Ризики та здобутки “Інтернету речей” (Internet ofthings)

Згідно з визначенням аналітиків InternationalDataCorporation, інтернет речей - це мережа, що складається з мереж з унікально ідентифікованими точками, які спілкуються між собою в обох напрямках по IP-протоколів без людського втручання. Визначення досить загальне, але воно здається найбільш несуперечливим. Спроби якось конкретизувати формулювання зазвичай призводять до того, що багато сегментів інтернету речей просто випадають з визначення IoT. Підрозділ Cisco - однієї з компаній, що створювала сучасний інтернет - вважає, що інтернет речей з'явився в 2008-2009 роках, коли кількість підключених пристроїв перевищила кількість людей, що живуть на Землі. Зараз же тільки кількість IoT-пристроїв і IoT-датчиків (без урахування комп'ютерів, смартфонів і інших призначених для користувача терміналів) перевищує 8,4 млрд, а до 2020 року їх кількість перевищить 20 млрд.

За даними всесвітнього дослідження PwCDigital IQ® за 2017 рік, IoT займає перше місце серед восьми проривних технологій, здатних змінити бізнес-моделі компаній або цілих індустрій, випереджаючи в цьому рейтингу штучний інтелект, доповнену реальність, технологію, пов'язану зі створенням дронів і управлінням ними, блокчейн і ряд інших.

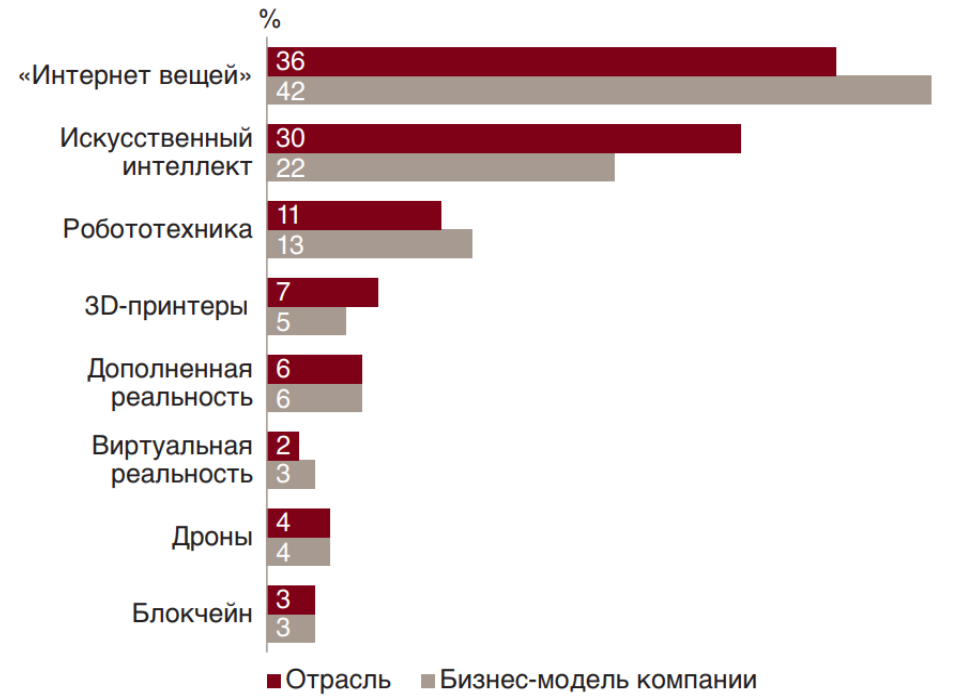

Рис.1 Рейтинг технологій, складений з урахуванням ступеня їх впливу на бізнес-моделі компаній або цілі галузі

Рис. 2. Рейтинг технологій, складений з урахуванням їх інвестиційної привабливості

Поширення IoT в світі стало можливим завдяки чотирьом технологічним трендам:

- знизилася вартість обчислювальних потужностей (Процесорів, пам'яті і систем зберігання даних);
- знизилася вартість передачі даних;
- Завдяки розвитку «хмарних» технологій і «великих даних» стають доступними гнучкі системи зберігання та аналізу даних, незважаючи на постійне збільшення обсягу одержуваної інформації;
- швидко зростає число «Підключених» пристроїв.

Застосування технологій IoT змінить вигляд багатьох індустрій і областей життєдіяльності. У ряді областей людські трудовитрати і помилки будуть зведені до мінімуму. Так, IoT в електроенергетиці кардинально змінить технології, забезпечить економію коштів і створить нові продукти у всіх ланках енергосистем. У сільському господарстві IoT дозволить впровадити точне землеробство і значно вдосконалити управління сільхозтранспортом. Рішення IoT в логістиці допоможуть скоротити витрати, підвищити прозорість ланцюжка доставки товарів і скоротити використання людської праці. технології **«SmartCity»** дозволять створити більш привабливу міську середу з ефективно працюючої транспортною системою, ЖКГ, зручною інфраструктурою і забезпечити безпеку населення. серед компонентів **«SmartCity»** найбільшою популярністю у споживачів користуються пристрої підвищення безпеки, контролю споживання води і енергії, «Розумні» побутові прилади і термостати.

“Сила”

Був реалізований проект в теплових мережах. Він вирішував основні проблеми в Тепломережевому бізнесі, такі як вдосконалення обліку, скорочення втрат, оптимізація витрат. Наприклад, в технічній політиці передбачено, що при капітальних ремонтах і реконструкціях використовуються тільки ізольовані трубопроводи (Трубопроводи високої заводської готовності) з системою дистанційного контролю зволоження та ізоляції(Система провідників, вбудованих в ізоляцію труби). передача сигналу з даних трубопроводів в єдину мережу дозволяє визначати пошкодження з точністю 1-3 метра. такі трубопроводи не вимагають обслуговування і дають можливість оптимізувати витрати на обслуговування і скорочувати втрати. Використання сучасної запірної арматури і тотальне «оприборювання» лічильниками, що дозволяють дистанційно знімати показання і управляти регуляторами і арматурою, стало альтернативою утримування численного персоналу обхідників.

Рис. 12. Области применения IoT в сельском хозяйстве и животноводстве

«Розумне сільське господарство» ставить перед собою мету максимально автоматизувати сільськогосподарську діяльність, підвищити врожайність і якість продукції. Точне землеробство (GPS, датчики, дрони) - це широкий спектр технологій від планування посіву та підготовки грунту, моніторингу стану і управління посівом, контролю рівня вологості, мінералізації грунту і температурного режиму до збору самого врожаю.

Точне землеробство покликане оптимізувати операційні витрати і підвищити врожайність (в середньому на 15-20%), які досягаються шляхом:

- скорочення обсягів використовуваних насіння, агрохімікатів, добрив і води (використання «За потребою»);

- • більш ефективного використання землі: з урахуванням особливостей тієї чи іншої ділянки визначається агрокультура з найбільшою врожайністю, а також оптимальна методика вирощування та догляду для максимізації урожайності.

При використанні **«розумних теплиць»** (Датчики, пристрої та комплектуючі, ПЗ для віддаленого управління теплицями) операційна економія досягається шляхом більш ефективної витрати добрив, хімікатів, а також води. Технологія також дозволяє оптимізувати кількість персоналу, який потрібен для догляду за культурами, і знизити втрати, що виникають через людський
фактор.

«Розумні ферми» (датчики, пристрою і ПО для моніторингу) дозволяють підвищити продуктивність тварин і якість продукції. За оцінкою експертів ринку, автоматизовані системи відгодівлі, доїння і моніторингу здоров'я поголів'я худоби можуть підвищити надої на 30-40%.

Моніторинг транспорту за допомогою GPS і датчиків дозволяє в першу чергу знизити витрату пального (Експерти прогнозують можливе зниження до 20%), а також оптимізувати маршрути і завантаження персоналу. В українській практиці актуальним також залишається питання збереження сировини в процесі його збору і переміщення - відповідні датчики дозволяють повністю відслідковувати як місцезнаходження, так і вага переміщуваного сировини, тим самим практично ліквідуючи можливості для шахрайства

Управління сировиною (датчики, пристрою і ПО для моніторингу) покликане скоротити втрати (до 25%) через неоптимальні умови зберігання сільгосппродукції. Спеціально задані алгоритми в режимі реального часу здійснюють моніторинг стану продукції (зокрема, температурний режим сховищ, рівень вологості, зміст вуглекислого газу) і допомагають прийняти рішення про необхідність збуту / подальшої переробки.

“Темна сторона сили”

Незважаючи на всі переваги IoT-технологій, звичайних людей все ж лякають їх можливості. Так згідно з опитуванням Gemalto, близько 90% користувачів не довіряють IoT-пристроям.

На думку технічного директора CheckPointSoftware Technologies Микити Дурова, з розвитком інтернету речей очевидно зростають ризики витоку даних. Одним з головних недоліків безпеки IoT-пристроїв є слабкий вбудований захист.

Восени 2107 року, фахівці виявили вразливість в мобільному і хмарному додатках LG SmartThinkQ, яка дозволила віддалено увійти в хмарне додаток SmartThinQ, і, заволодівши обліковим записом LG, отримати контроль над пристроями розумного будинку. Зокрема, стало доступним управління пилососом і головне, вбудованої в нього відеокамерою, яка в режимі реального часу надсилає відео в додаток LG SmartThinQ. Таким чином, користувач міг бути жертвою хакерської атаки і навіть не знати про це.

Загроза в масштабах країни

Ще одним результатом злому IoT-девайсів, на думку, може стати зараження пристроїв для створення ботнетів і проведення DDoS-атак. Крім того, IoT може стати новою віхою кібершіонажа. Ще в 2016 році, Джеймс Клеппер, який займав тоді пост директора національної розвідки США, не виключив, що спецслужби будуть використовувати інтернет речей для «з'ясування особи, спостереження, спостереження, визначення місцезнаходження та збору інформації, вербування, а також для отримання доступу до мереж і даних користувачів ».

Те що **«BigBrother»** отримає можливість буквально (завдяки тим же фітнес-трекера з GPS і розумним годинах) стежити за кожним нашим кроком, не приводить у захват навіть законослухняних громадян. Впровадження інтернету речей призведе до формування нової моделі розвідки, що базується на високоавтоматизованому комплексному збиранні та аналізі даних, що надходять через інтернет.

Однак найбільшим кошмаром для фахівців а області безпеки є, зовсім, не злом пилососів і телевізорів, і не всевидюче око «Великого брата», а злом індустріального та інфраструктурного IoT хуліганами, зловмисниками і терористами.

Сьогодні вже існують цілі ресурси для пошуку вразливих підключених пристроїв інтернету речей. Аналізуючи ці дані, зловмисники можуть отримати відомості про охорону, графіку роботи компанії або окремих осіб, а також підслуховувати конфіденційні розмови, а потім використовувати отриману інформацію в своїх цілях.

Хак кондиціонера, як показало наше дослідження, може залишити без світла цілий квартал. При зломі пристроїв міської та промислової інфраструктури дані можуть використовуватися для шантажу, вимагання і шпигунства. Реальну небезпеку становлять і атаки на транспорт - оскільки в разі злому виникає пряма загроза життю людей