

**ОГЛЯД ЗАКОНОДАВСТВА ЄС:
ТЕНДЕНЦІЇ У ПРАВОВОМУ
РЕГУЛЮВАННІ ЕЛЕКТРОННИХ
КОМУНІКАЦІЙ
(5G МЕРЕЖІ)**

Тараба Наталія

кандидат юридичних наук,
адвокатка

листопад 2021

ЗМІСТ

Коротке резюме.....	
Вступ та методологія.....	
1. Нормативне регулювання впровадження технології 5G у державах Європейського Союзу.....	
1.1. Публічно-приватні партнерства для тестування технології та основа для правового регулювання.....	
1.2. План дій 5G для Європи (5G Action Plan for Europe).....	
1.3. Європейський кодекс електронних комунікацій.....	
1.4. Рекомендація щодо посилення європейської з'єднаності (Connectivity Toolbox).....	
2. Нормативне регулювання кібербезпеки 5G мережі.....	
2.1. Визначення ризиків кібербезпеки 5G мереж.....	
2.2. Загальний ландшафт сучасних кіберзагроз та 5G мережа.....	
2.3. Заходи зі зменшення ризиків кібербезпеки 5G мереж.....	
ВИСНОВКИ.....	

Коротке резюме

Публічно-приватні партнерства у сфері 5G створюють необхідну базу для тестування, виявлення вразливостей, напрямів правового регулювання.

Розгортання 5G мереж потребує з боку держави прийняття ряду політичних рішень, таких як, визначення стратегії та основних цілей, вивільнення радіохвиль узгодженого спектру, визначення умов співпраці з приватним сектором, пошук джерел фінансування, розроблення нормативної бази.

Нормативною базою для розгортання 5G мереж залишається Європейський кодекс електронних комунікацій та Загальносоюзний Інструментарій кращих практик для забезпечення покриття, який було розроблено та схвалено державами-членами 25 березня 2021 року відповідно до рекомендації (EU) 2020/1307 від 18.09.2020. Процес їх імплементації у державах-членах ЄС все ще триває.

Розгортання 5G мереж, окрім безпрецедентних можливостей, обумовлює зростання існуючого рівня кіберзагроз і створює нові виклики. В процесі реалізації Інструментарію по зменшенню ризиків кібербезпеки мережі 5G держави-члени ЄС стикаються із наступними викликами:

- ✓ необхідність диференціації повноважень регулятора у розрізі різних суб'єктів (залежно від ризик-профілю) та об'єктів 5G мережі (залежно від вразливості об'єкта або сфери його використання);
- ✓ необхідність розроблення національної методології аудиту безпеки 5G мережі;
- ✓ необхідність розроблення методології оцінки ризик-профілю постачальників обладнання або програмного забезпечення для 5G мережі, встановлення для операторів мереж перехідного періоду у разі виявлення фактичної залежності від постачальника з високим ризик-профілем;
- ✓ визначення переліків вразливого обладнання та послуг для 5G мережі, які вимагають спеціального регулювання;
- ✓ визначення об'єктів критичної інфраструктури, які потребують спеціальних заходів безпеки у разі використання 5G технологій;
- ✓ розробка стратегії багатьох постачальників;
- ✓ складність стандартизації та сертифікації у сфері 5G технології, яка знаходиться у процесі розвитку.

Відповідно до експертних оцінок, створення законодавчої бази виявляється недостатнім для подолання практичних та безпекових викликів, пов'язаних із розгортанням 5G мереж. Натомість, особливе значення мають:

- ✓ розробка загальноєвропейських стандартів безпеки мереж;

- ✓ впровадження разом із новим законодавством технічних регламентів та методичних рекомендацій щодо його застосування;
- ✓ підвищення рівня співпраці між державним та приватним сектором, та також окремих регуляторів між собою;
- ✓ подолання нестачі експертів та матеріальних ресурсів для забезпечення безпеки 5G мережі та виконання регулятором своїх функцій;
- ✓ вдосконалення процедури повідомлення та розслідування інцидентів кібербезпеки.

Вступ та методологія

«5G – це не єдина бездротова технологія, а загальне визначення, яке використовують для класифікації бездротового зв'язку 5-го покоління, пропонуючи мережі, які в 100 разів швидше підтримують у 100 разів більше пристроїв і мають в п'ять разів меншу затримку», зазначається у статті Politico¹.

Як зазначив Міжнародний союз електрозв'язку², стандарт IMT-2020, відомий як технологія 5G, був винайдений Консорціумом розробників специфікації для мобільної телефонії 3GPP (The 3rd Generation Partnership Project).

Саме технологія 5G дозволить ефективно впровадження «Інтернету речей», віддаленні хірургічні втручання, медичний догляд, створення розумних міст, безпілотне управління автомобілями, безпілотні порти, електронне урядування, не говорячи вже про швидкість та якість самого Інтернет-зв'язку.

Україна також мала у планах розпочати впровадження технології 5G до кінця 2021 року. Однак, розпорядженням № 930-р від 4 серпня 2021 року³ Уряд вніс зміни до плану заходів щодо впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління, затвердженого розпорядженням Кабінету Міністрів України від 11 листопада 2020 р. № 1409⁴, відклавши до червня 2022 року проведення аукціону або конкурсу про надання в користування радіочастотного спектра з використанням радіотехнології мобільного зв'язку п'ятого покоління, та до серпня 2022 року відклавши надання операторам права на користування радіочастотним спектром з використанням радіотехнології мобільного зв'язку п'ятого покоління із застосуванням процедур аукціону або конкурсу.

¹5G EXPLAINED: HOW A NEW NETWORK OF TECHNOLOGIES IS SET TO TRANSFORM OUR WORLD:

<https://www.politico.com/sponsor-content/2018/11/5g-explained>

² Recommendation ITU-R M.2150-0 (02/2021) Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2020 (IMT-2020): https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2150-0-202102-1!!!PDF-E.pdf

³ <https://zakon.rada.gov.ua/laws/show/930-2021-%D1%80#n2>

⁴ <https://zakon.rada.gov.ua/laws/show/1409-2020-%D1%80#n9>

Незважаючи на те, що офіційне розгортання технології 5G в Україні було відкладено, тестування технології було розпочато вже 25 жовтня цього року⁵ з відкриттям тестової зони технології 5G - 5G Lab, яку було створено в результаті реалізації проекту Міністерства цифрової трансформації, Vodafone Україна, Huawei Ukraine та UNIT.City.

Оскільки Законом від 16.09.2014 № 1678-VII Україна ратифікувала Угоду про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, (далі – Угода про асоціацію), її зовнішньополітичний вектор був визначений. Угода про асоціацію поклала на Україну ряд обов'язків, серед яких імплементація до національної правової системи законодавчих актів ЄС у сфері телекомунікацій, в тому числі, нових⁶. І хоча Угода про асоціацію, враховуючи час її розробки та підписання, з об'єктивних причин не містить вимог щодо технології 5G, очевидно, що для України політика, практичні та регуляторні здобутки Європейського Союзу у сфері впровадження технології 5G будуть мати визначальне значення.

Проаналізовано порядок формування політики Європейського Союзу у галузі впровадження технології 5G, основні правові рішення та ступінь їх імплементації в окремих державах-членах Європейського Союзу.

Окрему увагу приділено питанням Загальносоюзний Інструментарію кращих практик для забезпечення покриття, який було розроблено та схвалено державами-членами 25 березня 2021 року відповідно до рекомендації (EU) 2020/1307 від 18.09.2020, та який може слугувати дороговказом щодо пріоритетних напрямів практичної та нормотворчої діяльності.

З урахуванням того, що впровадження 5G технологій та розгортання 5G мереж все більше оцінюється експертами як таке, що є викликом національної та загальноєвропейської безпеки та стабільності, досліджено також питання існуючого ландшафту кіберзагроз, специфічних кіберзагроз 5G мережі та інструментарію, який застосовується європейськими державами для їх попередження.

Приклади імплементації окремими країнами рекомендацій Європейської комісії в галузі розгортання 5G мереж та забезпечення їх безпеки, дозволяє скласти уявлення як про кращі практики такої імплементації, так і про існуючі виклики, які з усією очевидністю очікують і на Україну.

⁵ <https://thedigital.gov.ua/news/v-ukraini-zyavivsyia-innovatsiyniy-tekhnologichniy-maydanchik-pokritiy-merezheyu-5g-5g-lab>

⁶ Див.: Глава 14 Інформаційне суспільство: https://www.kmu.gov.ua/storage/app/sites/1/ugoda-pro-asociaciyu/TITLE_V.pdf; доповнення XVII-З «Правила, що застосовуються до телекомунікаційних послуг» Угоди про асоціацію: https://www.kmu.gov.ua/storage/app/sites/1/ugoda-pro-asociaciyu/17_Annexes.pdf

Інформація та висновки, які містяться в Огляді можуть бути використані:

- ✓ в процесі розробки та вдосконалення законодавства України з питань впровадження 5G технології,
- ✓ з метою підвищення інформованості споживачів, представників бізнесу, державних службовців з питань європейського досвіду впровадження 5G технологій;
- ✓ як основа для подальших досліджень законодавства Європейського Союзу.

1. Нормативне регулювання впровадження технології 5G у державах Європейського Союзу

1.1. Публічно-приватні партнерства для тестування технології та основа для правового регулювання

Однією з перших ініціатив щодо впровадження технології 5G у державах Європейського Союзу був проект METIS, який на консорціумній основі об'єднав декілька мобільних операторів, виробників обладнання, науково-дослідних установ для створення майбутнього концепту мобільного та бездротового зв'язку, який буде основою для цифрового суспільства⁷.

Більш визначним етапом стало укладення у грудні 2013 року Договору публічно-приватного партнерства у сфері 5G (5G PPP) між Європейською комісією, як представником публічного сектору, та Асоціацією 5G Інфраструктури, як представником приватного сектору, яка об'єднала різноманітних стейкхолдерів від індустрії, малого та середнього підприємництва, операторів мереж, дослідницьких, наукових та навчальних установ. Відповідно до Договору Європейська комісія взяла на себе зобов'язання з інвестування 5G проектів на суму 700 млн. євро. На першому етапі з 83 пропозицій було відібрано 19 проектів загальною вартістю 128 млн. Євро.

Метою цих проектів було, зокрема: визначити найбільш ефективні способи перехресно-доменного оркестрування послуг за наявності декількох адміністраторів, так само як і оркестрування декількох доменів за наявності одного адміністратора (5G-EXCHANGE); створити модель адаптивного та надійного мобільного 5G-зв'язку (5G NORMA); визначити технічні рішення та безпекові вимоги, які дозволяють надійну передачу чутливих даних: е-здоров'я, віддалена медична допомога, моніторинг стану здоров'я (CHARISMA); в режимі реального часу збирати «великі дані» роботи мереж 5G для створення алгоритмів, необхідних для адміністрування мережі,

⁷ "Challenges and Scenarios of the fifth Generation (5G) Wireless Communications System" (made by Dr. Afif Osseiran on November 15, 2013 at KTH, Stockholm) [https://metis2020.com/wp-content/uploads/presentations/W%40kth METIS overview scenarios 20131115 web.pdf](https://metis2020.com/wp-content/uploads/presentations/W%40kth%20METIS%20overview%20scenarios%2020131115%20web.pdf)

забезпечення її масштабування, стійкості та безпеки, недопущення несанкціонованого доступу (COGNET), тощо⁸.

1.2. План дій 5G для Європи (5G Action Plan for Europe)

Однак реальною точкою відліку з точки зору формулювання політики Європейського Союзу у сфері впровадження технології 5G став План дій 5G для Європи (5G Action Plan for Europe), розроблений та представлений Європейською комісією у 2016 році⁹.

В Плані дій 5G Європейська комісія визначила 8 основних напрямків, які вона прагнула реалізувати у співпраці із державами-членами:

- 1- вироблення графіку з метою одночасного розгортання технології 5G в державах-членах;
- 2- визначення нового спектру радіохвиль, необхідних для впровадження технології 5G;
- 3- визначення повного переліку спектру радіохвиль, які можуть бути використані для впровадження технології 5G (як нижче так і вище 6 ГГц) із закріпленням окремих вимог до користувачів хвиль вище 6 ГГц з урахуванням думки Органу європейських регуляторів електронних комунікацій ("BEREC") та Групи з питань радіоспектральної політики ("RSPG");
- 4- досягти до 2025 року наступних амбітних цілей:
 - всі важливі соціально-економічні установи, такі як школи, університети, дослідницькі центри, перевізники, надавачі публічних послуг, адміністрації, підприємства, діяльність яких спирається на цифрові технології, повинні мати доступ до надшвидкісного гігабіт-зв'язку (який дозволяє користувачам завантажувати 1 гігабіт даних в секунду);
 - усі домогосподарства повинні мати доступ до з'єднання, яке дозволяє завантажувати не менше 100 мегабіт даних в секунду з можливістю апгрейду до 1 гігабіт в секунду;
 - усі міста та основні автомобільні та залізничні шляхи повинні мати безперервне 5G покриття.
- 5- забезпечити доступність стандартів для початкового розгортання мережі 5G та їх подальшу цілісну розробку, залучати держави до участі у міжнародних та міжіндустріальних партнерствах з метою тестування мережі 5G та створення умов для діджиталізації індустрії;

⁸ Більш детально див.: The5G Infrastructure Public Private Partnership (5G PPP): <https://5g-ppp.eu/wp-content/uploads/2015/10/5GPPP-brochure-final-web.pdf>

⁹ 5G for Europe: An Action Plan:

file:///C:/Users/Admin/Downloads/com_2016_588_f1_communication_from_commission_to_inst_en_v4_p1_860_526_17131.pdf

- 6- прискорити проведення ключових експериментів з використанням можливостей зв'язку технології 5G;
- 7- обмірковувати потенційні можливості технології 5G у сфері публічних послуг;
- 8- працювати у напрямку створення публічно-приватного партнерства за рахунок як коштів приватного сектору, так і європейських фінансових організацій, з метою впровадження та тестування технології 5G.

Стратегія Європейської комісії в подальшому була схвалена рішенням Європейського Парламенту «Інтернет-з'єднання для зростання, конкурентоспроможності та об'єднання: Європейське гігабіт суспільство та 5G від 1 червня 2017 року¹⁰.

Також з метою вирішення питання звільнення радіохвиль необхідного спектру для надання їх у користування операторам майбутньої мережі 5G, було прийнято рішення Європейського парламенту та Ради Європи від 17 травня 2017 року щодо використання радіохвиль частотою 470–970 МГц¹¹.

Основні вимоги, зафіксовані у цьому рішенні були наступні:

- до 30 червня 2020 року держави-члени повинні були дозволити використання частот the 694-790 МГц («700 МГц») для встановлення бездротового електронного зв'язку у відповідності до гармонізованих технічних вимог, встановлених статтею 4 Рішення No 676/2002/ЕС¹²;
- вирішити при цьому питання дотримання прав споживачів організацій телерадіомовлення, які традиційно використовували вказані частоти, забезпечити їх релокацію.

Необхідним вбачається згадати також Талліннську міністерську декларацію від 18 липня 2017 року, якою міністри європейських держав, відповідальні за телекомунікації, виразили свою готовність вирішувати основні виклики на шляху впровадження технології 5G, зокрема:

- на передбачуваних, зрозумілих, недискримінаційних умовах надати операторам доступ до необхідних радіочастот,
- визначити пріоритетними для впровадження технології 5G великі міста та магістральні шляхи,

¹⁰ European Parliament resolution of 1 June 2017 on internet connectivity for growth, competitiveness and cohesion: European gigabit society and 5G (2016/2305(INI)): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0234>

¹¹ Decision (EU) 2017/899 of the European Parliament and of the Council of 17 May 2017 on the use of the 470-790 MHz frequency band in the Union: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017D0899&qid=1636039938881>

¹² Відповідно до п.3 цього рішення, при використанні радіозв'язку держави-члени повинні керуватися роботами Міжнародного союзу електрозв'язку та Європейської конференції адміністрацій поштової служби та служби зв'язку: Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002D0676&qid=1636044609338>

- визнати пріоритетом інтероперабельність мереж 5G різних держав-членів та провідну роль загальноєвропейської стандартизації для вирішення цього виклику;
- сприяти проведенню оптоволоконних мереж;
- підтримувати встановлення «малих сот», які потребують безперешкодного доступу до об'єктів інфраструктури та нерухомості;
- підтримувати стратегічний діалог.

1.3. *Європейський кодекс електронних комунікацій*

З метою гармонізації в ЄС правового регулювання електронних комунікаційних мереж, електронних комунікаційних послуг, пов'язаних засобів та пов'язаних послуг, а також деяких аспектів термінального обладнання, Європейським Парламентом та Радою Європи було прийнято Директиву (ЄС) 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій¹³ (далі – ЕСЕС).

В частині створення умов для розгортання та використання 5G мережі слід відзначити наступні положення та принципи, запроваджені ЕСЕС:

- визначено поняття «мережі надвисокої пропускної здатності» (стаття 2);
- держави-члени повинні сприяти підключенню і доступу до мереж надвисокої пропускної здатності, забезпечуючи при цьому:
 - регуляторну передбачуваність;
 - відсутність дискримінації;
 - технологічну нейтральність;
 - врахування умов інфраструктури, конкуренції, географічного району;
 - високого загального рівня захисту для кінцевих користувачів;
 - вибір та рівноцінний доступ для кінцевих користувачів з інвалідністю;
- держави-члени повинні забезпечити максимальне врахування настанов, висновків, рекомендацій, спільних позицій, кращих практик та методології, затверджених BEREC, а також наявність у національних регуляторних органів адекватних фінансових та кадрових ресурсів, які дозволяли б їм брати активну участь у діяльності BEREC та робити свій внесок до неї;
- національні регуляторні та/або інші компетентні органи мають провести географічний огляд територіального охоплення електронних комунікаційних мереж, здатних забезпечувати широкосмуговий доступ

¹³ DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code (Recast): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972&qid=1636117646124>

до 21 грудня 2023 року та вживати заходи для відкритого використання даних та розвитку таких мереж;

- національні регуляторні органи можуть, за обґрунтованим зверненням, накладати зобов'язання щодо надання доступу до електропроводки, кабелів та пов'язаних з ними засобів у будівлях або до першої точки концентрації чи розподілу, що визначається національним регуляторним органом, якщо така точка знаходиться поза межами будівлі;
- держави-члени та їхні компетентні органи повинні забезпечити, щоб використання радіочастотного спектра було організовано на їхній території таким чином, щоб не перешкоджати жодній іншій державі-члену дозволяти використання на її території гармонізованого радіочастотного спектра відповідно до права Союзу, зокрема через транскордонні шкідливі завади між державами-членами;
- з цією метою підтверджена необхідність і надалі дотримуватись Регламенту радіозв'язку МСЕ та регіональних угод МСЕ;
- закріплено процедуру спільного відбору користувача радіочастотного спектру;
- передбачено послідовне впровадження державами-членами процедур, стандартів та специфікацій, затверджених європейськими організаціями стандартизації (Європейський комітет зі стандартизації (CEN), Європейський комітет зі стандартизації в електротехніці (Cenelec) та Європейський інститут телекомунікаційних стандартів (ETSI)), а за відсутності опублікованих європейських стандартів або специфікацій, держави-члени повинні заохочувати імплементацію міжнародних стандартів або рекомендацій, ухвалених Міжнародним союзом електрозв'язку (МСЕ), Європейською конференцією адміністрацій зв'язку (СЕРТ), Міжнародною організацією зі стандартизації (КО) та Міжнародною електротехнічною комісією (ІЕС);
- передбачено обов'язковість повідомлення національного регулятора про інциденти безпеки та надання регулятором щорічних звітів до Комісії та ENISA про одержані повідомлення та вжиті заходи;
- держави-члени повинні забезпечити право регулятора вимагати від операторів телекомунікаційних мереж (а) надавати інформацію, необхідну для оцінювання безпеки їхніх мереж і послуг, включаючи задокументовані правила безпеки; та (б) проводити незалежний аудит безпеки телекомунікаційних мереж.

Разом з тим, деякі дослідники надають ЕСЕС, зокрема, та методам м'якого регулювання Європейською комісією питань впровадження 5G, взагалі, стримані оцінки, оскільки він надає можливість державам-членам

встановлювати власні регуляторні правила, які можуть відрізнятися¹⁴. Відтак, мета ЕСЕС може бути не досягнута в повній мірі.

Інша проблема, яка перешкоджає повноцінному впровадженню ЕСЕС на території Європейського Союзу, полягає в тому, що із таким впровадженням зволікають самі держави-члени.

Відповідно до ЕСЕС, держави-члени повинні були завершити процедури його імплементації у власне законодавство не пізніше 21 грудня 2020 року. З усіх держав ЄС дедлайну дотримались лише Греція, Угорщина та Фінляндія. У відповідь Європейська комісія у лютому 2021 року навіть ініціювала процедуру встановлення факту порушення відносно інших 24 держав ЄС¹⁵. Однак станом на 23 вересня 2021 року 19 держав-членів (Естонія, Іспанія, Хорватія, Ірландія, Італія, Кіпр, Латвія, Литва, Люксембург, Мальта, Нідерланди, Австрія, Польща, Португалія, Румунія, Словенія, Словаччина та Швеція) так і не повідомили Європейську комісію про виконання процедури імплементації ЕСЕС¹⁶.

Таким чином, станом на листопад 2021 року тільки 9 держав ЄС (Бельгія, Болгарія, Греція, Данія, Німеччина, Угорщина, Франція, Фінляндія, Чехія) імплементували ЕСЕС.

1.4. Рекомендація щодо посилення європейської з'єднаності

Наступним регулівним кроком стало прийняття Європейською комісією рекомендації (EU) 2020/1307 від 18.09.2020 про запровадження загального союзного інструментарію для зменшення вартості розгортання надшвидкісних мереж та забезпечення доброзичливого середовища для оперативного доступу до 5G радіоспектру (Connectivity Toolbox).

Метою Рекомендації (EU) 2020/1307 було з одного боку запропонувати державам-членам низку заходів, які на переконання Комісії, мають сприяти більш швидкому розгортанню 5G мереж, а з іншого, - започаткувати спільну роботу держав-членів в рамках Спеціальної групи з'єднання (Connectivity Special Group). Така спільна робота передбачала збір інформації та оцінку поточного стану регулювання у державах-членах¹⁷ з метою розробки та

¹⁴ Margarita Robles-Carrillo. European Union policy on 5G: Context, scope and limits: Telecommunications Policy Volume 45, Issue 8, September 2021, 102216 /

<https://www.sciencedirect.com/science/article/pii/S0308596121001208#fn52>

¹⁵ Commission opens infringement procedures against 24 Member States for not transposing new EU telecom rules: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_206

¹⁶ EU Electronic Communications Code: Commission calls on Member States to fully transpose new telecom rules into national law: <https://digital-strategy.ec.europa.eu/en/news/eu-electronic-communications-code-commission-calls-member-states-fully-transpose-new-telecom-rules>

¹⁷ Див.: Summary Report of Best Practices Outcome of phase 1 of the work of the Special Group for developing a common Union Toolbox for connectivity 16/10/2020-20/12/2020: <https://digital-strategy.ec.europa.eu/en/news/eu-member-states-present-report-best-practices-fast-network-rollout-first-step-towards-connectivity>

погодження Загальносоюзного Інструментарію на виконання Рекомендації (EU) 2020/1307.

Загальносоюзний Інструментарій кращих практик з покращення покриття було схвалено державами-членами 25 березня 2021 року¹⁸. Найкращими рекомендованими практиками було визнано наступні:

1) у сфері оптимізації процесу видачі ліцензій на використання радіохвиль:

- ✓ використання електронної комунікації під час видачі ліцензій, зокрема, запровадження «єдиного вікна» - порталу, через який заявник зможе комунікувати з державними органами щодо видачі всіх необхідних дозволів для прокладання мереж¹⁹;
- ✓ запровадження виключень та скорочених строків; при цьому, місцеві органи повинні максимально використовувати можливості існуючого законодавства (а не тільки очікувати прийняття нового) для надання необхідних дозволів на виключних умовах²⁰;
- ✓ розробка модельного нормативного регулювання, планів та інструкцій для органів влади, які здійснюють видачу дозволів на розгортання/прокладання мереж (особливо в ситуаціях, коли для видачі дозволів залучаються різні органи влади);
- ✓ проведення навчальних заходів для державних службовців з метою вивчення законодавства у сфері телекомунікацій та ознайомлення із засобами пришвидшення процесу надання дозволів;
- ✓ надання права проходу для прокладання мереж за принципом мовчазної згоди, якщо протягом 3 місяців не надано відповідь на заявку оператора (правило застосовується до об'єктів державної та комунальної власності та до випадків, які не зачіпають питання безпеки, дозволи на будівництво і т.ін.);
- ✓ призначення у складі регуляторних органів осіб зі специфічними функціями – координаторів широкосмугового доступу;
- ✓ запровадження спільного підготовчого процесу та проведення спільних нарад між оператором та усіма суб'єктами, дозволи яких є необхідними для прокладання мереж;
- ✓ політика ціноутворення при видачі дозволів та ліцензій операторам широкосмугового доступу повинна бути прозорою, раціональною недискримінаційною;

¹⁸ Common Union Toolbox for Connectivity: <https://digital-strategy.ec.europa.eu/en/news/connectivity-toolbox-member-states-agree-best-practices-boost-timely-deployment-5g-and-fibre>

¹⁹ Наразі більшість держав-членів звітували про індивідуальний характер комунікації та необхідність персоналізації при спілкуванні з кожним окремим державним органом та різних державних та регіональних органів між собою, що не сприяє меті досягнення швидкого розгортання мереж та покращення покриття. Там же: Р.10-11;

²⁰ Там же: Р.7

- 2) *у сфері посилення прозорості процесу надання дозволів та прокладання мереж* шляхом забезпечення наявності в електронній формі на єдиному інформаційному ресурсі всієї необхідної інформації щодо:
- ✓ існуючих об'єктів інфраструктури з прив'язкою до місцевості;
 - ✓ запланованих робіт з прокладання мереж з прив'язкою до місцевості
 - ✓ завантаженості об'єктів інфраструктури та/або наявності прокладених оптоволоконних мереж;
 - ✓ умов доступу до об'єктів інфраструктури
- 3) *у сфері розширення доступу до об'єктів інфраструктури:*
- ✓ забезпечити надання доступу до усіх публічних об'єктів інфраструктури, які можуть бути використані з метою прокладання/розгортання телекомунікаційних мереж;
 - ✓ призначати державний орган, який буде просувати та координувати доступ операторів до публічних об'єктів інфраструктури;
 - ✓ розробляти методичні рекомендації, типові умови, договори, стандарти з метою використання публічних об'єктів інфраструктури з метою прокладання/розгортання телекомунікаційних мереж;
- 4) *у сфері врегулювання конфліктів:*
- ✓ закріплення обов'язковості процедури медіації;
 - ✓ розроблення методичних рекомендацій, в тому числі щодо діяльності відповідного суб'єкта медіації, плати за його послуги, правил медіації;
 - ✓ доступність процедури медіації в електронній формі;
- 5) *у сфері зменшення впливу на навколишнє середовище:*
- ✓ ініціювання відповідних досліджень для оцінки такого впливу та реагування на виклики по мірі потреби;
 - ✓ виконання вимог існуючих регуляторних актів Європейського Союзу в тих випадках та обсягах, в яких їх норми можуть бути застосовані до нових технологій;
- 6) *у сфері стимулювання інвестицій у галузь телекомунікацій:*
- ✓ впроваджувати методики обґрунтованих розрахунків ціни ліцензій на використання радіохвиль, уникати максимізації цін;
 - ✓ на підставі індивідуального підходу забезпечити доступність радіохвиль узгодженого спектру для розгортання 5G мереж;
 - ✓ переглядати національні плани використання радіоспектру на регулярній основі;
 - ✓ надавати відстрочки та розстрочки операторам для сплати обов'язкових платежів за видачу дозволів та ліцензій;
 - ✓ запровадження гнучких механізмів авторизації для використання радіохвиль спектру 24.25-27.5 ГГц та спільного використання об'єктів інфраструктури операторами;
 - ✓ поєднання фінансових стимулів з покладенням обов'язків щодо належного покриття;

- ✓ використання європейських програм фінансової допомоги для розгортання 5G мереж;
- 7) *у сфері міждержавної координації для індустріального транскордонного використання 5G мереж:*
 - ✓ подальша гармонізація на базі ЕСЕС, оскільки індустрії ще не звертались із відповідними запитами²¹;
 - ✓ забезпечити інтеоперабельність через розробку та впровадження єдиних стандартів;
 - ✓ відстежувати особливості використання радіоспектру у транскордонному аспекті;
- 8) *у сфері охорони здоров'я та захисту від впливу електромагнітного поля:*
 - ✓ ініціювати та впроваджувати відповідні наукові дослідження на регулярній основі, особливо, в частині випромінювання станцій для 5G технологій;
 - ✓ вести роз'яснювальну роботу та суспільний діалог, побудований на реальних фактах та доказах, тощо.

Як і сама Рекомендація (EU) 2020/1307, Загальносоюзний Інструментарій не має для держав-членів обов'язкового характеру і кожна держава самостійно визначає доцільність та способи впровадження запропонованих заходів. Дорожні карти щодо виконання Загальносоюзного Інструментарію були надані державами-членами у квітні 2021 року²².

Відповідно до дорожніх карт, держави-члени звітували про наступні способи імплементації Інструментарію.

Щодо питання запровадження системи виключень та спеціальних скорочених процедур для надання ліцензій у сфері широкосмугового доступу, а також створення єдиного веб-порталу для ліцензування усіх процесів розгортання мереж в Австрії знаходиться на рівні національної дискусії²³. В галузі модельного регулювання: національний регулятор Австрії видав методичні рекомендації щодо планування території, надання права проходу для прокладання мереж, а також наказ про виплату компенсацій за використання права проходу. Забезпечення стейкхолдерів інформацією здійснюється в межах Платформи Інтернет-інфраструктура Австрії 2030. Інформація доступна, у найближчий час буде геологована, однак дублювання її на єдиному порталі вбачається недоцільним. Принцип мовчазної згоди не

²¹ Там же: P.36

²² Connectivity Toolbox: Member States develop and share roadmaps for the Toolbox implementation: <https://digital-strategy.ec.europa.eu/en/library/connectivity-toolbox-member-states-develop-and-share-roadmaps-toolbox-implementation>

²³ Connectivity Toolbox: Information on National Roadmap Austria: P.2: <https://digital-strategy.ec.europa.eu/en/library/connectivity-toolbox-member-states-develop-and-share-roadmaps-toolbox-implementation>

передбачений законом. Також не вбачається можливим спільна підготовка та координація процесів надання дозволів.

Естонія звітувала про фактичне врегулювання на рівні закону таких питань, як виключення для надання дозволів для прокладання мереж до існуючої інфраструктури, справедлива плата за одержання дозволів та ліцензій, можливість покладення на операторів зобов'язань щодо покриття та спільного використання об'єктів інфраструктури. Будівельний кодекс регулює питання медіації при вирішенні спорів у галузі прокладання мереж. Функції єдиного адміністративного та інформаційного веб-порталу виконує реєстр нерухомості (Registry of Building) і його функції можуть бути розширені за потреби. Також Естонія повідомила про імплементацію технічних умов, розроблених Європейською конференцією поштових та телекомунікаційних адміністрацій (CEPT) та Комітетом електронних комунікацій (ECC). Протягом 2021 – 2022 років планується проведення аукціонів щодо надання у користування радіохвиль спектру 700 МГц та 3.5 ГГц. Надавати у користування радіохвилі спектру 24.25-27.5 ГГц планується в першу чергу для публічних потреб, але частина спектру буде також зарезервована і для приватних осіб.

При цьому, частина заходів (розробка методичних рекомендацій, проведення навчальних заходів, застосування принципу мовчазної згоди при наданні права проходу, виконанні робіт, координація процесу надання дозволів між різними суб'єктами владних повноважень) передана на розсуд органів місцевого самоврядування.

У Латвії встановлення системи виключень та пришвидшення процесу видачі дозволів на виконання робіт з прокладання мереж передбачено рішеннями Кабінету Міністрів про внесення змін до Загальних правил забудови та Закону про надшвидкісні електронно-комунікаційні мережі. Інформаційне забезпечення здійснюється через портал Latvija.lv, який містить перехресні посилання на інші необхідні ресурси, зокрема, Інформаційну систему будівництва (Construction information system - BIS). Принцип мовчазної згоди законом не передбачено, які і скорочені процедури для надання права проходу. Закону про надшвидкісні електронно-комунікаційні мережі передбачає надання геолокованої інформації через єдиний інформаційний портал, однак межі доступу до такої інформації у процесі визначення, з огляду на дотримання вимог безпеки. Полегшений доступ до об'єктів інфраструктури з метою встановлення малих сот планується передбачити у новому Законі про електронні комунікації. Дотримання нормативів електромагнітного випромінювання є умовою для встановлення будь-якого телекомунікаційного обладнання. Гармонізовані технічні умови та

регламенти імплементуються шляхом затвердження національного плану використання радіоспектру, який переглядається щорічно.

У Литві для встановлення мобільного телекомунікаційного обладнання не вимагаються жодні дозволи, а прокладання мереж в дорожній мережі здійснюється без внесення будь-якої плати. Не планується спрощення процесу встановлення антен, який вимагає наразі авторизації та оцінюється як цілком пропорційним, з точки зору часу та умов надання. Одержання дозволів здійснюється через інформаційні портали «Infostatyba» (<https://www.planuojustatau.lt>) та централізований порта е-послуг <https://www.epaslaugos.lt/portal>. Підготовлена до впровадження нова вебсистема для надання геолокованої інформації «Territories planning and construction gates», роботу якої планується розпочати з прийняттям відповідного законодавства. Створення координаційних центрів не вбачається необхідним з огляду на індивідуальний підхід в процесі надання доступу до об'єктів публічної інфраструктури. Національний регулятор наділений широкими повноваженнями у сфері медіації, однак Литва звітує про фактичну відсутність ситуацій, які би вимагали її втручання.

У Фінляндії процедури спрощеного та пришвидшеного надання дозволів знаходяться у процесі дискусії. Національний регулятор TRAFICOM реалізує функцію модельного регулювання, затверджує правила проведення робіт зі встановлення мережевого обладнання, надання телекомунікаційних послуг, тощо, супроводжує такі правила відповідними роз'ясненнями щодо застосування. До 2023 року планує перевести надання усіх публічних послуг в електронну форму. Надання права проходу реалізується у випадках та порядку, передбачених Законом про дороги, за принципом повідомлення (тобто, фактично, за мовчазною згодою). Функціонування єдиного інформаційного порталу планується на базі порталу Lupapiste.fi, яким користується 195 з 310 муніципалітетів.

Отже, впровадження Загальносоюзного Інструментарію для покращення Інтернет-покриття триває, а більш завершену інформацію можна буде отримати після надання державами-членами звітів про імплементацію, дедлайн для яких встановлено до 30 квітня 2022 року.

2. Забезпечення кібербезпеки 5G мережі

Не буде перебільшенням стверджувати, що якщо на початку шляху впровадження технології 5G у державах Європейського Союзу, більше уваги приділялося питанням інфраструктури, звільнення та виділення необхідних діапазонів радіочастот, пошук моделей та джерел фінансування для розгортання мережі 5G, то в останні роки на вістрі дискусії знаходиться

питання національної та загальноєвропейської стратегії кібербезпеки в умовах гігабіт суспільства.

2.1. Визначення ризиків кібербезпеки 5G мереж.

З метою регулювання цього питання Європейською комісією 26 березня 2019 року була затверджена Рекомендація 2019/534 по кібербезпеці 5G мереж²⁴, яка зобов'язала держави-члени вжити ряд заходів з оцінки ризиків кібербезпеки та вироблення кращих практик захисту з метою управління такими ризиками на національному рівні та на рівні ЄС.

Серед іншого, у Рекомендації 2019/534 було визначено 5G мережу як сукупність відповідних елементів інфраструктури для мобільного та бездротового зв'язку, який використовується для з'єднання та додаткових видів обслуговування з характеристиками виконання нового покоління, такими як спроможність передавати надзвичайно великі обсяги даних за короткий час, низька затримка комунікації, висока надійність, підтримка великої кількості з'єднаних пристроїв. Така мережа може включати елементи мобільного та бездротового зв'язку попередніх поколінь телекомунікаційних технологій, таких як 4G або 3G. 5G мережа повинна розумітися як така, що включає усі елементи, які забезпечують її існування.

У липні 2019 року держави-члени надали результати оцінки ризиків, викладені у формі анкети, до Комісії та Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA). За результатами опрацювання цих анкет та за підтримки ENISA державами-членами 9 жовтня 2019 року було опубліковано Звіт щодо проведеної за ініціативою Європейського Співтовариства оцінки ризиків кібербезпеки у мережах 5G²⁵.

У Звіті звертається увага на якісно нові технології, такі як

- програмно-конфігуровані мережі SDN (Software Defined Networks) та віртуалізовані мережеві функції NFV (Network Functions Virtualisation),
- мережеве сегментування (Network Slicing),
- мобільні периферійні обчислення (Mobile Edge Computing),

існування яких стало можливим саме завдяки потужності 5G мереж, але які, водночас, створюють додаткові ризики кібербезпеки.

Основні ризики та сценарії їх виникнення, про які йдеться у Звіті, наступні:

²⁴COMMISSION RECOMMENDATION (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534&qid=1636060463752>

²⁵ EU coordinated risk assessment of the cybersecurity of 5G networks: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

1. ризики, пов'язані з неналежним захистом мережі;

Такі ризики виникають як через недостатність засобів захисту, визначених конфігурацією мережі під час її встановлення, так і значною кількістю постачальників послуг для її обслуговування, які потенційно можуть вносити зміни до конфігурації мережі, перенаправляти та відстежувати трафік, обходити впроваджені оператором механізми аудиту мережі.

Так, для обслуговування 5G мережі її оператором потрібні послуги, щонайменше: виробників мережевого обладнання та передавальних пристроїв, постачальників хмарних послуг, розробників програмного забезпечення для роботи обладнання та пристроїв мережі, адміністратори, оркестратори, системні інтегратори, спеціалісти з кібербезпеки, виробники пристроїв, які під'єднуються до мережі та розробники програмного забезпечення для роботи таких пристроїв.

Усі зазначені постачальники послуг мають потенційні можливості неправомірного доступу та втручання у роботу мережі, яке може скомпроментувати її конфіденційність, цілісність та/або призвести до втрати оператором контролю (доступу) до мережі.

2. ризики, пов'язані з ланцюгом поставок;

До цих ризиків відноситься:

- низька якість мережевого обладнання 5G, отримати несанкціонований доступ до якого стає можливим через недоліки у програмуванні або інженерному виконанні такого обладнання;

Слід також враховувати, що розгортання 5G мережі здійснюється поступово і на першому етапі за рахунок оновлення програмного забезпечення можуть використовуватись точки радіо-доступу 4G мереж. Таким чином, безпека майбутньої 5G мережі буде додатково залежати від якості обладнання, встановленого раніше для 4G мережі.

- залежність від одного постачальника, що може мати наслідком порушення роботи мережі, якщо постачальник обладнання не здійснить його своєчасної заміни та/або своєчасно не виправить недоліки програмного забезпечення у роботі обладнання.

3. ризики, пов'язані зі способами роботи носіїв загрози;

Ці ризики залежать від мотивів та засобів, які є в розпорядженні носія кіберзагрози²⁶.

²⁶ До носіїв кіберзагроз відносяться традиційно: хактивісти, окремі хакери, організована кіберзлочинність, інсайдери, кібертерористи, кіберзлочинці, спонсоровані недержавними державами: EU coordinated risk assessment of the cybersecurity of 5G networks: P.13:

Однією із серйозних загроз держави-члени ЄС вважають операторів мереж 5G та постачальників обладнання, які контролюються третіми країнами і від яких держава їх походження може вимагати вчинення неправомірних дій з метою шпигування або одержання конкурентних переваг на ринку. Втручання в роботу мережі при цьому може відбуватися шляхом використання або навмисного створення вразливостей мережі.

Загрози, пов'язані з діяльністю організованих злочинних кібергруп залишаються актуальними, при цьому, їх характер буде залежати від об'єкту, на який спрямована атака: це може бути як оператор мережі, так і кінцевий споживач, вразливість особистих даних якого зростають пропорційно потужності технології 5G.

4. ризики, пов'язані з взаємозалежністю мережі 5G та об'єктами критичної інфраструктури

З одного боку, недоліки мережі 5G можуть бути використані для кібератаки на такі об'єкти критичної інфраструктури, які виконують функції у галузі здоров'я, безпілотних приладів, газу та водопостачання, оборони, що може призвести до зупинки та руйнування таких систем.

З іншого боку, атака на електромережі та системи сповіщення про несанкціоноване втручання у мережу, може стати методом одержання контролю злочинцем над 5G мережею.

5. ризики, пов'язані з недоліками приладів кінцевих споживачів.

Ці ризики впливають як із факту очікуваного зростання кількості таких приладів та їх одночасного під'єднання до мережі 5G, так і зі слабкими вбудованими функціями безпеки таких приладів. Наслідки одночасного під'єднання до мережі 5G надвеликої кількості незахищених пристроїв можуть бути вкрай серйозними.

У звіті також зроблено акцент на тому, що в той час, як потенційні можливості мережі 5G є добре визначеними і відомими, сама технологія та її докладна архітектура знаходяться у процесі виникнення. Більше того, доки мережа 5G не розгорнута в повній мірі у державах Європейського Союзу, потенційні нові загрози ще не є вивченими і це необхідно враховувати під час процесу управління ризиками.

Цей підхід, безумовно, має застосовуватись і будь-якою державою під час управління ризиками та загрозами кібербезпеки, пов'язаними з мережами 5G: спиратися та повністю покладатися на вже існуючі найкращі практики необхідно, водночас, процес управління ризиками має бути налагоджено

таким чином, щоб їх виявлення, оцінка та нейтралізація відбувалися в режимі «реального часу» по мірі розгортання мережі.

У заключних положеннях до Звіту підкреслено²⁷, що з урахуванням кількості об'єктів інфраструктури, робота яких буде спиратися на 5G технології, цілісність та контроль доступу до 5G мережі стає питанням національної безпеки і вважається найбільшим безпековим викликом для Європейського Союзу.

2.2. Загальний ландшафт сучасних кіберзагроз та 5G мережа.

З метою кращого прогнозування майбутніх кіберзагроз, ENISA регулярно збирає, систематизує та публікує інформацію щодо поточного ландшафту кіберзагроз. Відповідно до останнього Звіту кіберзагроз ENISA, опублікованого 28 жовтня 2021 року²⁸, виявлено наступні тренди у кіберзагроз:

1. програми-вимагачі (ransomware) визнані основним трендом кібератак у 2020-2021 роках;

При цьому, основними шляхами доступу до даних залишаються фішингові листи та несанкціоноване віддалене управління комп'ютерним обладнанням користувачів, ризики якого, в свою чергу, пов'язуються з відсутністю двох-факторної ідентифікації або захищеного каналу, через який відбувається такий доступ (VPN). Деякі відомі випадки атак:

- іспанський телеком-оператор MasMovil зазнав атаки з викраденням даних від групи кіберзлочинців «REvil»: скріншоти з персональною інформацією клієнтів оператора почали розповсюджуватись в мережі TOR (червень-липень 2021 року);
- місто Л'єж зазнало атаки (блокування) системи надання публічних послуг в сфері громадянського стану: видачі документів, що посвідчують особу, право на керування транспортними засобами, подання заяв на вступ до шлюбу (червень 2021, атаку приписують групі «Ryuk»);
- один пацієнт помер (через вимушену відмову у терміновій госпіталізації) внаслідок атаки на госпіталь університету Дюссельдорфу: госпіталь був змушений припинити прийом пацієнтів через блокування роботи його ІТ-системи (вересень 2020 року);
- Португальська енергетична компанія була атакована групою «Ragnarok», яка погрожувала зливом фінансової інформації та

²⁷ Там же: Р.32

²⁸ ENISA THREAT LANDSCAPE 2021 (April 2020 to mid-July 2021):

<file:///C:/Users/Admin/Downloads/ENISA%20Threat%20Landscape%202021.pdf>

персональних даних клієнтів компанії, якщо не буде сплачено викуп у 10,9 мільйонів доларів (квітень 2020 року).

2. держави покращили свої навички на національному та міжнародному рівні у виявленні та протидії кібератакам геополітичного спрямування;
3. кіберзлочинців мотивує успіх програм-вимагачів;

Оскільки багато атакованих компаній погоджуються платити вимагачам, максимальні суми викупу зростають з кожним роком. Найбільша сума викупу у 2019 році становила 15 мільйонів доларів, а у 2020 році збільшилась до 30 мільйонів доларів. Група REvil збільшувала свої апетити протягом березня – липня 2021 року: у березні вимагала в Acer 50 мільйонів доларів, через місяць ту ж суму запросили в Quanta Computer, постачальника Apple, а в липні вимагали Kaseya вже 70 мільйонів доларів США, погрожуючи опублікувати дешифратор для доступу до всіх інфікованих девайсів по всьому світу²⁹.

4. криптовалюта залишається основним методом платежу для кіберзлочинців;

Кіберзлочинці, при цьому, відмовляються від використання Bitcoin, який вважається псевдоанонімним, і віддають перевагу криптовалютам з високим рівнем анонімності, таким як Monero³⁰.

5. зниження випадків використання вірусів (malware), яке спостерігалось у 2020 році, продовжується у 2021 році, разом з тим, у випадках його використання відзначається використання кіберзлочинцями маловідомих або рідкісних мов програмування.

Оскільки більшість програм для виявлення вірусів побудовані на статичних індикаторах, вони стають неефективними, якщо програма-вірус написана на іншій (маловідомій) мові програмування. Це також ускладнює процедуру зворотнього аналізу. Цей тренд було підтверджено, коли відомий вірус Buer було переписано мовою Rust, відтак, він отримав назву RustyBuer. Їхня схожість була при цьому ідентифікована завдяки ідентичним командним структурам.

Відомим випадком спроби інсталяції вірусу з використанням інсайдерської тактики, була спроба найму громадянином Росії працівника Tesla за винагороду в біткойнах вартістю 1 мільйон доларів для того, щоб останній встановив вірус в ІТ-системі компанії³¹.

У січні 2021 року, за участю української кіберполіції, було викрито та заблоковано діяльність транснаціонального хакерського злочинного

²⁹ ENISA Threat Landscape 2021: P.39:

<file:///C:/Users/Admin/Downloads/ENISA%20Threat%20Landscape%202021.pdf>

³⁰ Там же: P.51;

³¹ <https://www.justice.gov/opa/press-release/file/1308766/download>

угруповання з розповсюдження найнебезпечнішого і найстійкішого вірусного програмного забезпечення – «ЕМОТЕТ»³². Інфраструктура «ЕМОТЕТ» включала більше 90 серверів, розташованих по всьому світу, і фактично була БОТ-мережею. ЕМОТЕТ демонструє, як еволюціонували віруси від програм, налаштованих на передачу даних, до високорозвинених ботів з ефективною командною системою, постійним оновленням та здатністю довгий строк уникати їх виявлення.

6. зафіксовано рекордно високий рівень прихованого майнінгу криптовалют (cryptojacking) порівняно з попередніми роками;

Також однією з форм шахрайства у сфері криптовалют та завантаження вірусів стало поширення платних мобільних додатків, які начебто дозволяють користувачу майнити криптовалюту³³. и

7. COVID-19 залишається домінуючою приманкою для e-mail атак;

Цей вид кібератак більшою мірою використовує вразливості людської поведінки, звичок, «вбудованої» довіри до своїх e-mail комунікацій, ніж технологічні вразливості останніх.

З початком пандемії COVID-19 кіберзлочинці для проведення фішингових атак використовували повідомлення з пропозицією купівлі засобів захисту, першочергового отримання вакцини, неправдиву інформацію про дію тих чи інших вакцин.

Споживачі щонайменше 26 держав стали об'єктом фішингових атак з використанням SMS-повідомлень, направлених начебто від поштової служби для одержання відправлення. В такий спосіб в 2021 році у державах Європи було розповсюджено вірус Flubot Android.

Поширення QRішингу також набуло поширення у пандемію: на e-mail жертви направлялося повідомлення начебто від відомого банку з QR-кодом, який переадресовував споживача на сторінку, яка або завантажувала вірус автоматично, або з використанням інтерфейсу, ідентичного до банківського, пропонувала споживачу ввести свій логін та пароль.

Загальносвітові втрати від ВЕС-атак (Business Email Compromise, одержання доступу до акаунтів ділового листування) у 2020 році становили 1,8 мільярдів доларів США. Відома масована ВЕС-атака 2021 року була проведена з використанням підробленого сайту Office 365. В якості приманки для вищого керівництва компаній було використано листи, які містили посилання на сайт для оновлення Office 365. Одержавши логін та пароль до

³² <https://www.cyberpolice.gov.ua/news/kiberpolicziya-vykryla-transnacionalne-ugrupovannya-xakeriv-urozpovsyudzhenni-najnebezpechnishogo-v-sviti-kompyuternogo-virusu-emotet-2504/>

³³ https://www.trendmicro.com/en_us/research/21/h/fake-cryptocurrency-mining-apps-trick-victims-into-watching-ads-.html

акаунта користувача, злочинці отримали можливість надсилати підроблені листи для ініціювання та проведення банківських переказів на свої рахунки.

Новими трендами фішингових атак стає завантаження вірусів через надіслані відео або безпосередньо під час розмови.

8. спостерігався сплеск витоків медичних даних;

Таке збільшення пояснюється з одного боку, перевантаженням і відтак ситуативною вразливістю національних постачальників медичних послуг, а також попитом на послуги e-health, віддалене медичне спостереження, телемедицину, який різко зріс і збільшив «площу ураження».

Крім того, медичні дані мають більшу цінність для особи і більший потенціал для експлуатації, порівняно, наприклад з одержанням доступу до реквізитів банківської карти, яку легко заблокувати.

9. традиційні DDoS атаки стали більш цілеспрямованими, наполегливими та різнонаправленими через запровадження інтернету речей (IoT);

Пандемія та масовий перехід бізнесу на віддалену роботу мимоволі сприяє проведенню DDoS атак, оскільки пропускна здатність мережі, яка використовувалась для протидії DDoS атакам, вимушено використовується для налагодження каналів віддаленої роботи.

10. кампанії з дезінформації проводяться за допомогою штучного інтелекту;

Штучний інтелект використовується для створення фейкових акаунтів, зміни зображень та текстів, які поширюються завдяки алгоритмам соціальних мереж, створюючи хаос.

Кампанія «письменника-привида» відбувалася у Литві, Латвії та Польщі протягом 2017 – 2021 років, метою якою була критика присутності НАТО у Східній Європі. Хакери зламували сайти та акаунти електронної пошти та використовували їх для публікації підроблених документів. Останні в подальшому також поширювались через фейкові акаунти. Аналітики пов'язують цю атаку з російськими спецслужбами.

11. у 2020 та 2021 роках продовжуються спостерігатися сплески кіберінцидентів, пов'язані з помилковими діями самих користувачів (загрози з необережності, non-malicious threats).

Через помилки конфігурації у загальному доступі опинились 7 ТБ даних сховища ElasticSearch, які містили мільярди логінів, імен та платіжних даних користувачів вебсайту CAM4.com. (травень 2020 року). Місяцем раніше з того самого сховища було виявлено витік 8 ТБ даних французької газети Le Figaro.

Окремі звіти готуються ENISA відносно ландшафту кіберзагроз 5G мережі. Зокрема, у грудні 2020 року ENISA підготувала оновлений Звіт щодо оцінки основних кіберзагроз 5G мережі³⁴, із тим застереженням, що його предметом є вивчення гіпотетичних загроз, які впливають із вразливостей архітектури та дизайну 5G мережі, оскільки у 2020 році не було зафіксовано реальних кібератак на 5G мережі.

Разом з тим, зазначений Звіт, більшу частину якого складають додатки, містить деталізовані переліки можливих вразливостей 5G мереж³⁵, які можуть слугувати дороговказом при розробці та плануванні таких мереж.

Також ENISA робить акцент на тому, що вивчення архітектури та дизайну 5G мережі і оцінка відповідних ризиків здійснювались відповідно до політик та специфікацій на такі мережі. Отже, положення щодо оцінки та зменшення ризиків кібербезпеки можуть зазнавати змін в процесі реального впровадження та розгортання 5G мережі³⁶.

2.3. Заходи зі зменшення ризиків кібербезпеки 5G мереж.

На основі визначених державами-членами основних загроз, Група по співробітництву у сфері безпеки мереж та інформаційних систем (NIS cooperation group) підготувала Інструментарій по зменшенню ризиків кібербезпеки мережі 5G (Cybersecurity of 5G networks EU Toolbox of risk mitigating measures)³⁷, до якого належать:

1) Загальноєвропейське регулювання кібербезпеки Інтернет-мережі:

✓ Директива EU 2016/1148 з безпеки мереж та інформаційних систем (NIS Directive);

Директива EU 2016/1148 присвячена регулюванню 3-х основних блоків питань:

i) наявність в кожній державі-члена національної стратегії та системи відстежування та розслідування інцидентів кібербезпеки;

ii) міждержавна кооперація, зокрема, створення Групи по співробітництву у сфері безпеки мереж та інформаційних систем

iii) запровадження кожною державою нагляду за операторами мереж, які мають критичну вагу на ринку, нагляду у сфері критичної інфраструктури (енергетика, транспорт, водопостачання, охорона здоров'я, цифрові мережі, фінансовий сектор), нагляду у сфері постачальників онлайн послуг, що

³⁴ ENISA Threat Landscape for 5G Networks Report: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/>

³⁵ Там же: Р. 124 - 250

³⁶ Там же: Р. 10 - 11.

³⁷ Cybersecurity of 5G networks EU Toolbox of risk mitigating measures: <https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf>

мають критичну вагу на ринку (маркет-плейси, хмарні послуги, пошукові браузері).

Відповідні положення згодом увійшли і до Європейського кодексу електронних комунікацій.

Варто зауважити, що з урахуванням стрімкого технічного прогресу, у грудні 2020 року було запропоновано для розгляду нову редакцію Директиви ЕУ 2016/1148³⁸, яка передбачає: більш жорсткі заходи нагляду за безпекою мереж із застосуванням штрафних санкцій, утворення Європейського кризового кібер центру (EU- CyCLONe) для кращої відповіді на загальноєвропейські інциденти та загрози, посилені вимоги до політик кібербезпеки, використання шифрування, запровадження відповідальності менеджменту операторів та постачальників послуг за проведення належного ризик-менеджменту кіберзагроз³⁹.

- ✓ Закон про кібербезпеку (the Cybersecurity Act)⁴⁰, який запровадив систему сертифікації кібербезпеки на рівні Європейського Союзу, посилив та остаточно утвердив позиції ENISA в новій системі сертифікації кібербезпеки.
 - ✓ Європейський кодекс електронних комунікацій (див. вище).
- 2) Система практичних заходів.

З метою зменшення ризиків кібербезпеки мережі 5G Інструментарій рекомендує державам-членам вжити ряд практичних заходів, об'єднаних у три групи:

а. Стратегічні заходи (strategic measures):

- посилення ролі національних регуляторів (SM01)
- здійснення аудиту операторів та збір інформації (SM02)
- оцінка ризик-профілю постачальників та застосування обмежень до постачальників, ризик-профіль яких визначено як високий (SM03)
- контроль за постачальниками послуг з адміністрування (MSPs) та постачальників обладнання третьої черги підтримки (SM04)
- забезпечення різноманітності постачальників для кожного оператора за допомогою стратегії багатьох постачальників (SM05)
- забезпечення стійкості на національному рівні (SM06)

³⁸ DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:823:FIN>

³⁹ Revised Directive on Security of Network and Information Systems (NIS2): <https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2>

⁴⁰ REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1637549173097>

- визначення ключових об'єктів і впровадження різноманітної та життєздатної 5G екосистеми в ЄС (SM07)
- підтримка та побудова різноманітності та потенціалу ЄС у майбутніх мережевих технологіях (SM08)

b. Технічні заходи (technical measures):

- забезпечити застосування основних вимог безпеки до дизайну та архітектури мережі (TM010)
- забезпечити та прискорити імплементацію заходів безпеки існуючих 5G стандартів (TM02)
- забезпечити жорсткий контроль доступу (TM03)
- збільшувати безпеку віртуалізованих мережевих функцій (TM04)
- забезпечити безпеку управління, виконання операцій та моніторингу 5G мережі (TM05)
- посилити фізичну безпеку (TM06)
- посилити цілісність, оновлення та виправлення помилок програмного забезпечення (TM07)
- посилення стандартів безпеки бізнес-процесів постачальника завдяки жорстким умовам поставок (TM08)
- використовувати сертифікацію ЄС для компонентів 5G мережі, обладнання замовника та/або бізнес-процесів постачальника (TM09)
- для інших продуктів та послуг у сфері інформаційно-комунікаційних технологій, які не є 5G-специфічними (підключені прилади (connected devices), хмарні послуги) також використовувати сертифікацію ЄС (TM10)
- запровадити плани щодо посилення стійкості та безперервності роботи мереж (TM11)

c. Заходи з підтримки (supporting actions)

- перегляд та створення керівних настанов та кращих практик мережевої безпеки (SA01)
- збільшення потенціалу у галузі тестування та аудиту на національному та загальноєвропейському рівнях (SA02)
- підтримка та розробка стандартів у галузі 5G (SA03)
- створення керівних настанов щодо імплементації існуючих стандартів 5G (SA04)
- забезпечення дотримання технічних стандартів та організаційних заходів з безпеки завдяки загальноєвропейській схемі сертифікації (SA05)
- обмін найкращими практиками впровадження стратегічних заходів, особливо в частині оцінки ризик-профілю постачальників (SA06)

- розвиток взаємодії у сферах реагування на інциденти та кризового менеджменту (SA07)
- проведення аудиту взаємозалежності між 5G мережею та іншими критично важливими послугами (SA08)
- вдосконалення механізмів співпраці, координації та обміну інформацією (SA09)
- забезпечення врахування ризиків кібербезпеки під час впровадження 5G проектів, які фінансуються за рахунок публічних фондів (SA10).

Як впливає зі Звіту держав-членів щодо прогресу в імплементації Інструментарію по зменшенню ризиків кібербезпеки мережі 5G⁴¹, станом на середину 2020 року європейські країни знаходились приблизно на середні шляху до впровадження заходів, передбачених Інструментарієм.

Аналіз вказаного Звіту дозволяє виділити наступні акценти та виклики, з якими стикаються держави-члени під час імплементації зазначених заходів:

- ✓ надання регуляторним органам права регулювати вимоги до постачальників обладнання мережі 5G та постачальників послуг для її обслуговування, з правом забороняти встановлення обладнання та/або програмного забезпечення для мережі 5G або навіть вимагати його демонтажу;
- ✓ використання регуляторними органами повноважень з ретроспективним ефектом, оскільки для розгортання мережі 5G може використовуватись вже наявне обладнання та послуги;
- ✓ відмінність обсягу повноважень регулятора у розрізі різних суб'єктів (залежно від ризик-профілю) та об'єктів 5G мережі (залежно від вразливості об'єкта або сфери його використання);
- ✓ необхідність розроблення національної методології аудиту та комплаєнсу безпеки 5G мережі;
- ✓ необхідність розроблення методології оцінки ризик-профілю постачальників обладнання або програмного забезпечення для 5G мережі, встановлення для операторів мереж перехідного періоду у разі виявлення фактичної залежності від постачальника з високим ризик-профілем;
- ✓ визначення переліків вразливого обладнання та послуг для 5G мережі, які вимагають спеціального регулювання;
- ✓ визначення об'єктів критичної інфраструктури, які потребують спеціальних заходів безпеки у разі використання 5G технологій;

⁴¹ Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity / <https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>

- ✓ посилення вимог до прозорості відносин між операторами та постачальниками обладнання та послуг для 5G мережі;
- ✓ визначення послуг для обслуговування 5G мережі, які оператори мають право передавати на аутсорсинг;
- ✓ розробка стратегії багатьох постачальників, яка виявилась складним завданням, з огляду на розмір держави, реальну пропозицію відповідного обладнання на ринку, недостатню інтегровуваність обладнання різних постачальників;
- ✓ складність стандартизації та сертифікації у сфері 5G технології, яка знаходиться у процесі розвитку.

Держави-члени вирішують зазначені виклики в різний спосіб.

В Естонії на рівні закону передбачено право уряду встановлювати вимоги до оператора та обов'язок останнього надавати інформацію відносно мережевого обладнання та його програмного забезпечення. Обладнання та програмне забезпечення для потреб оборони використовуються за дозвільним принципом. Процедурні питання мають бути врегульовані підзаконними актами.⁴²

Французький закон № 2019-810 від 01.08.2019 наділяє регулятора правом обмежувати, забороняти, визначати умови та правила постачання, встановлення та керування обладнанням для 5G мережі. При цьому оператор повинен одержати попередній дозвіл від Прем'єр-Міністра для розгортання та керування вразливим обладнанням для 5G мережі та інших технологій майбутнього. Перелік такого обладнання встановлено підзаконним актом. В процесі надання дозволу оцінюються архітектура мережі, процеси її управління та обслуговування, контроль доступу, перелік постачальників обладнання та послуг, необхідних для обслуговування 5G мережі⁴³

Закріпити дозвільний порядок встановлення та надання послуг 5G мережі планує також Бельгія в рамках спеціального закону. Законом передбачається закріплення процедури попередньої авторизації операторів 5G мережі. Перелік вразливого обладнання та високоризикових постачальників має визначатися декретом короля Бельгії. Також він матиме право заборонити допуск на ринок окремих постачальників обладнання та послуг для 5G мережі⁴⁴.

Змінами до Закону про електронні комунікації Швеції передбачено, що використання передавачів радіохвиль може бути дозволено тільки за умови, що це не шкодить національній безпеці. Відповідність умовам безпеки є

⁴² Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity: P. 11,

⁴³ Там же: P. 12, 18, 20

⁴⁴ Law introducing additional security measures for the supply of mobile 5G services:

<https://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2021&num=206>

обов'язковою для учасників аукціонів щодо набуття права на використання радіочастот для 5G мережі.

Відповідно до законодавства Австрії, оператори 5G мережі повинні виконувати вимоги Системи управління інформаційною безпекою відповідно до ISO/IEC 27 001, стандартів 3GPP та подальших стандартів, двічі на рік звітувати регулятору про стан роботи мережі та своїх постачальників.⁴⁵

У Нідерландах, Декретом щодо безпеки та цілісності телекомунікаційних мереж від 28.11.2019 визначено ознак, за якими можуть встановлюватись ознаки ризикових постачальників, зокрема, 1) передбачений законодавством країни, до якої належать контролери постачальника, обов'язок співпрацювати з державою для виконання розвідувальних або військових завдань; 2) контролером постачальника є держава; 3) країна походження постачальника належить до тих, які здійснюють або з огляду на поточний стан відносин можуть здійснювати агресивну розвідувальну політику відносно Нідерландів.⁴⁶

Відповідно до закону Італії, Уряд необхідно інформувати про намір розгортання 5G мережі з використанням обладнання або послуги, постачальники яких походять з країни, які не є учасницями Європейського Союзу. При цьому, міжвідомча координаційна група може рекомендувати Уряду заборонити здійснення відповідної поставки або встановити вимоги безпеки. На операторів мобільних мереж покладено обов'язок розробки планів «горизонтальної» та «вертикальної» диверсифікації поставок системоутворюючого обладнання та послуг для 5G мережі⁴⁷

В Ірландії впровадження Інструментарію здійснюється на рівні Правил безпеки телекомунікацій (Telecoms Security Requirements, TSRs), які знаходяться в процесі розробки. Правилами планується визначити цілий ряд технічних та організаційних вимог, які повинні вживати оператори мереж для забезпечення їх безпеки. Також оператори мереж повинні закріплювати безпекові вимоги у контрактах з постачальниками обладнання та послуг для потреб мережі. Правилами планується закріпити ряд вимог щодо дизайну мережі та контролю доступу, включаючи правила авторизації, мульти-факторної ідентифікації, принцип найменших привілеїв, розподіл обов'язків, використання належних протоколів доступу та моніторинг незвичної активності мережі.⁴⁸

У 2021 році ENISA також провела та опублікувала результати експертного дослідження щодо імплементації державами-членами політики

⁴⁵ Там же: Р. 13, 30

⁴⁶ Там же: Р. 18,

⁴⁷ Там же: Р. 18, 22

⁴⁸ Там же: Р. 20, 31

Європейського Союзу щодо безпеки телекомунікацій⁴⁹. Відповідно до цього дослідження, експерти відзначили, що в цілому імплементація в національне законодавство регуляторних норм Європейського Співтовариства підвищує рівень безпеки телекомунікаційних мереж, а вимоги законодавства в галузі кібербезпеки вбачаються адекватними та такими, що відповідають своїй меті.

Разом з тим, виявлено і низку викликів, які виникають у процесі регулювання та виконання політики Європейського Союзу щодо безпеки телекомунікацій:

- ✓ законодавство є складним і як результат, застосовується неоднозначно (наприклад, немає єдиного підходу до тлумачення поняття «інциденту» у телекомунікаційних мережах)⁵⁰;
- ✓ регулятори мають достатньо повноважень відповідно до закону, але відчують брак експертного та технічного забезпечення;
- ✓ система інформування регулятора про інциденти мережі дозволяє підвищити їх безпеку, але:
 - через неоднозначне тлумачення інциденту та врахування його тривалості, деякі інциденти (наприклад, витoki даних) залишаються поза сферою звітування;
 - через розгалужену систему регуляторів, звіти про один і той же інцидент можуть хаотично відправлятися до різних державних органів;
 - оператори не мають достатньо довіри до державних органів (і не поспішають зі звітами про інциденти у мережі);
- ✓ відзначається нестача загальноєвропейської стандартизації.

Разом з тим, деякі держави показують гарний приклад у вирішенні наведених викликів⁵¹. Так, у Португалії національний регулятор (ANACOM) розробляє для телеком-операторів методичні рекомендації, які полегшують застосування законодавства; кожен оператор повинен мати у штаті експерта з питань комплаєнсу та безпеки мереж, а для того, щоб такі експерти між собою та регулятором могли постійно обмінюватись досвідом, регулятор створив спеціальну платформу.

Бельгійський регулятор (BIPR) наділений повноваженнями у разі потреби отримувати експертну та ресурсну підтримку від інших державних органів, в тому числі, кризисних центрів, розвідувальної служби, національної служби реагування на інциденти в мережі.

⁴⁹ Assessment of EU Telecom Security Legislation: <https://www.enisa.europa.eu/publications/assessment-of-eu-telecom-security-legislation>

⁵⁰ Там же: Р.10

⁵¹ Там же: Р. 18-19.

У Фінляндії національний регулятор Traficom, навпаки, максимально концентрує усі функції (нагляду, кібербезпеки, реагування на інциденти), що дає можливість сконцентрувати необхідні для роботи ресурси.

У Данії створено спеціальний Центр кібербезпеки, який одержує всі повідомлення про кіберінциденти і самостійно визначає органи, відповідальні за їх розгляд. Бельгійський центр поштового та телекомунікаційного зв'язку запропонував іншим органам свою платформу для отримання повідомлень про інциденти безпеки мережі для спільного використання з іншими державними органами (відповідно, створення таких платформ не дублюється, як і розслідування одних і тих самих інцидентів).

Позитивно відзначається практика держав-членів, спрямована на створення середовища співпраці з учасниками ринку телекомунікацій. Так, Національний центр кібербезпеки Ірландії активно співпрацює з приватним сектором (Amazon, Microsoft), який надає йому підтримку у разі необхідності. Агенство з радіокомунікацій Нідерландів у своїй роботі намагається уникати штрафів, як мети нагляду за ринком, натомість, концентрується на підвищенні свідомості операторів для впровадження належних заходів безпеки та ризик-менеджменту мереж.

З урахуванням кращих європейських практик, експерти рекомендували при впровадженні політик кібербезпеки:

- ✓ якнайшвидше завершувати на національному рівні імплементацію ЕСЕС та EU 5G Toolbox;
- ✓ розробляти загальноєвропейські стандарти безпеки мереж;
- ✓ впроваджувати разом із новим законодавством деталізовані технічні регламенти та методичні рекомендації щодо його застосування;
- ✓ збільшувати рівень співпраці між державним та приватним сектором;
- ✓ покращувати рівень співпраці регуляторів між собою з метою подолання нестачі експертів та необхідної ресурсної бази для виконання своїх функцій;
- ✓ уникати покладення на операторів надмірних та перехресних зобов'язань перед різними державними органами, особливо в частині звітування про інциденти у мережі;
- ✓ налагоджувати зворотній зв'язок за результатами розслідування інцидентів кібербезпеки.

ВИСНОВКИ:

Під час засідання 21-22 жовтня 2021 року Європейська Рада закликала розглянути пропозицію Єврокомісії щодо запровадження Програми «Шлях до цифрового десятиліття», яка визначатиме політику ЄС у цифровій сфері до 2030 року, а також прискорювати процес розробки Закону про цифрові

послуги, Закону про цифрові ринки, Закону про штучний інтелект та Закону про цифрову ідентичність⁵².

Проект програми «Цифровий компас 2030» демонструє ще більш амбітні цілі держав-членів ЄС для досягнення цифрового майбутнього. До 2030 року:

- 80% дорослих повинні мати базові цифрові навички;
- всі домогосподарства повинні мати гігабітний зв'язок;
- всі населені пункти повинні мати 5G;
- в Європі має бути побудований перший квантовий комп'ютер;
- три з чотирьох компаній повинні використовувати хмарні обчислення та штучний інтелект;
- всі ключові державні послуги повинні надаватись в електронній формі;
- медичні карти усіх громадян мають бути переведені в електронну форму;
- щонайменше 80% повинні мати електронні посвідчення особи, тощо.

Досягнення цих цілей обумовлюється пришвидшенням процесу імплементації державами-членами ЄС нормативної бази для розгортання 5G мереж, якими залишаються Європейський кодекс електронних комунікацій та Загальносоюзний Інструментарій кращих практик для забезпечення покриття, який було розроблено та схвалено державами-членами 25 березня 2021 року відповідно до рекомендації (EU) 2020/1307 від 18.09.2020.

Україною положення Європейського кодексу електронних комунікацій та кращі практики для забезпечення покриття в цілому імplementовані в Законі № 1089-IX від 16.12.2020 «Про електронні комунікації», який набуде чинності з 01 січня 2022 року. Отже, за ознакою наявності прогресивної законодавчої бази, Україна навіть випереджає деякі держави-члени ЄС. Однак, практична реалізація прогресивного законодавства вбачається неможливою без врахування та вирішення безпекових викликів, пов'язаних з 5G мережею.

В державах-членах ЄС значна увага приділена питанню безпеки 5G мереж та технологій, розроблено необхідний Інструментарій, очікується створення загальної системи стандартизації та сертифікації.

Держави-члени ЄС стикаються із такими викликами як:

- розробка загальноєвропейських стандартів безпеки мереж та необхідність розроблення національної методології аудиту безпеки 5G мережі;

⁵² Outlook for the European Council meeting of 21-22 October 2021: P.3:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/694238/EPRS_BRI\(2021\)694238_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/694238/EPRS_BRI(2021)694238_EN.pdf)

- необхідність розроблення методології оцінки ризик-профілю постачальників обладнання або програмного забезпечення для 5G мережі, встановлення для операторів мереж перехідного періоду у разі виявлення фактичної залежності від постачальника з високим ризик-профілем;
- визначення переліків вразливого обладнання та послуг для 5G мережі, які вимагають спеціального регулювання;
- визначення об'єктів критичної інфраструктури, які потребують спеціальних заходів безпеки у разі використання 5G технологій;
- розробка стратегії багатьох постачальників;
- впровадження разом із новим законодавством технічних регламентів та методичних рекомендацій щодо його застосування;
- підвищення рівня співпраці між державним та приватним сектором, та також окремих регуляторів між собою;
- подолання нестачі експертів та матеріальних ресурсів для забезпечення безпеки 5G мережі та виконання регулятором своїх функцій;
- вдосконалення процедури повідомлення та розслідування інцидентів кібербезпеки.
- складність стандартизації та сертифікації у сфері 5G технології, яка знаходиться у процесі розвитку.

Ті ж самі завдання постануть перед Україною по мірі розгортання 5G мереж та впровадження 5G технологій. Натомість, ситуація навіть із загальними ризиками кібербезпеки вбачається критичною, про що відверто зазначено у Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021⁵³, відповідно до якої залишаються невиконаними завдання Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, зокрема: не сформовано перелік об'єктів критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства. Розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились епізодично.

Водночас, затвердження нової Стратегії дає привід сподіватись, що Україна зможе подолати зазначені виклики та спираючись на інструментарій та досвід держав-членів ЄС зможе здійснити належне впровадження 5G технологій та зайняти гідне місце у цифровій Європі.

⁵³ УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": <https://www.president.gov.ua/documents/4472021-40013>