



**РЕГИОНАЛЬНЫЙ СЕМИНАР МСЭ ДЛЯ СТРАН СНГ И ГРУЗИИ**  
**“ТЕНДЕНЦИИ РАЗВИТИЯ КОНВЕРГЕНТНЫХ СЕТЕЙ:  
РЕШЕНИЯ ПОСТ – NGN, 4G и 5G”**

Секция “Безопасность в сетях мобильной связи”

Доклад на тему:

**“Защита информационных ресурсов в сетях нового поколения”**

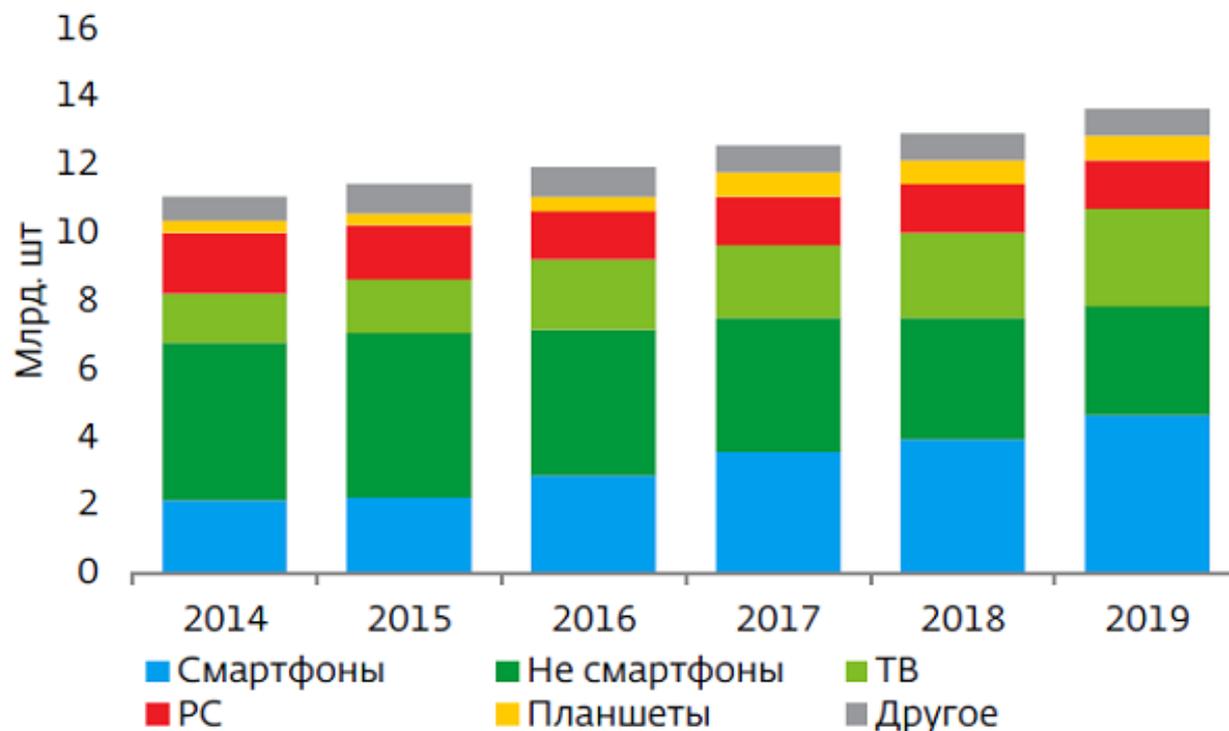
Докладчик: директор Учебно-научного института защиты информации  
Государственного университета телекоммуникаций  
д.т.н., с.н.с. Наконечный Владимир Сергеевич

# Развитие ИТ создает основы современной экономики государства и благосостояния ее людей

В развитых странах мира продолжается переход к информационной сервисно-технологической экономике, где значительная часть ВВП обеспечивается деятельностью по производству, обработке и распространению информации и знаний.

Экономистами и политиками всего мира осознанно, что развитие ИТ создает фундамент современной экономики государства и благосостояния ее людей.

## РОСТ КОЛИЧЕСТВА ПОЛЬЗОВАТЕЛЬСКИХ УСТРОЙСТВ...



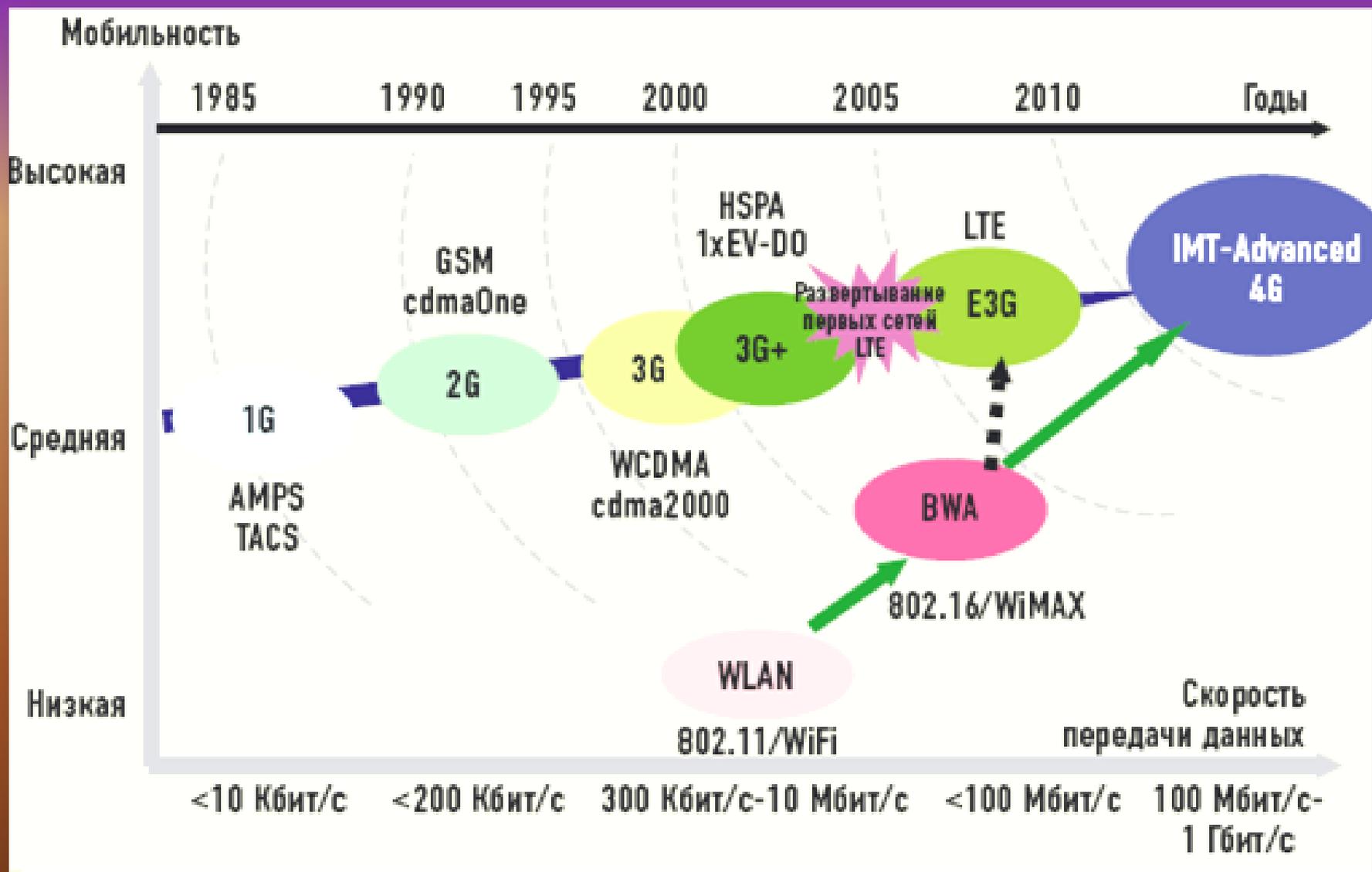
источник: cisco, май 2015

Без высокоскоростного мобильного интернета, доступного прямо  
здесь и сейчас, уже нельзя



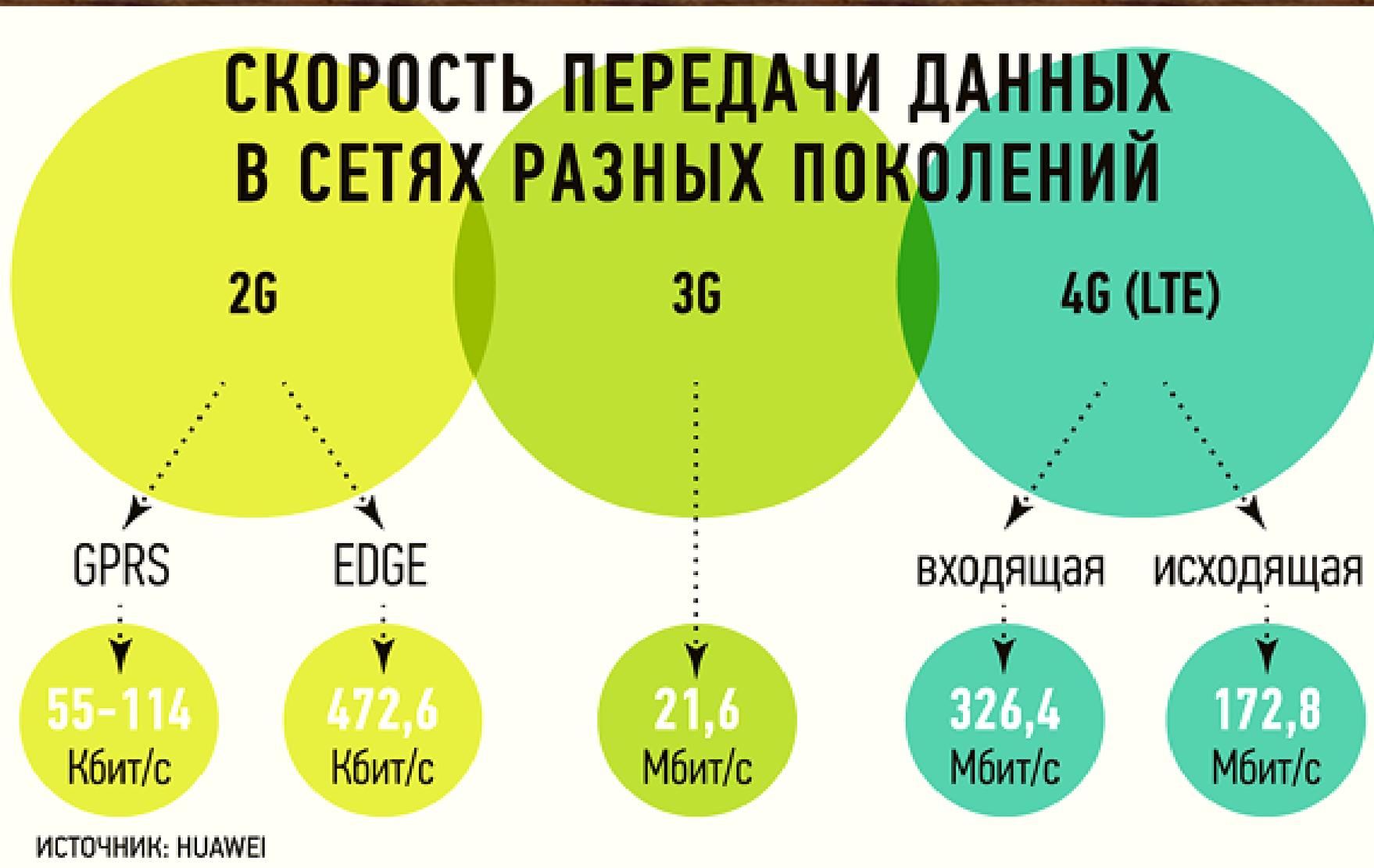
Видеохостинги, потоковые сервисы воспроизведения музыки, общение по FaceTime, Skype или другому популярному мессенджеру с функцией видеозвонков – всё это **требует качественного высокоскоростного соединения.**

Стоит только раз попробовать возможности LTE – отказаться от этого будет уже невозможно. А главное – незачем. **За ними будущее!**



Источник: Samsung Electronics

# Какой прирост скорости стоит ожидать пользователям новых сетей?



## ЦЕЛИ СОЗДАНИЯ СТАНДАРТА LTE:

- ✓ Увеличение возможностей высокоскоростных систем мобильной связи.
- ✓ Уменьшение стоимости передачи данных.
- ✓ Возможность предоставления широкого спектра недорогих услуг.

### ТЕХНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ LTE

**Flexible Bandwidth** – гибкий выбор полосы канала: 1.4, 3, 5, 10, 15, 20 МГц.

**Более широкий выбор частотного диапазона** для внедрения LTE: 700, 800, 900, 1800, 2100, 2300, 2600, 3500 МГц и др.

**OFDMA** технология радиодоступа.

**Три схемы модуляции QPSK, 16QAM, 64QAM.** Выбор необходимой схемы модуляции в зависимости от конкретных радиоусловий.

**Технология MIMO (Multiple Input Multiple Out)** – использование нескольких антенн для передачи данных.

**Carrier Aggregation** – технология агрегации частот для увеличения скорости передачи данных.

**All IP архитектура и отсутствие контролера.**



**Улучшение  
качественных и  
количественных  
показателей  
сетей нового  
поколения  
выдвигает и  
новые  
требования,  
связанные с  
повышением  
безопасности  
передаваемой  
информации.**



**Поскольку  
технология 4G  
полностью  
основана на  
протоколе IP, не  
превратятся ли  
мобильные сети в  
Интернет с  
присущими ему  
опасностями и  
проблемами?**



Два основных варианта технологий LTE:

- ✓ с дуплексным частотным разделением **LTE-FDD** (Frequency Division Duplex);
- ✓ и временным разделением **LTE-TDD** (Time Division Duplex).

Опора на множество различных технологий **затрудняет поиск уязвимостей в LTE**, что хорошо с точки зрения безопасности — взлом радиоканала для одних методов может сработать, а для других — нет.

В компании **Cisco** считают, что все угрозы безопасности передаваемой информации связаны именно с протоколом **IP**.



Для минимизации вреда наносимого в случае кражи информации о ключах из базовых станций разработаны специальные меры противодействия:

- ✓ проверка целостности устройства;
- ✓ взаимная аутентификация базовой станции оператора (выдача сертификатов);
- ✓ безопасные обновления;
- ✓ механизм контроля доступа;
- ✓ синхронизация времени;
- ✓ фильтрация трафика.

# Стандарт LTE выделяет пять основных групп безопасности:

- ✓ Архитектура безопасности сети должна обеспечить пользователей надежным доступом к сервисам и защиту от атак на интерфейсы.
- ✓ Сетевой уровень должен позволять узлам сети безопасно обмениваться как пользовательскими, так и управляющими данными и обеспечивать защиту от атак на проводные линии.
- ✓ Пользовательский уровень должен обеспечивать безопасный доступ к мобильному устройству.
- ✓ Уровень приложений должен гарантировать безопасный обмен сообщениями.
- ✓ Видимость и возможность изменения настроек безопасности должна позволять пользователю узнавать, обеспечивается ли безопасность и включать различные режимы.

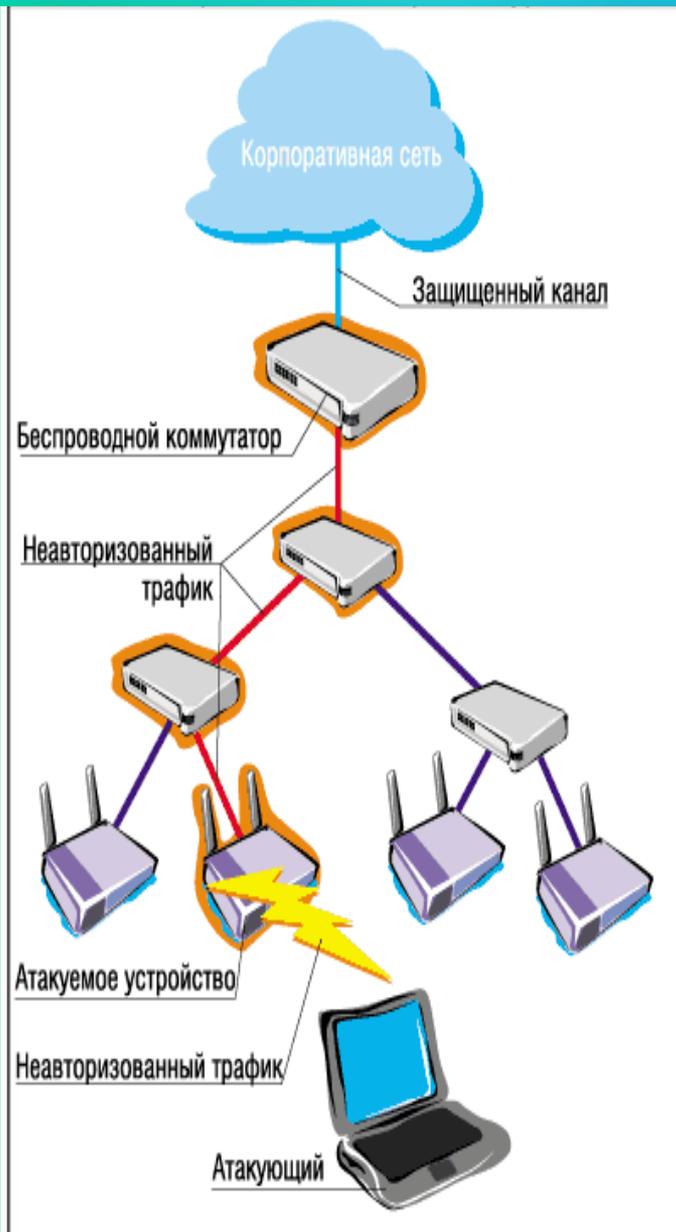


Вирусы на компьютерах стали делом обычным, троянцев для Android становится все больше, следовательно, внедрение высокоскоростного стандарта LTE может принести в мобильные средства связи все те угрозы, которые мы сейчас наблюдаем в ситуации с обычными компьютерами



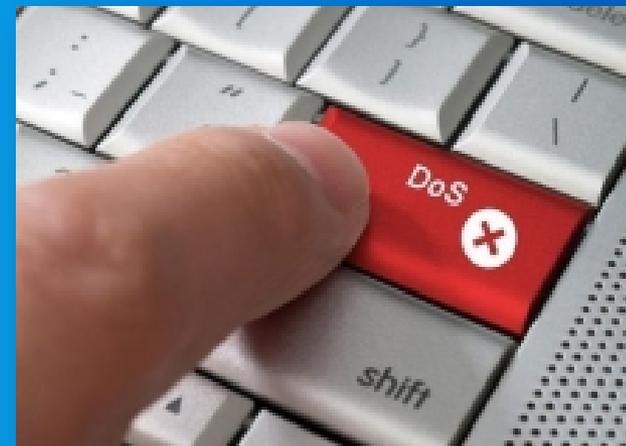
4G LTE





# Атаки DoS на сеть

Емкость радиоканала в LTE предполагается большая, но все же она имеет ограничения. Сетевые ресурсы базовой станции делятся между абонентами, и хотя есть ограничения для монополизации полосы отдельным пользователем, тем не менее, атака на отказ в обслуживании сети вполне возможна.



# Вирусные атаки

Хотя таким атакам подвержены устройства, а не сеть, **технология LTE увеличивает скорость распространения вредоносных программ,** поскольку сам этот стандарт является **высокоскоростным.**

# Атаки на дополнительные сервисы



**LTE** разрабатывалось не только для обеспечения доступа к Интернету мобильных пользователей, а скорее как платформа для внедрения новых услуг: видео, игровых и многих других.

Эти сервисы могут быть уязвимы для разнообразных атак — как из Интернета, так и из мобильной сети. Атаковав один из сервисов, злоумышленники смогут внедрить в клиентские устройства опасные программы.



Google



**Сервисы геопозиционирования**  
(Location-based service, **LBS**) можно  
использовать для слежки за абонентом,  
что создает опасность новых угроз.  
Поэтому сервисы на основе LBS можно  
назвать сервисами двойного назначения.



2010	2011	2012	2013	2014	2015	2016
HSPA 7.2/5.76 Mbps	HSPA 14.4/5.76 Mbps	HSPA 42.2/5.76 Mbps	HSPA 42.2/5.76 Mbps	HSPA 42.2/5.76 Mbps	HSPA 42.2/5.76 Mbps	HSPA 42.2/5.76 Mbps
					LTE Cat6 300/50 Mbps	LTE Cat9 450/50 Mbps

#### КОМПАС/GPS

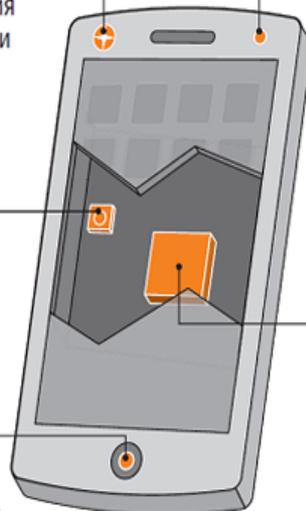
Точная информация о местонахождении может использоваться для планирования кражи

#### СЕНСОРЫ

Датчик движения распознает удары по клавиатуре ПК, рядом с которой лежит смартфон

#### МИКРОФОН

Через него можно незаметно прослушать разговоры



#### ВЕБ-КАМЕРА

Смартфон непрерывно поставляет изображения, из которых хакеры могут составить панораму

#### UMTS

Хакеры способны выяснить через подключение по 3G, в какой радиосоте находится смартфон в данный момент

A 3D white egg-shaped character with a large head, wearing a dark suit, white shirt, and blue tie. The character is leaning over a white rectangular sign, with its right hand pointing towards the text on the sign. The background is a dark blue and black space with glowing, swirling light trails in shades of blue and green, suggesting a futuristic or technological environment.

## Проблемы стандарта

- **Очень остро стоит задача взаимодействия с недоверенными (не LTE) сетями.**
- **Отсутствие обязательной аутентификации между ядром сети и базовой станцией.**

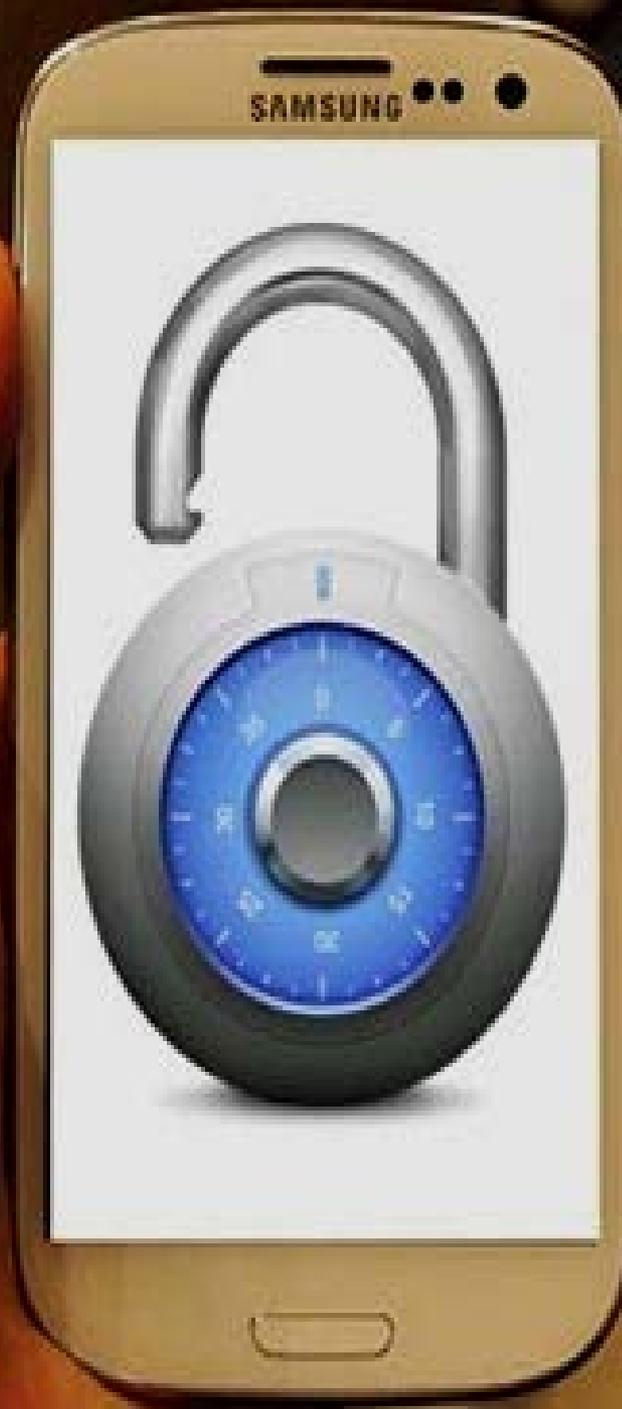
**Все функции защиты в LTE объединены стандартом и подразумевают защиту на нескольких уровнях:**

- ✓ на уровне доступа к сети;
- ✓ на уровнях сетевого и пользовательского доменов;
- ✓ на уровне приложений;
- ✓ на уровне отображения и конфигураций.

Технология LTE предусматривает использование не только IP-адреса, но и системы распространения ключей шифрования для всех устройств подключенных к сети, с возможностью перехода со 128 на 256-битные ключи и введения новых алгоритмов, сохраняя обратную совместимость.



**В LTE сохраняются и методы аутентификации пользователей по привязке к SIM карте, как в традиционной мобильной связи. Пользователь может заблокировать доступ к телефону по PIN-коду.**



**Специалисты по безопасности совместно с разработчиками LTE постоянно отслеживают появление новых угроз безопасности и предпринимают все необходимые шаги для обеспечения целостности и конфиденциальности передаваемых данных.**

## Какие принципиальные изменения принесет мобильная связь пятого поколения в нашу жизнь?

Полностью доработанная сеть 5G будет поддерживать обмен информации на скоростях, в сотни раз превышающих возможности 4G-сетей.

Новая технология позволит абонентам просматривать онлайн-контент, требующий подключения на больших скоростях, например, 3D-фильмы высокого разрешения, прямую трансляцию видео сверхвысокой четкости.

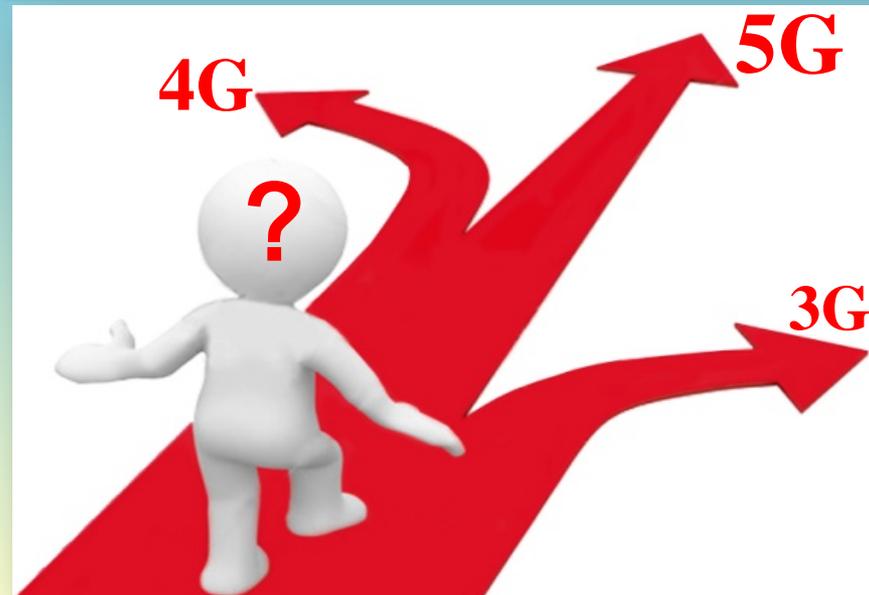
**Связь пятого поколения должна обеспечить инфраструктуру для автоматизированных аппаратов (например, в сфере межмашинного взаимодействия), подключенных к интернету автомобилей, беспилотных электрокаров, дистанционную медицину и многое другое.**



«Энергосообщество может служить примером платформы для развития цифрового сообщества и Украина является нашим первым и самым желанным партнером в этом направлении.

Нам нужна гигабайтная инфраструктура в последующие 5-10 лет, мы должны использовать спутниковую связь. Украина должна имплементировать 5G до 2020 года и прийти, таким образом, к общим стандартам с Европейским Союзом».

Эттингер убежден в том, что у Украины достаточно высокий потенциал в цифровых технологиях, и этот сектор экономики является первым, в котором можно достичь добавочной стоимости. Кроме того комиссар ЕС по вопросам цифровой экономики и общества подчеркнул, что в Украине **должны быть внедрены международные стандарты кибербезопасности.**





**СПАСИБО  
ЗА  
ВНИМАНИЕ!**