Урядовий офіс координації європейської та євроатлантичної інтеграції
Секретаріату Кабінету Міністрів України

Переклад затверджений

Державний експерт
Урядового офісу координації європейської та
євроатлантичної інтеграції
Секретаріату Кабінету Міністрів України — О. О. Шаповал
(найменування посади) (підпис) (ініціали та прізвище)

18 серпня 2021 р.

29.03.2019 UA Офіційний вісник Європейського Союзу L 88/42

РЕКОМЕНДАЦІЯ КОМІСІЇ (ЄС) 2019/534

від 26 березня 2019 року

щодо кібербезпеки мереж 5G

ЄВРОПЕЙСЬКА КОМІСІЯ,

беручи до уваги Договір про функціонування Європейського Союзу, зокрема його статтю 292,

Оскільки:

(1) Комісія визнала використання мережевих технологій п'ятого покоління (5G) основним рушієм майбутніх цифрових послуг та пріоритетом стратегії щодо Єдиного цифрового ринку. Комісія ухвалила План дій з розвитку мережі 5G з метою забезпечення конективності інфраструктури Союзу для її цифрової трансформації починаючи з 2020 року ([1]).

(2) Мережі 5G будуть побудовані на сучасних мережевих технологіях четвертого покоління (4G), при цьому вони запропонують нові сервісні можливості та стануть центральною ланкою інфраструктури і рушієм розвитку великої частини економіки Союзу. Одразу після впровадження мережі 5G стануть основою широкого діапазону послуг, необхідних для функціонування внутрішнього ринку та обслуговування і виконання надважливих соціально-економічних функцій, зокрема у сфері енергетики, транспорту, банківської діяльності, охорони здоров'я та промислових систем контролю. Організація демократичних процесів, таких як вибори, також дедалі більше спиратиметься на цифрову інфраструктуру та мережі 5G.

(3) Залежність багатьох критично важливих послуг від мереж 5G може мати особливо негативні наслідки в разі системного та широкомасштабного порушення їх роботи. Як результат, забезпечення кібербезпеки мереж 5G — це питання стратегічного значення для Союзу в часи дедалі частіших та більш витончених кібератак.

(4) Функціонування цифрової екосистеми ґрунтується на інфраструктурах взаємопов'язаної та транснаціональної природи, тож пов'язані з нею загрози мають транскордонний характер. Відповідно, виникнення в одній з держав-членів будь-яких значних вразливостей та/або інцидентів стосовно кібербезпеки мереж 5G матиме негативний вплив на Союз у цілому. Саме тому необхідно вжити заходів для підтримки загального високого рівня кібербезпеки мереж 5G.

(5) Держави-члени підтвердили потребу у вжитті заходів на рівні Союзу. У своїх висновках від 21 березня 2019 року Європейська Рада висловила сподівання щодо якомога скорішого

РЕКОМЕНДАЦІЯ КОМІСІЇ (ЄС) 2019/534

від 26 березня 2019 року

щодо кібербезпеки мереж 5G

ЄВРОПЕЙСЬКА КОМІСІЯ,

беручи до уваги Договір про функціонування Європейського Союзу, зокрема його статтю 292,

Оскільки:

(1) Комісія визнала використання мережевих технологій п'ятого покоління (5G) основним рушієм майбутніх цифрових послуг та пріоритетом стратегії щодо Єдиного цифрового ринку. Комісія ухвалила План дій з розвитку мережі 5G з метою забезпечення конективності інфраструктури Союзу для її цифрової трансформації починаючи з 2020 року ([1]).

(2) Мережі 5G будуть побудовані на сучасних мережевих технологіях четвертого покоління (4G), при цьому вони запропонують нові сервісні можливості та стануть центральною ланкою інфраструктури і рушієм розвитку великої частини економіки Союзу. Одразу після впровадження мережі 5G стануть основою широкого діапазону послуг, необхідних для функціонування внутрішнього ринку та обслуговування і виконання надважливих соціально-економічних функцій, зокрема у сфері енергетики, транспорту, банківської діяльності, охорони здоров'я та промислових систем контролю. Організація демократичних процесів, таких як вибори, також дедалі більше спиратиметься на цифрову інфраструктуру та мережі 5G.

(3) Залежність багатьох критично важливих послуг від мереж 5G може мати особливо негативні наслідки в разі системного та широкомасштабного порушення їх роботи. Як результат, забезпечення кібербезпеки мереж 5G — це питання стратегічного значення для Союзу в часи дедалі частіших та більш витончених кібератак.

(4) Функціонування цифрової екосистеми ґрунтується на інфраструктурах взаємопов'язаної та транснаціональної природи, тож пов'язані з нею загрози мають транскордонний характер. Відповідно, виникнення в одній з держав-членів будь-яких значних вразливостей та/або інцидентів стосовно кібербезпеки мереж 5G матиме негативний вплив на Союз у цілому. Саме тому необхідно вжити заходів для підтримки загального високого рівня кібербезпеки мереж 5G.

(5) Держави-члени підтвердили потребу у вжитті заходів на рівні Союзу. У своїх висновках від 21 березня 2019 року Європейська Рада висловила сподівання щодо якомога скорішого ухвалення рекомендації Комісії щодо узгодженого підходу до безпеки мереж 5G ([2]).

(6) Основною ціллю має залишатися забезпечення європейського суверенітету з повним дотриманням європейських цінностей відкритості та толерантності ([3]). Іноземні інвестиції у стратегічні сектори, придбання критичних активів, технологій та інфраструктури в Союзі, а також постачання критично важливого обладнання можуть також становити ризик для безпеки Союзу.

(7) У Спільному повідомленні «Стратегічна перспектива відносин ЄС та Китаю» кібербезпеку мереж 5G визнано основним елементом забезпечення стратегічної автономії Союзу ([4]).

(8) Резолюція Європейського Парламенту щодо загроз для безпеки, пов'язаних зі зростанням присутності китайських технологій у Союзі, також закликає Комісію та держави-члени вжити заходів на рівні Союзу ([5]).

(9) Ця Рекомендація охоплює питання ризиків кібербезпеки в мережах 5G та при цьому визначає вказівки щодо аналізу відповідних ризиків і заходів управління на національному рівні, розробки скоординованого оцінювання ризиків ЄС та формування процесу для розробки спільного інструментарію найкращих заходів з управління ризиками.

(10) Для захисту електронних комунікаційних мереж існують суворі законодавчі рамки Союзу.

(11) Рамки Союзу в сфері електронних комунікацій ([6]) покликані сприяти посиленню конкуренції, розвитку внутрішнього ринку та захисту інтересів кінцевих користувачів, а Європейський кодекс електронних комунікацій ([7]) переслідує як додаткову ціль забезпечення конективності, сформульовану такими результатами, як широкий доступ та впровадження фіксованого та мобільного зв'язку високої якості для всіх підприємств і громадян Союзу, з одночасним захистом інтересів громадян. Директива 2002/21/ЄС вимагає, щоб держави-члени забезпечили підтримку цілісності та безпеки комунікаційних мереж загального користування, при цьому з обов'язком забезпечення того, щоб суб'єкти господарювання, які надають комунікаційні мережі загального користування або публічно доступні електронні комунікаційні послуги, застосовували технічні та організаційні заходи для належного управління ризиками, що можуть виникати для безпеки мереж і послуг. Директива також передбачає наявність у компетентних національних регуляторних органів повноважень, включно з повноваженнями видавати обов'язкові до виконання інструкції, з метою забезпечення дотримання таких обов'язків.

(12) Крім того, Директива Європейського Парламенту і Ради 2002/20/ЄС ([8]) дозволяє державам-членам доповнювати умови загальної авторизації умовами стосовно захисту мереж загального користування від несанкціонованого доступу з метою захисту конфіденційності комунікацій відповідно до Директиви Європейського Парламенту і Ради 2002/58/ЄС ([9]).

(13) З метою підтримати виконання таких обов'язків, Союз створив низку відповідних органів для співпраці. Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), Комісія, держави-члени та національні регуляторні органи розробили для національних регуляторних органів технічні настанови зі звітування про інциденти, заходи безпеки, загрози та активи ([10]). Група співпраці, створена Директивою Європейського Парламенту і Ради (ЄС) 2016/1148 ([11]) («Група співпраці») об'єднує компетентні органи з метою підтримки та сприяння співпраці, зокрема шляхом надання стратегічних вказівок щодо діяльності мережі груп для реагування на інциденти в сфері комп'ютерної безпеки, що на технічному рівні сприяє оперативній співпраці.

(14) Майбутні європейські рамки сертифікації кібербезпеки ([12]) повинні стати важливим допоміжним інструментом для сприяння досягненню відповідного рівня безпеки. Вони також мають сприяти розвитку схем сертифікації кібербезпеки у відповідь на потреби користувачів програмного забезпечення та обладнання, пов'язаних із мережами 5G. Критична важливість цих інфраструктур повинна зробити першочерговим пріоритетом розвиток відповідних європейських схем сертифікації кібербезпеки для продуктів, послуг або процесів інформаційно-комунікаційних технологій, що використовуються для мереж 5G. Держави-члени та учасники ринку повинні брати активну участь у розвитку таких схем сертифікації, а також у забезпеченні підтримки у визначенні специфічних профілів захисту для мереж 5G.

(15) За відсутності згармонізованого права Союзу, держави-члени можуть визначити обов'язковість використання європейських схем сертифікації кібербезпеки через національні технічні регламентами, ухвалені відповідно до права Союзу. Держави-члени також можуть використовувати європейські схеми сертифікації кібербезпеки в контексті публічних закупівель та Директиви Європейського Парламенту і Ради 2014/24/ЄС ([13]), а також можуть підтримувати розвиток механізмів надання допомоги, наприклад, таких як хаб допомоги, для надання допомоги публічним покупцям під час закупівлі рішень щодо кібербезпеки.

(16) Високий рівень захисту даних та приватності є важливим елементом забезпечення безпеки мереж 5G. На рівні Союзу було також визначено правила для забезпечення безпеки опрацювання персональних даних, у тому числі при використанні засобів електронної комунікації. Загальний регламент про захист даних ([14]) встановлює зобов'язання щодо опрацювання персональних даних у спосіб, що забезпечує їх безпеку та запобігає несанкціонованому доступу або використанню персональних даних чи обладнання, яке використовується для їх опрацювання.

Директива про приватність та електронні комунікації встановлює спеціальні правила захисту конфіденційності комунікацій та термінального обладнання кінцевих користувачів. Директива також зобов'язує надавачів послуг вживати необхідних технічних та організаційних заходів для гарантування безпеки послуг, які вони надають.

(17) Союз також ухвалив документ, покликаний забезпечити захист критичної інфраструктури та технологій, подібних до тих, що використовуються у сфері комунікацій, дозволивши державам-членам перевіряти прямі іноземні інвестиції з підстав безпеки чи громадського порядку та створивши механізм співпраці, у рамках якого в держав-членів та Комісії буде можливість здійснювати обмін інформацією та висловлювати занепокоєння стосовно окремих інвестицій ([15]).

(18) Наразі держави-члени й оператори роблять важливі кроки для підготовки до широкомасштабного розгортання мереж 5G. Деякі держави-члени висловили занепокоєння щодо потенційних безпекових ризиків, пов'язаних із мережами 5G в контексті здійснення процедур з надання прав на користування смугами радіочастотного спектра для мереж 5G ([16]), та вже розпочали роботу з дослідження заходів, які могли б сприяти усуненню таких ризиків.

(19) При усуненні ризиків кібербезпеки в мережах 5G необхідно брати до уваги як технічні, так і інші фактори. До технічних факторів можна віднести вразливості кібербезпеки, що можуть використовуватися для отримання несанкціонованого доступу до інформації (кібершпіонаж з економічних чи політичних причин) або з іншими зловмисними намірами (кібератаки, спрямовані на пошкодження чи руйнування систем та даних). При цьому важливо враховувати такі аспекти, як потреба в захисті мереж протягом усього їхнього життєвого циклу та потреба в охопленні всього відповідного обладнання, зокрема, на етапах проектування, розробки, закупівлі, розгортання, функціонування та обслуговування мереж 5G.

(20) Інші важливі фактори можуть включати регуляторні чи інші вимоги до постачальників обладнання інформаційно-комунікаційних технологій. При оцінюванні важливості таких факторів потрібно враховувати, між іншим, загальний ризик впливу третьої країни, зокрема, з огляду на її модель врядування, відсутність угод про співпрацю в питаннях безпеки або подібних механізмів, таких як рішення про достатність, щодо захисту даних між Союзом та відповідною третьою країною, а також те, чи є ця країна учасницею багатосторонніх, міжнародних чи двосторонніх угод з питань кібербезпеки, боротьби з кіберзлочинністю або захисту даних.

(21) Як важливий крок під час розробки підходу Союзу до кібербезпеки в мережах 5G, на національному рівні необхідно здійснити та завершити оцінювання ризиків. Це допоможе державам-членам адаптувати національні заходи щодо безпекових вимог та управління ризиками з огляду на це оцінювання.

(22) Необхідно розвивати взаємодію з метою забезпечення ефективності заходів, спрямованих на усунення цих загроз кібербезпеки, заходів, необхідних для безперебійного функціонування внутрішнього ринку, та захисту персональних даних і приватності.

(23) Національні оцінювання ризиків повинні сформувати основу для скоординованого оцінювання ризиків Союзу з метою окреслення потенційних загроз та подальшого спільного огляду держав-членів у цій сфері за підтримки Комісії та Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA).

(24) Беручи до уваги національні оцінювання ризиків та оцінювання ризиків Союзу, Група співпраці повинна створити інструментарій заходів із визначенням типів ризиків кібербезпеки та можливих заходів з пом'якшення ризиків у сферах сертифікації, тестування та контролю доступу. Інструментарій заходів також повинен визначити можливі спеціальні заходи, необхідні для усунення ризиків, виявлених однією чи більше держав-членів. Група співпраці повинна покладатися на підтримку Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), Європолу, Органу європейських регуляторів електронних комунікацій (BEREC) та на Розвідувально-ситуаційний центр ЄС. Цей інструментарій заходів повинен слугувати для

Комісії як орієнтир для розробки мінімальних загальних вимог задля подальшого забезпечення високого рівня кібербезпеки мереж 5G на території всього Союзу.

(25) У разі побудови будь-якої єдиної мережі вжиття заходів з усунення ризиків кібербезпеки повинне враховувати сприяння кібербезпеці через диверсифікацію постачальників.

(26) Ця Рекомендація не обмежує компетенцій держав-членів щодо діяльності, пов'язаної з громадською безпекою, обороною, національною безпекою та діяльністю держави у сферах кримінального права, включаючи право держав-членів на заборону діяльності провайдерів та постачальників з міркувань національної безпеки.

УХВАЛИЛА ЦЮ РЕКОМЕНДАЦІЮ:

I. МЕТА

(1) Для підтримання розвитку підходу Союзу, спрямованого на забезпечення кібербезпеки мереж 5G, ця Рекомендація визначає заходи, яких необхідно вжити, для:

(a) здійснення державами-членами оцінювання ризиків кібербезпеки, що негативно впливають на мережі 5G, на національному рівні та вжиття необхідних заходів безпеки.

(b) спільної розробки державами-членами та відповідними установами, агентствами та іншими органами Союзу скоординованого оцінювання ризиків Союзу на основі національного оцінювання ризиків.

(c) створення Групи співпраці згідно з Директивою (ЄС) 2016/1148 (Група співпраці) для визначення можливого загального комплексу заходів, спрямованого на пом'якшення ризиків кібербезпеки, пов'язаних з інфраструктурою, що є основою для цифрової екосистеми, зокрема мереж 5G.

II. ТЕРМІНИ ТА ОЗНАЧЕННЯ

(2) Для цілей цієї Рекомендації:

(a) «мережі 5G» означає набір усіх відповідних елементів мережевої інфраструктури для технологій мобільного та бездротового зв'язку, що використовуються для надання послуг зв'язку та додаткових послуг з удосконаленими експлуатаційними характеристиками, такими як висока швидкість передачі даних та висока пропускна спроможність, зв'язок із низькою затримкою, дуже висока надійність або підтримка великої кількості під'єднаних пристроїв. Сюди також можна віднести елементи традиційних мереж, що ґрунтуються на попередніх поколіннях технологій мобільного та бездротового зв'язку, як-от 4G чи 3G. Мережі 5G слід сприймати як такі, що включають усі відповідні частини мережі.

(b) «інфраструктури в основі цифрової екосистеми» означає інфраструктури, що використовуються для забезпечення цифровізації широкого діапазону критично важливих застосунків в економіці та суспільстві.

III. ЗАХОДИ НА НАЦІОНАЛЬНОМУ РІВНІ

(3) До 30 червня 2019 року держави-члени повинні здійснити оцінювання ризиків інфраструктури мереж 5G, включно з визначенням найвразливіших елементів, у яких порушення безпеки матиме значний негативний вплив. До тієї самої дати держави-члени повинні також переглянути безпекові вимоги та методи управління ризиками, що застосовуються на національному рівні, щоб врахувати загрози кібербезпеці, що можуть бути викликані: (i) технічними чинниками, такими як специфічні технічні характеристики мереж 5G, або (ii) іншими чинниками, такими як правові чи політичні рамки, під які надавачі інформації та технологічного комунікаційного обладнання можуть підпадати у третіх країнах.

(4) На основі такого національного оцінювання ризиків, перегляду вживаних заходів та врахування наявних скоординованих заходів на рівні Союзу, держави-члени повинні:

(a) оновити безпекові вимоги та методи управління ризиками, що застосовуються до мереж 5G;

(b) оновити відповідні зобов'язання, накладені на суб'єкти господарювання, які надають комунікаційні мережі загального користування або публічно доступні електронні комунікаційні послуги згідно зі статтями 13a і 13b Директиви 2002/21/ЄС;

(c) доповнити вимоги для надання загальної авторизації вимогами стосовно захисту мереж загального користування від несанкціонованого доступу, та встановити як передумову відповідності суб'єктів господарювання, що будуть брати участь у будь-яких майбутніх процедурах з надання прав на користування радіочастотними смугами 5G, безпековим вимогам до мереж згідно з Директивою 2002/20/ЄС;

(d) вжити інших запобіжних заходів, спрямованих на пом'якшення потенційних ризиків кібербезпеки.

(5) Заходи, зазначені в пункті 4, повинні включати посилення зобов'язань з боку постачальників та операторів з метою забезпечення безпеки вразливих частин мереж, а також зобов'язань, у відповідних випадках, щодо надання відповідної інформації компетентним національним органам стосовно запланованих змін в електронних комунікаційних мережах або щодо вимог включення окремих компонентів інформаційних технологій та систем, які пройшли попереднє тестування в національних аудиторських або сертифікаційних лабораторіях на предмет безпеки та надійності.

(6) Дві або більше держав-членів повинні проводити спільні перевірки безпеки з використанням та обміном відповідними технічними експертними знаннями та засобами, пов'язаними з інфраструктурами в основі цифрової екосистеми та мереж 5G, наприклад, у разі ситуацій, коли один і той самий суб'єкт господарювання функціонує чи будує мережеву інфраструктуру більш ніж в одній державі-члені, або в разі схожості конфігурацій мережі. Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), Європол та Орган європейських регуляторів електронних комунікацій (BEREC) повинні в першочерговому порядку опрацьовувати запити держав-членів щодо підтримки в цій сфері. Результати таких перевірок повинні бути надіслані Групі співпраці та мережі груп для реагування на інциденти в сфері комп'ютерної безпеки.

IV. СКООРДИНОВАНІ ЗАХОДИ НА РІВНІ СОЮЗУ

(7) З метою забезпечення єдиного підходу до усунення ризиків кібербезпеки в мережах 5G, держави-члени повинні розпочати роботу в цьому напрямку діяльності в рамках Групи співпраці до 30 квітня 2019 року. Держави-члени повинні залучити до роботи у рамках Групи співпраці відповідні органи, якщо в цьому буде потреба.

Скоординоване оцінювання ризиків ЄС

(8) Держави-члени повинні обмінюватися інформацією між собою та з відповідними органами Союзу з метою формування загальної обізнаності щодо наявних та потенційних ризиків кібербезпеки, пов'язаних із мережами 5G.

(9) Держави-члени повинні передати свої національні оцінювання ризиків Комісії та Агентству Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) до 15 липня 2019 року.

(10) Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) повинне окреслити потенційні загрози для мереж 5G. Група співпраці та мережі груп для реагування на інциденти в сфері комп'ютерної безпеки повинні забезпечити підтримку цього процесу згідно з положеннями Директиви (ЄС) 2016/1148.

(11) Беручи до уваги всі ці елементи, до 1 жовтня 2019 року держави-члени за підтримки Комісії та разом з Агентством Європейського Союзу з питань мережевої та інформаційної безпеки

(ENISA) повинні виконати спільний загальноєвропейський огляд вразливості інфраструктур в основі цифрової екосистеми, зокрема, мереж 5G, перед потенційними ризиками.

(12) Цей спільний огляд повинен акцентувати увагу на аналізі ризиків, що стосуються особливо чутливих та вразливих елементів, які входять до складу основних елементів мереж 5G, операційних центрів та центрів технічного обслуговування, а також елементів доступу до мереж 5G, призначених для промислового застосування.

(13) На наступному етапі предмет цього спільного огляду повинен бути розширений для включення інших стратегічних елементів цифрового ланцюга доданої вартості.

Загальний інструментарій Союзу для усунення ризиків

(14) Група співпраці повинна визначити найкращі практики заходів для застосування на національному рівні, як передбачено в пункті 4. На основі таких національних найкращих практик заходів до 31 грудня 2019 року повинен бути розроблений інструментарій відповідних, ефективних та пропорційних заходів з управління ризиками задля пом'якшення визначених ризиків кібербезпеки на національному рівні та на рівні Союзу. Від слугуватиме як основа для розробки Комісією мінімальних загальних вимог для подальшого забезпечення високого рівня кібербезпеки мереж 5G по всьому Союзу.

(15) Інструментарій повинен включати:

(a) перелік типів ризиків безпеки, що можуть негативно впливати на кібербезпеку мереж 5G (зокрема ризики ланцюга постачання, ризики вразливості програмного забезпечення, ризики контролю доступу, а також ризики, що виникають з огляду на правові та політичні рамки, яких надавачі інформації та обладнання комунікаційних технологій можуть зазнавати у третіх країнах; та

(b) набір можливих заходів з пом'якшення ризиків (зокрема, стороння сертифікація апаратного та програмного забезпечення, послуг, офіційне тестування апаратного та програмного забезпечення або перевірки відповідності, процеси для підтвердження існування та здійснення контролю доступу, визначення продуктів, послуг та надавачів, що є потенційно ненадійними тощо). Ці заходи є необхідними для боротьби з кожним типом ризиків безпеки, виявлених в одній чи більше держав-членів у рамках оцінювання ризиків.

(16) Після розробки європейських схем сертифікації кібербезпеки, що стосуються мереж 5G, держави-члени повинні ухвалити, у відповідності до положень права Союзу, національні технічні регламенти, що передбачають обов'язкову сертифікацію інформаційно-комунікаційних технологічних продуктів, послуг чи систем, охоплених такими схемами.

(17) Держави-члени, разом із Комісією, повинні визначити умови щодо забезпечення безпеки мереж загального користування від несанкціонованого доступу, які повинні бути додатковими до умов загальної авторизації та безпекових вимог для мереж, метою яких повинно бути встановлення додаткових добровільних зобов'язань для суб'єктів господарювання, що беруть участь у процедурах надання прав на користування смугами радіочастотного спектра 5G згідно з Директивою 2002/20/ЄС. Такі умови повинні бути відображені, наскільки це можливо, у заходах, вжитих згідно з пунктом 4(c).

(18) Держави-члени повинні співпрацювати з Комісією для розробки спеціальних безпекових вимог, що можуть застосовуватися в контексті публічних закупівель, пов'язаних із мережами 5G. Така робота повинна охоплювати обов'язкові вимоги щодо реалізації схем сертифікації кібербезпеки при публічних закупівлях, оскільки такі схеми наразі не є обов'язковими для всіх постачальників, надавачів та операторів.

V. ПЕРЕГЛЯД

(19) Держави-члени співпрацюють з Комісією в підготовці оцінки впливу цієї Рекомендації до 1 жовтня 2020 року з метою визначення відповідних напрямків подальшої діяльності. Таке оцінювання повинне враховувати результати скоординованого оцінювання ризиків Союзу та інструментарію Союзу.

Вчинено у Страсбурзі 26 березня 2019 року.

За Комісію

Julian KING

Член Комісії

([1]) COM(2016)588 final.

([2]) Висновки Європейської Ради від 21 та 22 березня 2019 року.

([3]) Звернення 2018 року стосовно становища Союзу — «Година європейського суверенітету», 12 вересня 2018 року.

([4]) JOIN (2019) 5 final.

([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//EN.

([6]) Директива Європейського Парламенту і Ради 2002/21/ЄС від 07 березня 2002 року про спільні регулятивні рамки для електронних комунікаційних мереж та послуг (Рамкова директива) (ОВ L 108, 24.04.2002, с. 33) та спеціальні директиви.

([7]) Директива Європейського Парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій (ОВ L 321, 17.12.2018, с. 36).

([8]) Директива Європейського Парламенту і Ради 2002/20/ЄС від 07 березня 2002 року про авторизацію електронних комунікаційних мереж та послуг (Директива про авторизацію) (ОВ L 108, 24.04.2002, с. 21).

([9]) Директива Європейського Парламенту і Ради 2002/58/ЄС від 12 липня 2002 року про опрацювання персональних даних і захист приватності в секторі електронних комунікацій (Директива про приватність та електронні комунікації) (ОВ L 201, 31.07.2002, с. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 06 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (ОВ L 194, 19.07.2016, с. 1).

([12]) Пропозиція Регламенту Європейського Парламенту і Ради щодо Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA, Агентство з кібербезпеки), щодо скасування Регламенту (ЄС) № 526/2013, а також щодо сертифікації кібербезпеки інформаційно-комунікаційних технологій (Акт про кібербезпеку) (COM(2017) 477 final — 2017/0225 (COD).

([13]) Директива Європейського Парламенту і Ради 2014/24/ЄС від 26 лютого 2014 року про публічні закупівлі та про скасування Директиви 2004/18/ЄС (ОВ L 94, 28.03.2014, с. 65).

([14]) Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЕС (Загальний регламент про захист даних) (ОВ L 119, 04.05.2016, с. 1).

([15]) Регламент Європейського Парламенту і Ради (ЄС) № 2019/452 від 19 березня 2019 року про встановлення рамки для перевірки прямих іноземних інвестицій у Союз (ОВ L 79I, 21.03.2019, с. 1).

([16]) Процедура аукціону принаймні стосовно однієї смуги частот запланована на 2019 рік в 11 державах-членах: Австрії, Бельгії, Чехії, Франції, Німеччині, Греції, Угорщині, Ірландії, Нідерландах, Литві та Португалії. На 2020 рік заплановано шість інших аукціонів у: Іспанії, Мальті, Литві (щодо інших частот), Словаччині, Польщі та Сполученому Королівстві. Джерело: http://5gobservatory.eu/observatory-overview/observatory-reports/