



Европейска  
комисия



# ИНСТРУМЕНТАРИУМ НА ЕС ЗА СИГУРНОСТТА В ОБЛАСТТА НА 5G

Набор от стабилни и всеобхватни мерки за координиран подход на ЕС за гарантиране на сигурността на 5G мрежи

Януари 2020 г.  
#Cybersecurity

## 5G: нова технология

Докато 3G технологиите дадоха възможност за мобилен интернет, а с 4G се появиха мобилните широколентови услуги, се очаква 5G да се превърне в инфраструктурата за свързаност, която ще проправи пътя за нови продукти и услуги и ще засегне всички сектори на обществото. Ползите ще включват:



### ЕЛЕКТРОННО ЗДРАВЕОПАЗВАНЕ

- Дистанционно наблюдение на здравето, медицински досиета и интелигентно диагностициране
- Използване на роботи за подпомагане на хирургите и подобряване на медицинските резултати



### ИНТЕЛИГЕНТНИ ЕНЕРГИЙНИ МРЕЖИ

- Високоэффективни електро-проводи и по-малко аварийни изключения в по-малък мащаб
- По-лесно внедряване с по-слабо въздействие върху околната среда



### ФАБРИКИ НА БЪДЕЩЕТО

- По-добър контрол върху чувствителни към фактора време вътрешни процеси
- Дистанционно контролиран достъп до складови съоръжения



### МЕДИИ & ЗАБАВЛЕНИЯ

- Подсилени зрителски преживявания като виртуалната реалност
- Свръхбързи широколентови приложения като видео стрийминг



### МОБИЛНОСТ

- Възможност за свързана и автоматизирана мобилност с цел пълно избягване на произшествията
- Възможност за свързаност при всички видове транспорт

Европа е един от най-развитите региони в света, що се отнася до въвеждането на 5G услуги с търговска цел, като инвестициите възлизат на 1 милиард евро, включително 300 милиона евро финансиране от ЕС. До края на тази година се очаква първите 5G услуги да станат достъпни в 138 европейски града.

## Киберсигурност на 5G: задължително предварително условие

5G мрежите са бъдещият гръбнак на нашите все по-цифровизирани икономики и общества. Засегнати са милиарди свързани предмети и системи, включително използваните в критични сектори като енергетиката, транспорта, банковото дело и здравеопазването, както и в системи за промишлен контрол, пренасящи чувствителна информация и подпомагащи системите за безопасност. Поради това гарантирането на киберсигурността и стабилността на 5G мрежите е от основно значение.

В същото време, поради по-малко централизираната си архитектура, интелигентната изчислителна мощност в периферията си, нуждата от повече антени и повишената си зависимост от софтуера, 5G мрежите предлагат повече потенциални входни точки за нападателите.

## График



## Инструментариум на ЕС за сигурността в областта на 5G

Въз основа на координираната оценка на риска на равнището на ЕС за сигурността на 5G мрежите, в инструментариума се излага набор от мерки за сигурност, които дават възможност за ефективно смекчаване на рисковете и за гарантиране на това, че в Европа се внедряват сигурни 5G мрежи. В него се определят подробни **планове за смекчаване** за всеки от установените рискове и се препоръчва набор от **ключови стратегически и технически мерки**, които следва да бъдат предприети от всички държави членки и/или от Комисията.



### СТРАТЕГИЧЕСКИ МЕРКИ

- Регулаторни правомощия
- Доставчици трети страни
- Диверсификация на доставчиците
- Устойчивост и разнообразие на веригата на доставки и на създаване на стойност в областта на 5G



### ТЕХНИЧЕСКИ МЕРКИ

- Сигурност на мрежата — основни мерки
- Сигурност на мрежата — специфични мерки за 5G
- Изисквания, свързани с процесите и оборудването на доставчиците
- Стабилност и приемственост

## Планове за смекчаване на риска

За всяка от деветте рискови области, определени в доклада за координираната оценка на риска на равнището на ЕС, в инструментариума са посочени и предвидени планове за смекчаване на риска. Те се състоят от възможна комбинация от мерки, основаващи се на тяхната ефективност.

## Заклучения относно инструментариума на ЕС: ключови мерки

**Държавите членки** следва да въведат мерки и да имат правомощия за смекчаване на рисковете. По-специално те следва да обърнат внимание на тези аспекти:

- укрепване на **изискванията за сигурност за операторите на мобилни мрежи**;
- оценяване на рисковия профил на доставчиците; прилагане на съответните ограничения за доставчиците, считани за високорискови, включително необходимите изключения за ключови активи;
- гарантиране на това, че всеки оператор разполага с подходяща **стратегия за използване на множество доставчици**, за да се **избегне** или **ограничи** всяка **съществена зависимост** от един-единствен доставчик и да се избегне зависимостта от доставчици, които се считат за високорискови.

**Европейската комисия** заедно с държавите членки следва да предприеме мерки за:

- поддържането на **разнообразна и устойчива верига на доставки в областта на 5G**, за да се избегне дългосрочната зависимост, включително чрез:
  - пълноценно използване на съществуващите средства и инструменти на ЕС (скрининг на преките чуждестранни инвестиции, инструменти за търговска защита, правила за конкуренцията);
  - по-нататъшно укрепване на капацитета на ЕС при технологиите за 5G и след 5G чрез използване на съответните програми и финансиране от ЕС;
- улесняване на координацията между държавите членки по отношение на **стандартизацията** за постигане на конкретни цели в областта на сигурността и разработване на съответни **схеми за сертифициране** в целия ЕС.

- Освен това мандатът на групата за сътрудничество за **МИС „Работен процес“** следва да бъде разширен, за да включи подкрепа, наблюдение и оценка на прилагането на инструментариума.

© Европейски съюз, 2020 г.

Повторната употреба е разрешена, при условие че се посочи източникът. Политиката относно повторната употреба на документи на Европейската комисия е уредена с Решение 2011/833/ЕС (ОВ L 330, 14.12.2011 г., стр. 39). За употребата или възпроизвеждането на елементи, които не са собственост на Европейския съюз, трябва да се поиска разрешение директно от носителите на авторските права.

Всички изображения © Европейски съюз, освен ако не е посочено друго.

Print ISBN 978-92-76-15577-5 doi:10.2775/392095 NA-03-20-052-BG-C

PDF ISBN 978-92-76-15562-1 doi:10.2775/554442 NA-03-20-052-BG-N