



Информзащита
Системный интегратор



«Бумажная» и «реальная» кибербезопасность Industrial Internet

Даренский Дмитрий

Начальник отдела промышленных систем

ЗАО НИП «Информзащита»

«Информзащита» сегодня



Industrial Internet

Концепция развития новых цифровых сервисов и бизнес-моделей в результате подключения к сети и друг к другу «умных» устройств и машин, использования больших данных и облачных технологий.

Accenture Winning with the Industrial Internet of Things



«Industrial Internet» – сочетание анализа больших данных и интернета вещей, несущее огромные возможности в таких отраслях, как нефтегаз, электроэнергетика, производство, здравоохранение, добывающая промышленность, транспорт...

...возможность получать, обрабатывать и использовать результаты анализа больших данных, генерируемых промышленным оборудованием, которые напрямую влияют на стоимость, эффективность и конкурентоспособность бизнеса

General Electric and Accenture Alliance (Industrial Internet Insights Report for 2015)



Информзащита
Системный интегратор



Industrial Internet и «Industrie 4.0»



«Industrie 4.0» – технологическая концепция, объединяющая киберфизические системы (CPS), Интернет вещей (IoT) и телекоммуникационные сервисы. Стратегическая инициатива, направлена на обеспечение конкурентоспособности и защиту интересов промышленности Германии.

Industrie 4.0 Working Group (Recommendations for implementing the strategic initiative INDUSTRIE 4.0)



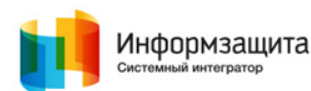
«Industrial Internet» – телекоммуникационная среда, объединяющая машины, системы управления, системы обработки больших данных и людей для получения максимальной производительности предприятий и гибкости бизнес-процессов с целью получения конкурентных преимуществ.

Industrial Internet Consortium (IIRA)



«Internet+» – новая экономическая форма, которая предполагает использование Интернета для оптимизации производственных ресурсов, направлена на распространение инноваций в промышленности и социальной сфере, а также предлагает новые, более обширные формы модели экономического развития, которая использует Интернет в качестве основного объекта и инструмента.

China Internet Plus Strategy (SESEC III Report)



Инициативы в области Industrial Internet

Инициатива	Учредители	Участники	Стандарты и инициативы
Industrie 4.0 Plattform	Правительство Германии	Более 150 пром. предприятий, ИТ-компаний и научных организаций Германии	Recommendations for implementing the strategic initiative INDUSTRIE 4.0
Industrial Internet Consortium (IIC)	GE, AT&T, CISCO, Intel, IBM	Более 250, включая SAP, Schneider Electric, Siemens, Kaspersky Lab UK, ABB, NIST, Waterfall, HP	Industrial Internet Reference Architecture ver.1.7
Open Interconnect Consortium (OIC)	GE, CISCO, Intel, Samsung, Arris	Более 150, включая Honeywell, Dell, IBM, Huawei, McAfee	OIC Specification 1.0 • Smart Home Device Specification 1.0.0 • Security Specification 1.0.0 • Resource Specification 1.0.0 • Remote Access Specification 1.0.0 • Core Specification 1.0.0
Internet Plus Strategy	Правительство Китая	Промышленность, ИТ-компании, научные организации и правительство Китая	Practical Application • Internet+Manufacturing Industry • Internet+Finance • Internet+Medical System • Internet+Government • Internet+Agriculture



Информзашита
Системный интегратор



Векторы развития «Industrie 4.0»

- Обеспечение конкурентных преимуществ за счет возможности давать задание непосредственно «умным машинам» и «умному производству» на разработку, производство и логистику продукции с уникальными характеристиками в промышленных масштабах
- Внедрение саморегулируемых производств на основе технологий M2M, машинного обучения и искусственного интеллекта
- Возможность гибкой оптимизации производственных и бизнес-процессов за счет использования результатов анализа больших данных в системах автоматизации, планирования и распределения ресурсов, систем управления производством с учетом быстро меняющихся рыночных условий и спроса
- Исключение «человеческого фактора» как источника ошибок и низко эффективной активности на всех стадиях производственной деятельности
- Перевод предприятий от «умных машин» к «умному производству» с использованием «умных сетей»



Информзашита
Системный интегратор



Значение вопросов кибербезопасности



Security by Design в качестве ключевого принципа проектирования. В современных промышленных системах управления безопасность обеспечивается путем физической защиты и ограничения доступа. В производственных системах на основе киберфизических систем (CPS) не достаточно добавить функции безопасности после внедрения. Все аспекты, относящиеся к кибербезопасности, должны быть разработаны в системах изначально.

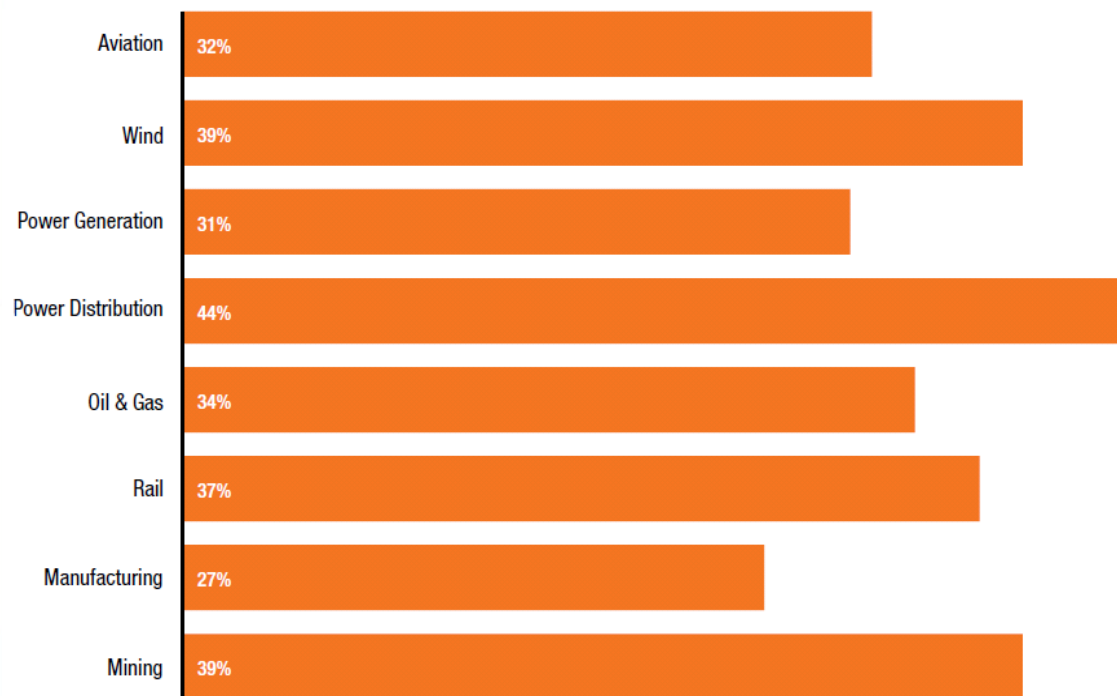
Industrie 4.0 Working Group (Recommendations for implementing the strategic initiative INDUSTRIE 4.0)



Безопасный дизайн систем, функционирующих как Industrial Internet System требует рассмотрения не только угроз и типичных проблем программного обеспечения, но также и аппаратного обеспечения, вопросов безопасной разработки и проектирования, программ обеспечения безопасности персонала и безопасности цепочек поставок.

Industrial Internet Consortium (IIRA)

Значение вопросов кибербезопасности



«Более трети предприятий в основных отраслях промышленности ставят задачи обеспечения безопасности в тройку приоритетных при использовании новых технологий, таких как анализ больших данных, M2M, Industrial Internet и т.д.»

General Electric and Accenture Alliance (Industrial Internet Insights Report for 2015)



accenture
High performance. Delivered.



Информзащита
Системный интегратор



Подходы к вопросам кибербезопасности Industrial Internet

Инициатива	Разработка вопросов кибербезопасности	Стандарты и инициативы
	Industrie 4.0 Plattform Отдельные разделы в рекомендациях по реализации инициатив Industry 4.0 (2013)	Recommendations for implementing the strategic initiative INDUSTRIE 4.0
	Industrial Internet Consortium (IIC) Разделы по безопасности референсной Архитектуры Промышленного Интернета. Разработаны на основе стандартов безопасности ИТ и ICS, таких как ENISA, NIST, IEEE, ANSI, ISA, IEC (2015)	Industrial Internet Reference Architecture ver.1.7
	Open Interconnect Consortium (OIC) Набор спецификаций, разрабатываемых в качестве приложений к референсной архитектуре интернета вещей (2015)	OIC Specification 1.0 • Smart Home Device Specification 1.0.0 • Security Specification 1.0.0 • Resource Specification 1.0.0 • Remote Access Specification 1.0.0 • Core Specification 1.0.0
	Internet Plus Strategy Разрабатываются стратегические и прикладные инициативы для каждой критичной отрасли	Practical Application • Internet+Manufacturing Industry • Internet+Finance • Internet+Medical System • Internet+Government • Internet+Agriculture

Актуальность темы Industrial Internet в России

СОКРАЩЕНИЕ ТЕХНОЛОГИЧЕСКОГО ОТСТАВАНИЯ

- Всегда есть к чему стремиться, особенно нам

ФОРМИРОВАНИЕ ЗАПРОСА НА КОНКРЕТНЫЕ ИННОВАЦИИ И ТЕХНОЛОГИИ ОТ КОНКРЕТНЫХ ПРОМЫШЛЕННЫХ «ПОЛЬЗОВАТЕЛЕЙ»

- У нас уже есть примеры реализации и использования технологий

ПОВЫШЕНИЕ КОНКУРЕНТОСПОСОБНОСТИ ЗА СЧЕТ АВТОМАТИЗАЦИИ ПРОИЗВОДСТВА ПО ПРИНЦИПУ «END-TO-END»

- В отдельных отраслях уже начаты работы с применением аналогичных технологий



Информзащита
Системный интегратор



Текущая ситуация с кибербезопасностью индустриальных систем в России

Участники рынка	«Бумажная» безопасность	«Реальная» безопасность
Владельцы систем	Классификацию АСУ ТП по 31 приказу не проводят, потому что никто не обязывает. Отнесение к КСИИ проводят с целью отбиться от регуляторов по формальному отсутствию КСИИ (даже на КВО). Отдельные отраслевые ведомства (Минэнерго, например) только приступили к разработке собственных требований	Стараются защититься преимущественно организационными и компенсирующими мерами. Внедрение накладных СЗИ у единичных организаций и их функциональность под вопросом
Производители систем	Не сертифицируются по требованиям безопасности в России, потому что никто не требует этого от них.	Крупнейшие производители (Emerson, Rockwell, Schneider Electric, Siemens, Yokogawa и др.) предлагают собственные решения по защите информации и компонентов. Но эти решения либо не внедряют в целях экономии бюджетов, либо не используют в целях облегчения эксплуатации
Производители средств защиты информации	Сертифицируют свою продукцию по требованиям безопасности, но самих решений крайне мало	Реальных кейсов с внедрением промышленных СЗИ мало, в основном, это межсетевые экраны и антивирусы



Информзащита
Системный интегратор



Кибербезопасность промышленных систем в России

«Бумажная» безопасность

- Нормативно-техническая база документов прикладного характера ограничена и без учета отраслевых специфик
- Нормативно правовые акты носят рекомендательный характер.
- Нормативы предписывающего или обязательного характера не введены
- Ввод в действие международных стандартов на территории России идет медленно

«Реальная» безопасность

- Спрос на «реальную защиту» промышленных систем только начал появляться
- Предприятия не спешат финансировать создание систем защиты, т.к. не видят экономической целесообразности, практической пользы и конкурентных преимуществ
- Распространен подход «сначала отбиться от регулятора, а защищаться потом (когда-нибудь, если захотим)»

Переход к Industrial Internet

«Бумажная» безопасность

- Остается открытым вопрос государственного и технического регулирования
- Нет понимания на какие стандарты опираться. Своих нет, зарубежные только появляются

«Реальная» безопасность

- Нет понимания необходимости и запроса на технологию Industrial Internet
- Подходы к обеспечению безопасности Industrial Internet и существующих промышленных системах принципиально отличаются
- Отсутствует кооперация по вопросам развития Industrial Internet между технологическими компаниями, владельцами телекоммуникационных инфраструктур и представителями отдельных отраслей

Принципы реализации инициатив Industrial Internet

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ РАЗВИТИЯ ТЕХНОЛОГИЙ INDUSTRIAL INTERNET ДЛЯ КОНКРЕТНЫХ ОТРАСЛЕЙ И ПРОМЫШЛЕННОСТИ В ЦЕЛОМ

**ФОРМИРОВАНИЕ СПРОСА НА ТЕХНОЛОГИИ INDUSTRIAL INTERNET
«СНИЗУ»**

**СТИМУЛИРОВАНИЕ РАЗРАБОТОК НОВЫХ ТЕХНОЛОГИЙ, ОБОРУДОВАНИЯ
И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**



Информзащита
Системный интегратор



Развитие инициатив Industrial Internet в России

СОЗДАНИЕ НАЦИОНАЛЬНОГО КОНСОРЦИУМА ИЗ ПРЕДСТАВИТЕЛЕЙ ПРОМЫШЛЕННОСТИ И ТЕХНОЛОГИЧЕСКИХ КОМПАНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ СТАНДАРТИЗАЦИИ И МЕЖОТРАСЛЕВОГО ВЗАИМОДЕЙСТВИЯ

- ОИС и ИИС созданы не более двух лет назад. В России аналог будет создан в ближайшие месяцы



Информзащита
Системный интегратор



Использованные источники

- Industrial Internet Reference Architecture ver.1.7
- OIC Specification 1.0
 - Smart Home Device Specification 1.0.0
 - Security Specification 1.0.0
 - Resource Specification 1.0.0
 - Remote Access Specification 1.0.0
 - Core Specification 1.0.0
- Industrial Internet Insights Report for 2015
- Recommendations for implementing the strategic initiative INDUSTRIE 4.0
- China Internet Plus Strategy SESEC III Report
- The Industrial Internet Consortium's Approach to Securing Industrial Internet Systems
- ISA/IEC 62443
- NIST 800-82 Rev.2
- NISTIR 7628 Revision 1
- IEC 62351
- IEEE C37.240-2014
- ГОСТ Р МЭК 62443-2-1-2015
- Приказ №31 от 14.03.2014 ФСТЭК
- ГОСТ Р 8.654-2009
- Р 50.2.077-2014
- МИ 2955-2010
- Результаты проектов ЗАО НИП «Информзащита» для промышленных предприятий



Информзащита
Системный интегратор



СПАСИБО! ВОПРОСЫ?

Даренский Дмитрий,
Начальник отдела промышленных систем
ЗАО НИП «Информзащита»
d.darensky@infosec.ru