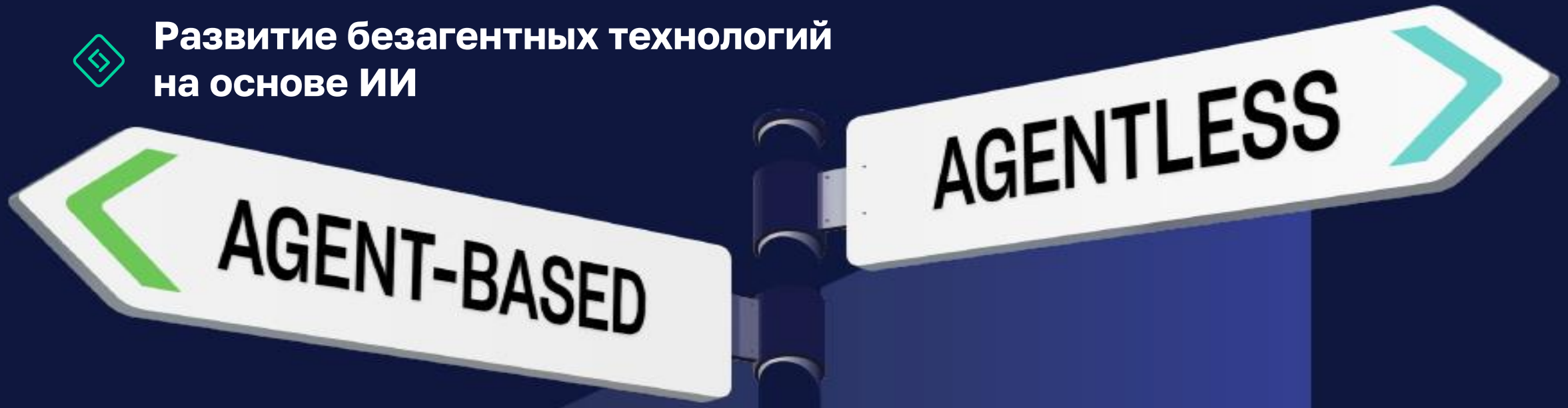
УРОВЕНЬ 3:
УПРАВЛЕНИЕ ПРОИЗВОДСТВОМ

УРОВЕНЬ 2:
КОНТРОЛЬ ОБЩИХ ПРОЦЕССОВ

УРОВЕНЬ 1:
ЛОКАЛЬНЫЕ КОНТРОЛЛЕРЫ

УРОВЕНЬ 0:
ФИЗИЧЕСКИЕ КОМПОНЕНТЫ

Развитие безагентных технологий на основе ИИ



- Подходят для сетей с ограниченной пропускной способностью
- Подходят для часто отключённых от сети хостов
- Требуют развертывания и обслуживания
- Клиентские части работают по технологии запросов/задач

- Зависимы от сетевых подключений
- Не требуют развертывания
- Применяются в случаях невозможности установить агентов на хосты

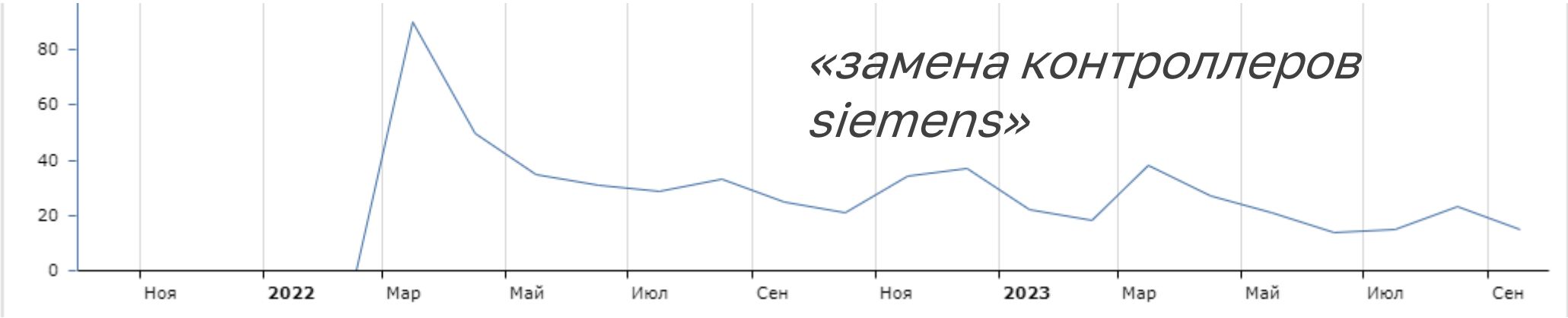
Zero Trust Architecture (ZTA) применительно к АСУ ТП

1. Невозможность поддержки ZTA на полевом уровне и уровне ПЛК → применение на уровнях модели Purdue 3, 4, 5, OT DMZ
2. ZTA влияет на задержку ответа на запросы ресурсов → ограниченное применение подходов ZTA
3. Использовании общих учётных данных → дополнительная идентификация лиц

NIST SP 800-82r3 Guide to Operational Technology (OT) Security, сентябрь 2023 г.

Импортозамещение

«контроллеры прософт»



«замена контроллеров siemens»

udv|group

СПАСИБО ЗА ВНИМАНИЕ!

Закажите пилотный проект или персональную демонстрацию наших решений

commercial@udv.group

udv.group