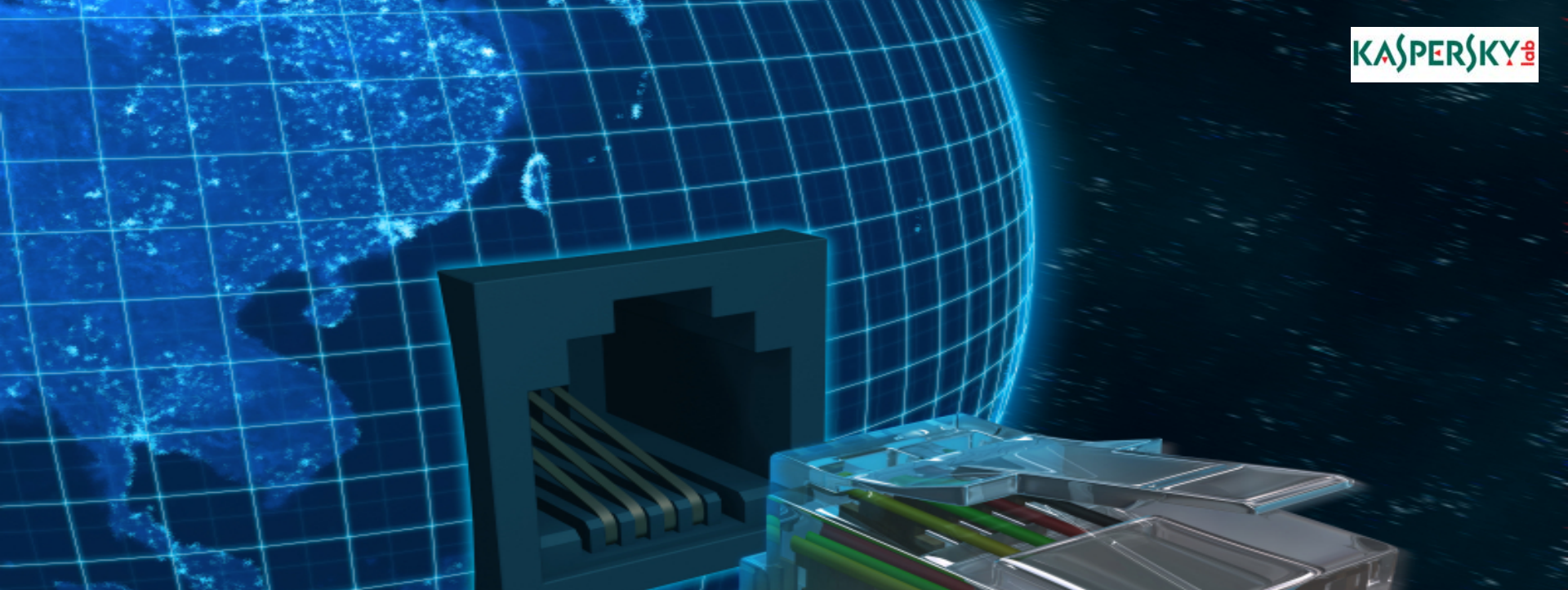




IIoT – Industrial Internet of Threats?

IIoT: Промышленный Интернет Угроз?

# Internet of Things: начало новой эры



Кевин Эштон — помощник бренд-менеджера Proctor & Gamble

В 1999 году предложил термин Internet of Things  
В XX веке компьютеры были мозгом без чувств — они знали только то, что мы могли сказать им. Это было огромным ограничением: в мире во много миллиардов раз больше информации, чем люди могу ввести с клавиатуры или сканировать с помощью бар-кодов. В XXI веке, в рамках парадигмы «Internet of Things», компьютеры смогут чувствовать вещи самостоятельно

**IoT: концепция вычислительной сети физических объектов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой (*Gartner IT glossary, 2012*)**

## An abstract graphic featuring a dark grey background with a light grey, angular, mountain-like shape on the left. Overlaid on this are several thin, light green lines that form a network or circuit-like pattern, connecting small white circular nodes. The lines and nodes are distributed across the upper and middle portions of the image.



# Internet of Things: умные города



# Internet of Things: инциденты

**SECURELIST** УГРОЗЫ ▾ КАТЕГОРИИ ▾ ТЕГИ ▾ ЭНЦИКЛОПЕДИЯ СТАТИСТИКА ОПИСАНИЯ

## Атаки на больницы в 2016 году

Сергей Ложкин · март 24, 2016. 11:54

11 0

Facebook Google+ Mail.ru

0 3

0 Comments 3 YouTube 0 Twitter

**В АНАЛИТИКЕ**  
Kaspersky Security Bulletin 2015:  
Развитие угроз в 2015 году  
Учимся жить в «интернете вещей»  
Интернет вещей: как и какую свою  
бюм

**В БЛОГЕ**  
Как обмануть датчики бортового  
безопасности  
Эксперт: как я взломал больницу  
Эксперт на Smart TV?  
0-day: теперь и в медицине  
Голливудский сценарий:  
незащищенные системы  
видеонаблюдения

**КАЖДЫЙ ВИДИТ НЕ ТО,  
ЧТО ХОЧЕТ ВИДЕТЬ**

**БАНКОВСКИЙ ТРОИЦЕЦ  
ЛИНК: СПЕЦИАЛЬНО ДЛЯ  
РОССИИ**

2016 год начался значительным числом инцидентов, связанных со взломом больниц и медицинского оборудования. Среди них — атака на больницу в Лос-Анжелесе с применением программы-вымогателя, аналогичные атаки на две немецких больницы, взлом исследователями в области безопасности монитора, с помощью которого контролируется состояние пациента, и системы раздачи лекарств, атака на больницу в Мельбурне. — список можно продолжать. Все эти инциденты произошли в первые два месяца 2016 года! Представителям индустрии безопасности есть о чем задуматься.

В действительности в этом нет ничего неожиданного. Интернет вещей активно развивается, а

<https://securelist.ru/blog/issledovaniya/28312/hospitals-are-under-attack-in-2016-2/>

**SC MAGAZINE** FOR IT SECURITY PROFESSIONALS

SC US SC UK

Stream Stealer malware attacks on gamers' credentials gaining steam

Report: IoT data leaks, unreported vulnerabilities, among top threats that lay ahead

'Suckfly' in the environment: Chinese API group steals code-signing certificates

LATEST ISSUE

LOG IN | REGISTER

NEWS PRODUCT REVIEWS BLOGS SC CONGRESS SC EXTRAS EVENTS RESOURCE LIBRARY

SC Magazine > News > Ransomware holds data hostage in two German hospitals

Rene Millan  
February 29, 2016

## Ransomware holds data hostage in two German hospitals

This article originally appeared on SC Magazine UK

Share this content

A ransomware campaign has hit two German hospitals, soon after another ransomware campaign hit a Los Angeles medical centre, and the clean up is set to take weeks.

Two German hospitals have fallen victim to a ransomware attack that has left them unable to access their systems. It is thought the clean-up operation to remove all traces of the malware could take weeks.

According to a report by German broadcaster Deutsche Welle, the attack took place two weeks ago at the Lukas Hospital in the city of Neuss. Another attack took place at the Klinikum Amberg hospital which is located in North Rhine-Westphalia. It is not known if the two attacks are related.

Two more German hospitals have been hit with ransomware

**SIGN UP TO OUR NEWSLETTERS**

SC Magazine Featured White Paper of the Day  
SC Magazine Newswire  
SC Magazine Product Reviews  
SC Magazine Product/Industry Buzz

United States

Enter your email address Sign up

<http://www.scmagazine.com/ransomware-holds-data-hostage-in-two-german-hospitals/article/479835/>

# Internet of Things: инциденты

07:48 07 июля 16+ Газета

**ВЕДОМОСТИ**

Подписаться Войти

Бизнес Экономика Финансы Мнения Политика Технологии Недвижимость Авто Менеджмент Стиль жизни

USD 65.3275 Euro 74.3 RUB 7015.54 PTS 162.91 SAR 500 2109.41 Brent 50.55 Золото 1245.6

Дизайн и технологии

## Хакеры смогли взять под контроль движущийся Jeep Cherokee

Прежде манипулировать электроникой автомобиля удавалось, только подсоединившись к нему через кабель

22.07.15 20:37 Видеомосты Геннадий Анисимов



Пока не ясно, в скольких машинах существует проблема безопасности jeep.com

Два исследователя компьютерной безопасности продемонстрировали, что могут взять под контроль движущийся Jeep Cherokee через систему беспроводного подключения автомобиля к интернету, пишет *The Wall Street Journal*. Это ставит новые вопросы о безопасности интернет-подключенных автомобилей, отмечает издание.

<https://www.vedomosti.ru/auto/articles/2015/07/22/601762-hakeri-smogli-vzyat-pod-kontrol-dvizhushchiysya-jeep-cherokee>

Экспорт RSS 7 июля 2014, 07:48 15+ Выходя за пределы

**газета.ru**

Москва +4°C

Политика Бизнес Общество Армия Мнения Культура Наука Технологии Авто Стиль жизни Спорт

Тест-драйвы Замор и приво Город Автомеханика Происшествия Дороги Авторьнок Становление

Автомобили и город

## Вирус скорости

Все подмосковные комплексы фото- и видеонаблюдения вышли из строя из-за вируса

Анатолий Караваев 13.01.2014, 16:00



По данным «Газеты.Ru», ни одна из установленных в Подмоскowie камер ГИБДД «Стрелка-СТ» не работает. Более 100 комплексов вывел из строя загадочный вирус, парализовавший работу всей системы в ночь с 9 на 10 января. В ГИБДД подтвердили коллапс, но пока не называют причин случившегося. Эксперты считают собой беспрецедентным — восстановление работы всех камер займет не меньше месяца.

О серьезных проблемах, возникших несколько дней назад с комплексами автоматической фото- и видеонаблюдения правонарушений «Стрелка-СТ», «Газета.Ru» стало известно сразу из нескольких источников, в том числе в подмосковном континенте.

**Главное**

Комитет Госдумы одобрил законопроект о платном въезде в города +

МВД усилит контроль за телемониторингом +

У стел Крылья за крупную взятку задержали трех инспекторов ГИБДД +

В Москве у безработного уроженца Дагестана украли Mercedes за 6 млн рублей +

Из-за скандала ИАТО польская таможня решила проверить российских водителей +

**Читайте также**

Испытка для «уникала» Бразилия +

Смартфон-конструктор LG G5: Первое знакомство +

Книги на Классик.плотности +

[http://www.gazeta.ru/auto/2014/01/13\\_a\\_5845877.shtml](http://www.gazeta.ru/auto/2014/01/13_a_5845877.shtml)

# Состояние информационной безопасности в мире промышленной автоматизации

## Документированная статистика инцидентов в АСУ ТП



|                        | 2014 |      | 2015 |      |
|------------------------|------|------|------|------|
| Всего инцидентов       | 245  | 100% | 295  | 100% |
| Critical manufacturing | 27   | 11%  | 97   | 33%  |
| Energy                 | 32   | 13%  | 46   | 16%  |
| Water                  | 6    | 2%   | 25   | 8%   |
| Government facility    | 5    | 2%   | 18   | 6%   |
| Transportation         | 5    | 2%   | 23   | 8%   |
| Chemical               | 2    | 1%   | 7    | 2%   |
| Nuclear                | 2    | 1%   | 7    | 2%   |

По данным US ICS-CERT.

# цифровая подстанция

В октябре 2015 года Лаборатория Касперского в рамках своей конференции, посвященной информационной безопасности АСУ ТП провела соревнования среди команд, специализирующихся на поисках уязвимостей в информационных системах (CTF)

## Стадии атаки:

- Перехват сетевого трафика
- Получение доступа к системе
- Отключение защитной автоматики (РЗА)
- Короткое замыкание на макете ЛЭП

Три из четырех команд-финалистов реализовали аварийную ситуацию в первый день знакомства с объектом:

- Специалисты в области РЗА – за 3 часа
- Хакеры широкого профиля – за 5 часов



# Industrial Internet of Things: начало новой эры

**МЭФ 2015:** Концепция Индустриального Интернета приведет к трансформации многих отраслей включая машиностроение, нефтяную и газовую промышленность, сельское хозяйство, добычу полезных ископаемых, транспорт и медицину. В общей сложности эти изменения затронут 2/3 мировой экономики.

[Industrial Internet of Things: Unleashing the Potential of Connected Products and Services](#). Отчет Мирового Экономического Форума. Январь, 2015

**Accenture:** Потенциальный рост производства за счет внедрения IIoT оценивается в \$12 триллионов увеличения ВВП к 2030

Эффективная промышленность за счет:

- Эффективное использование энергии
- Эффективные склады и сети поставки
- Аналитика состояния оборудования
- Предсказание мероприятий по обслуживанию
- Индивидуальное и мелко-серийное производство по стоимости продукции сравнимо с крупносерийным

# Безопасность CPS: подход к снаряду

## Два измерения безопасности систем

**Safety** (внутренняя безопасность) – свойство системы сохранять работоспособность, не наносить вред окружающей среде и людям при условии ее эксплуатации в соответствии с predetermined правилами и в заданных условиях.

**Security** (внешняя безопасность) – степень устойчивости к внешним угрозам или степень защиты от внешних угроз. Применимо к значимым и уязвимым системам. Безопасность предоставляет форму защиты когда создается какое-либо разделение между системой и угрозой.

Для CPS значимым является соблюдение обоих условий = safety + security

# IoT: основные принципы

**Концепция, рассматривающая организацию «умных» сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека (Кевин Эштон, 2009)**

Аспекты, которые необходимо учитывать в целях безопасности

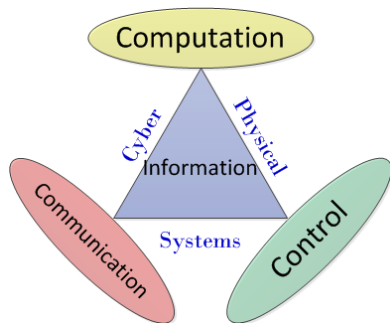
- «вещи»: однозначно идентифицируемые сущности (RFID, bar-code, GPS, etc)
- «вещи умные»: встроенные (информационные) технологии
- «вещи взаимодействующие»: сети и протоколы обмена информацией
- «вещи чувствующие»: датчики, информация об окружающей среде
- «большие данные»: вычислительные средства, способные обрабатывать большие объемы данных

**кибер-физические системы (CPS):** системы, способные реагировать и воздействовать на окружающую среду

# Безопасность IIoT: подход к снаряду

Чем отличается кибер-безопасность CPS от IT systems

## Cyber-Physical system (CPS)



## Приоритеты целей

| IT                 | CPS                |
|--------------------|--------------------|
| Конфиденциальность | Доступность        |
| Целостность        | Целостность        |
| Доступность        | Конфиденциальность |

# Безопасность IIoT: подход к снаряду

Сейчас существует уникальная возможность разрабатывать устройства и системы «with security in mind». Необходимо учитывать опыт разработки систем АСУ ТП

Необходимо использовать экспертизу безопасности на ранних стадиях проектирования IIoT систем. Мы уже видели последствия, когда этого не происходит. Jason Porter, Vice President, Security Solutions, AT&T

Совершенно необходимо разрабатывать IoT устройства с учетом требований информационной безопасности. Для минимизации риска их компроментации очень важно изолировать критические устройства от избыточных коммуникаций

Chris Penrose, Senior Vice President,  
Internet of Things Solutions, AT&T



Спасибо  
за  
ВНИМАНИЕ

**sIIoT: Secure** Industrial Internet of Things!

**sIIoT: Безопасный** Промышленный Интернет Вещей!

Андрей Духвалов  
Руководитель департамента Перспективных Технологий  
Andrey.Doukhvalov@Kaspersky.com

7 июня 2016, Санкт Петербург, IoT Summit

KASPERSKY  
lab