



КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ



Екатеринбург

12.07.2023

# Йоханн Воронин

PMP®, Project Management Institute  
Scrum Master®, Product Owner®

- Дипл. Инж. Бизнес-Информатика, университет Дортмунд
- Управление проектами
- Интегрированная информационная безопасность
- Эксперт в области оцифровки процессов





**Промышленный интернет вещей  
угрозы и решения.**

# Немного статистики

**IoT Endpoint Market by Segment, 2018-2020, Worldwide  
(Installed Base, Billions of Units)**

Segment	2018	2019	2020
Utilities	0.98	1.17	1.37
Government	0.40	0.53	0.70
Building Automation	0.23	0.31	0.44
Physical Security	0.83	0.95	1.09
Manufacturing & Natural Resources	0.33	0.40	0.49
Automotive	0.27	0.36	0.47
Healthcare Providers	0.21	0.28	0.36
Retail & Wholesale Trade	0.29	0.36	0.44
Information	0.37	0.37	0.37
Transportation	0.06	0.07	0.08
<b>Total</b>	<b>3.96</b>	<b>4.81</b>	<b>5.81</b>

Source: Gartner (August 2019)

-  1. Внедрение вредоносного программного обеспечения со съемных и внешних носителей
-  2. Заражение вредоносным ПО через Интернет и Интранет
-  3. Проступки и саботаж со стороны людей
-  4. Компрометация компонентов экстранет и облака
-  5. Социальная инженерия и фишинг
-  6. (D)DoS-атаки
-  7. Подключенные к Интернету компоненты управления
-  8. Взлом через удаленный доступ для обслуживания
-  9. Технические нарушения и форс-мажорные обстоятельства
-  10. Компрометация смартфонов в производственной среде

# Слабые места

- Ландшафт угроз Интернета вещей быстро расширяется. Тем не менее, многие организации не осознают ответственности за управление рисками Интернета вещей.
- Персонал и бюджет недостаточны для управления сторонними рисками Интернета вещей. (Supply Chain Management)
- Управление рисками третьих лиц должно Риски Интернета вещей существуют , но в большинстве случаев их еще нет.
- Предприятия должны быть готовы к появлению новых стандартов соответствия для Интернета вещей.
- Большинство компаний не проводят обучение сотрудников рискам, связанными с устройствами Интернета вещей.





Цель: Встроенная безопасность

# Безопасность на всех слоях

Человек

Безопасность приложения

Безопасность облака

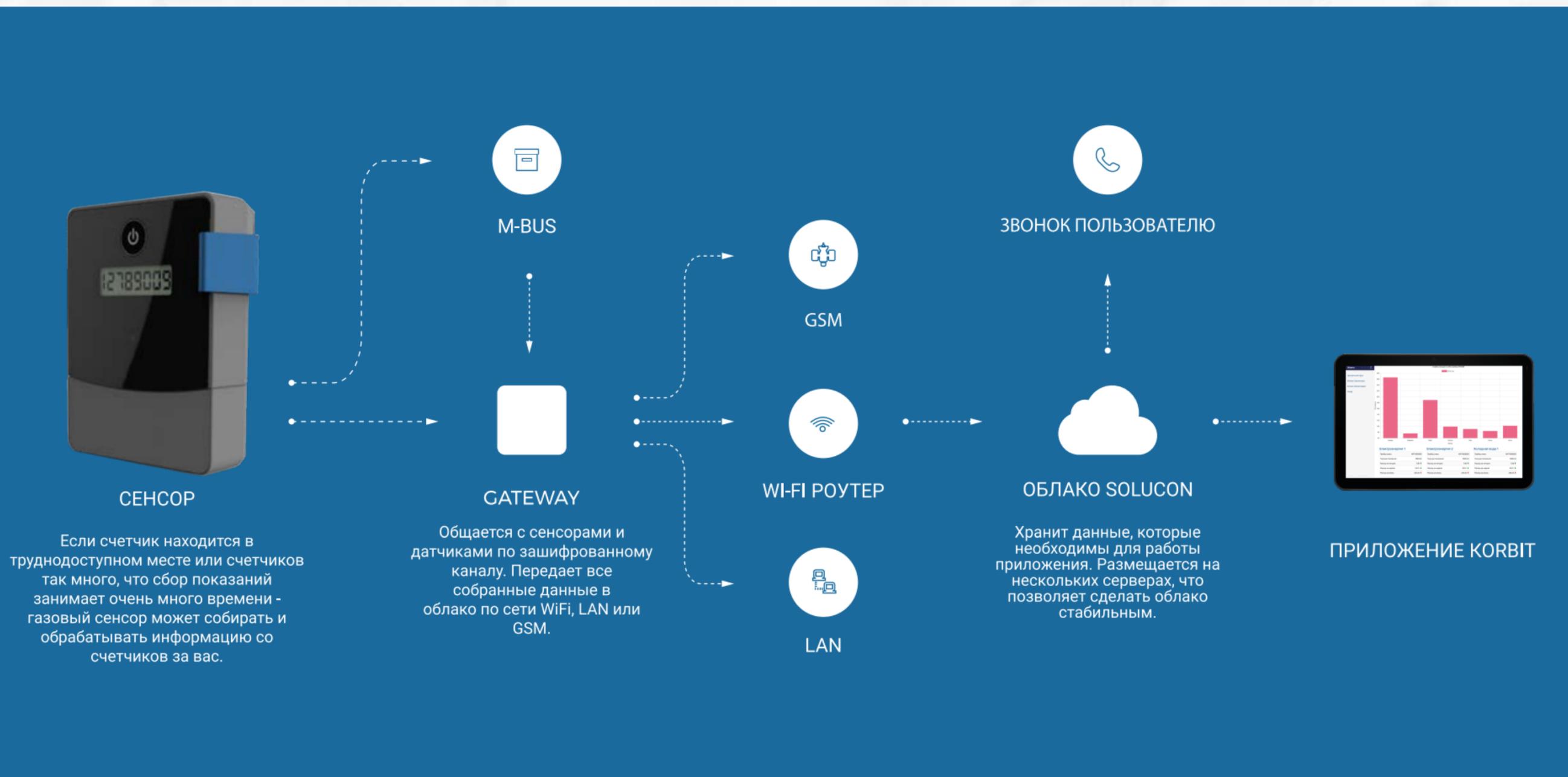
Безопасность шлюза

Шифрование протокола

Аппаратная часть (Security by Chip)



# Безопасность на всех слоях





# Целенаправленные меры безопасности

Контроль доступа

Стороннее программное обеспечение

Безопасная коммуникация

Этика безопасности

Процессы безопасности

Безопасная реализация



# ГОТОВ ОТВЕТИТЬ на ваши вопросы

E-mail: [jvoronin@gmail.com](mailto:jvoronin@gmail.com)

Phone: +7 906 219 66 00

