ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

КОНВЕРГЕНТНАЯ ЭВОЛЮЦИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ

РАЗВИТИЕ ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ ПРИМЕНИТЕЛЬНО К НОВЫМ ОБЪЕКТАМ, НОВЫМ ТЕХНОЛОГИЯМ И УГРОЗАМ

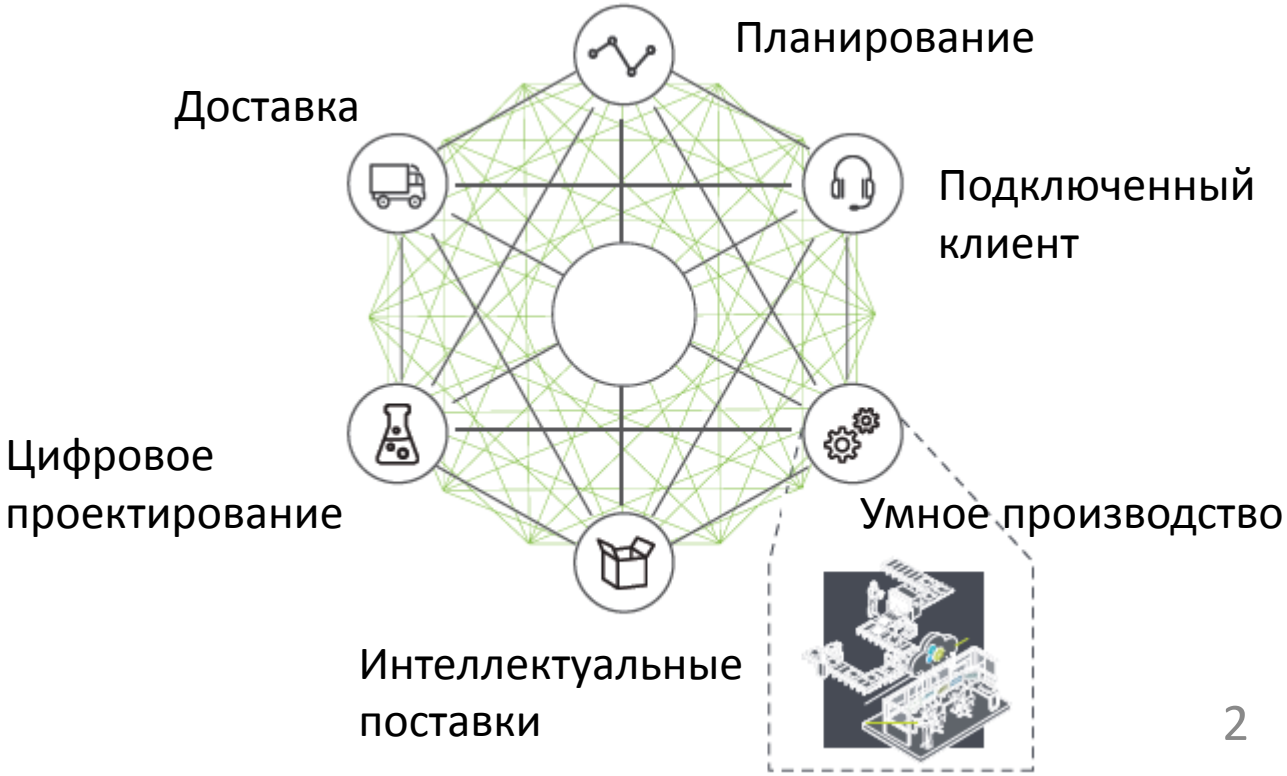
Д.Т.Н., ПРОФЕССОР КАФЕДРЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ» СПбПУ
ЗАСЛУЖЕННЫЙ ДЕЯТЕЛЬ НАУКИ РФ
П.Д. ЗЕГЖДА

Санкт-Петербург
2018

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

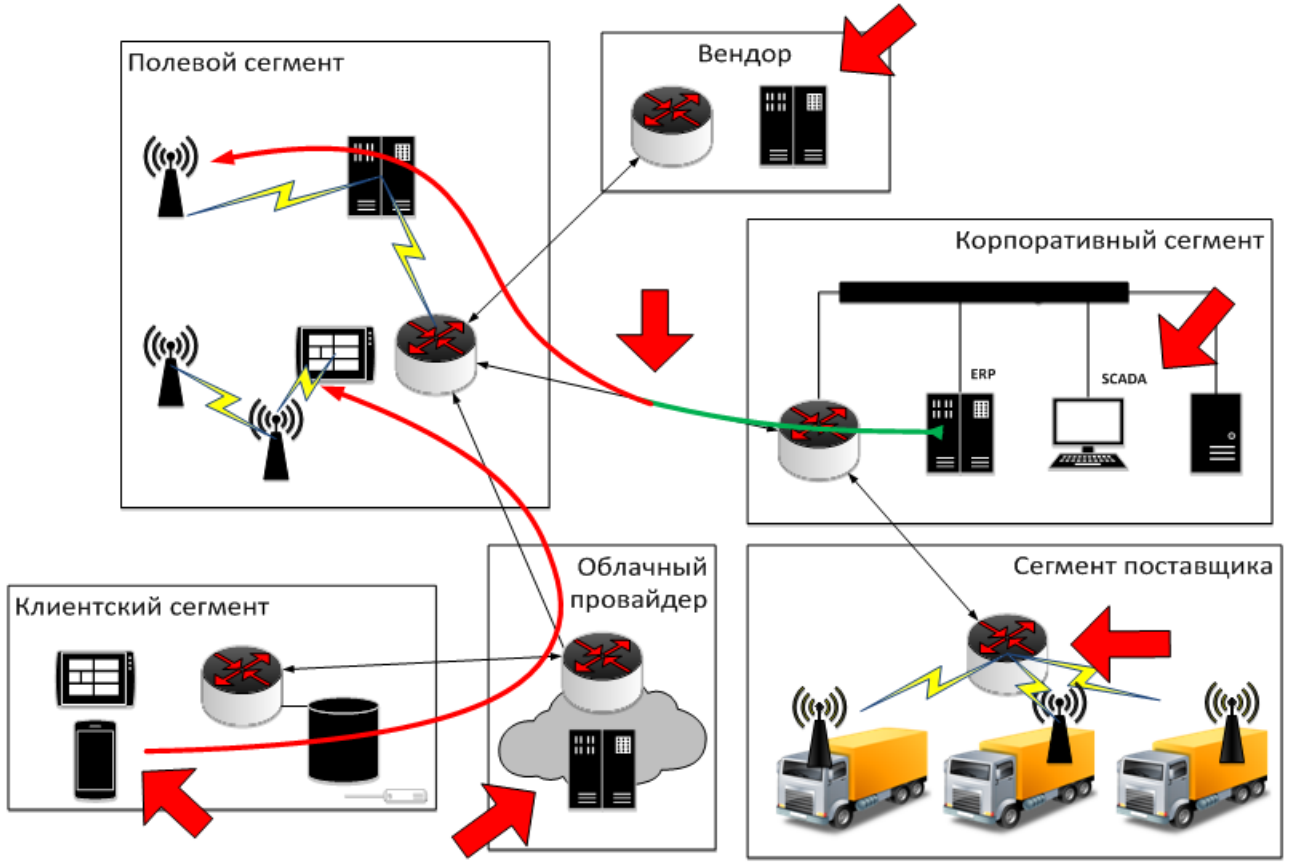
Эпоха цифрового производства

Цифровое производство – интегрированная киберфизическая система, обеспечивающая полный цикл проектирования и выпуска продукции, включающая как средства численного моделирования, визуализации, инженерного анализа, разработки конструкции изделий, так и автоматизированные технологические процессы их изготовления



ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

Новые возможности нарушителя безопасности



БЕЗОПАСНОСТЬ ИЛИ ВЫСОКИЙ УРОВЕНЬ ЦИФРОВИЗАЦИИ ПРОИЗВОДСТВА

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Безопасность VS цифровизация

Цифровые технологии, получившие возможность модифицировать (создавать) сами себя не ставят целью обеспечить безопасность, т.к. безопасность – всегда ограничения функциональности и разнообразия возможностей.

Комфортно ли человеку в рациональном и **небезопасном** мире?

ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

СПЕЦИФИКА ЗАЩИТЫ КФС И КОНВЕРГЕНЦИЯ ЗАДАЧ БЕЗОПАСНОСТИ В ХОДЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Что обеспечит безопасность цифрового производства

АДАПТИРОВАТЬ ТРАДИЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ ИЛИ РАЗРАБОТАТЬ НОВЫЕ, СПЕЦИФИЧНЫЕ ДЛЯ ЦП?

- Криптографические средства защиты сети (VPN, TLS)
- Антивирусные средства
- Средства межсетевого экранирования
- Системы обнаружения/предотвращения атак
- Системы обнаружения аномалий

Недостатки:

- *Традиционные средства защиты легко адаптировать для работы на «верхних» уровнях сети ЦП. Насколько эффективно их применение в технологическом сегменте?*
- *Невозможность применения апостериорных средств защиты информации ввиду необратимости производственных процессов*

- Использование «цифровых двойников» для тестирования безопасности?
- Еще идеи…

Недостатки:

- *Как построить модель атак на цифровое производство, если множество атак развивается хаотично и непредсказуемо?*

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Кто обеспечит безопасность цифрового производства

- Приказ ФСТЭК России от 14.03.2014 №31 «Об утверждении Требований к обеспечению защиты информации **в автоматизированных системах управления производственными и технологическими процессами** …»
- Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации» ставит целью **обеспечение устойчивого функционирования в условиях реализации угроз безопасности информации.**

Нужны ли новые нормативные документы, определяющие требования к обеспечению защиты **цифровых производств?**

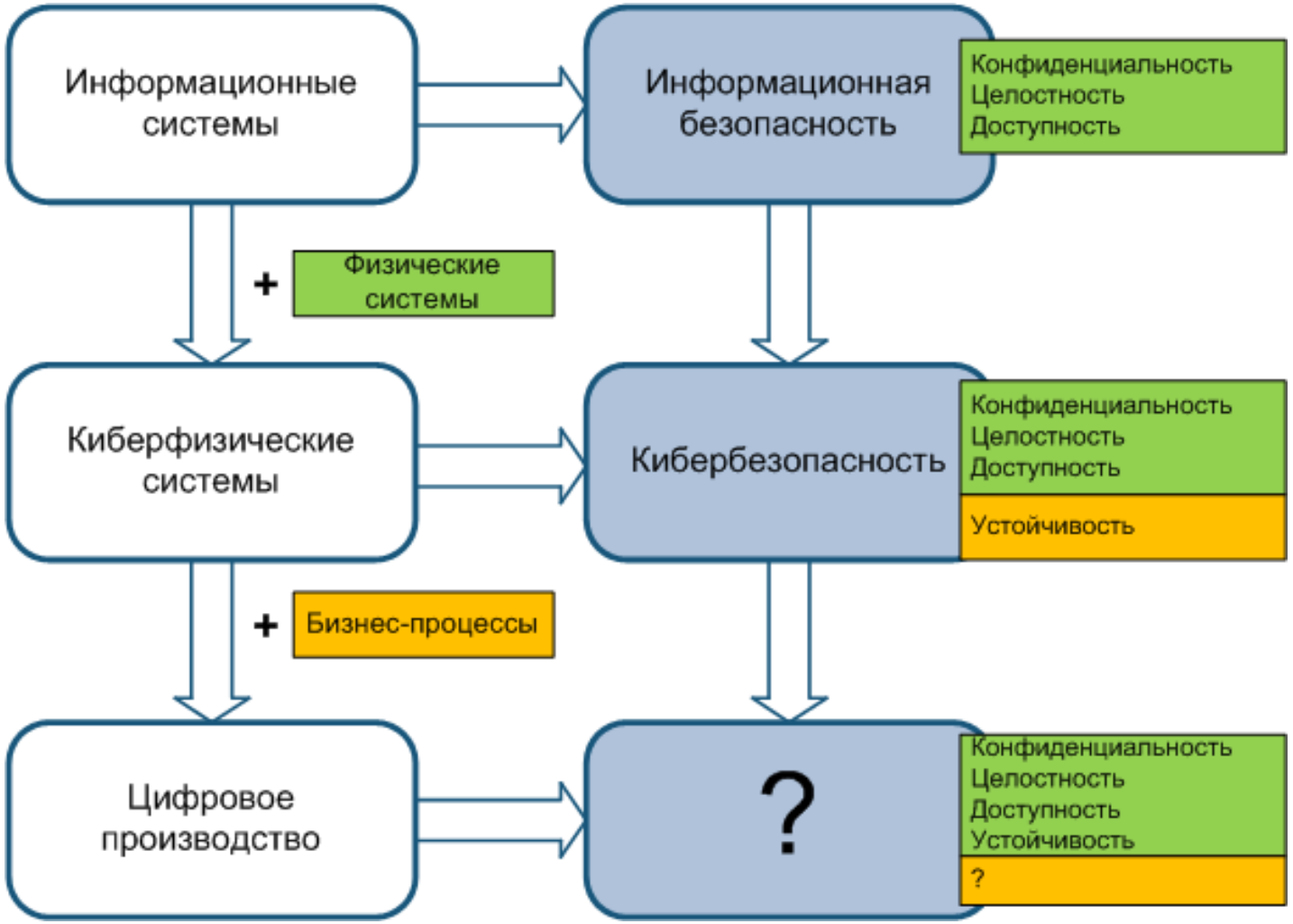
ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Проблемы обеспечения безопасности КФС

- **Традиционные подходы не решают главную задачу**
  - Цель защиты КФС – обеспечение непрерывности производственного процесса, а цель ИБ – обеспечение конфиденциальности, целостности, доступности данных
- **Непродуманность КФС с точки зрения безопасности**
  - Возможность идентификации КФС и ПО в локальных и глобальных сетях
  - применение в современных КФС устаревших аппаратных и программных средств общего назначения
  - Слабые средства авторизации и аутентификации («вшитые» в ПО аутентификационные данные по умолчанию, ненадежные алгоритмы и т.д.)
  - Отсутствие шифрования в промышленных транспортных протоколах (modbus, s7comm и др.)
  - Слабые средства аудита и регистрации событий
- **Негибкая архитектура КФС и АСУ ТП**
  - Невозможность внесения существенных изменений в системы
  - Отсутствие обновлений операционных систем и приложений или невозможность их применить
  - Высокий риск автоблокировки системы при внедрении средств защиты
- **Человеческий фактор**

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

А что такое безопасность цифрового производства?



- С появлением киберфизических систем и Интернета вещей к понятию информационной безозопасности добавилось понятие кибербезопасности
- **Произойдет ли** при интеграции киберфизических систем с бизнес-процессами **расширение традиционного понятия информационной безопасности** еще на одну ступень?
- Альтернативный подход (Industrial Internet Consortium): меняется приоритет свойств безопасности, только не для данных, а для бизнес-процессов

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Существующие решения в области обеспечения безопасности производства

SIEMENS → *Defense in Depth*

KASPERSKY lab → *Industrial CyberSecurity*

CISCO → *Industrial Security*

- Защита физического доступа
- Межсетевое экранирование и VPN
- Сегментирование сетей
- Деактивация неиспользуемых интерфейсов
- Менеджмент обновлений
- Контроль целостности системы
- Поиск аномалий
- Комплексный мониторинг безопасности
- Обучение сотрудников

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Новые вызовы - новые задачи кибербезопасности

ГЛОБАЛЬНАЯ КИБЕРСРЕДА

БЕЗГРАНИЧНОСТЬ КИБЕРСРЕДЫ

- **Гигантское число** пользователей, узлов, потоков информации и управления
- **Нечеткий** периметр одноранговых инфраструктур
- **Автоматизация** администрирования **разнородных** компонентов
- Мониторинг и управление = **проблема «больших данных» и «умных решений»**

МОБИЛЬНОСТЬ КИБЕРСРЕДЫ

- **Перемещение** узлов, **высокая динамика** топологии
- **Отсутствие** фиксированной связности узлов
- **Ограничение вычислительной мощности** узлов
- **Сложность** соблюдения **единой** надсистемной и **согласованной** с ней внутрисистемной политики безопасности
- Необходимость **непрерывного** управления и контроля доступа

Новые задачи безопасности

ГЛОБАЛЬНОЕ ДОВЕРИЕ

КОГНИТИВНОСТЬ

БОЛЬШИЕ ДАННЫЕ

ДЕЦЕНТРАЛИЗАЦИЯ

АДАПТИВНОСТЬ

КИБЕРУСТОЙЧИВОСТЬ

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Конвергенция кибербезопасности в эпоху цифровизации

1. Эволюция безопасности для цифрового мира (ЦМ)

- Безопасность платформы ЦМ и всего ЦП от ЦД до приемки;
- Новые подходы к критериям ИБ;
- Новые цели и механизмы угроз, защита системы управления;
- Динамическая защита саморегулируемых систем.

2. Развитие фундаментальных основ кибербезопасности:

- Интеллектуализация защиты, учет динамических свойств КФС;
- Технологии BigData, машинное обучение, нейросети;
- Управление безопасностью и киберустойчивость
- Вычислительные проблемы, влияние размерности

Стратегия кибербезопасности

Предотвращение кибернападений, создание самоуправляющих систем, способных предотвратить угрозу и обеспечить устойчивость процессов всех промышленных и оборонных технологий, в эпоху глобальной цифровой трансформации становится основной задачей и условием технического прогресса.

От сохранности информации - к устойчивости управления передовыми технологиями - вот нарратив современного этапа нового технологического уклада.

ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

Кафедра ИБКС
ФГБОУ ВПО «СПбГПУ»

Главный учебный корпус, к. 173
Политехническая ул., 29,
Санкт-Петербург
195251

Тел: +7 (812) 552-76-32

Web: http://ibks.spbstu.ru
E-mail: zeg@ibks.spbstu.ru