ПОРІВНЯЛЬНИЙ АНАЛІЗ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ 5G В УКРАЇНІ ТА ЄВРОПЕЙСЬКИХ КРАЇНАХ: НІМЕЧЧИНІ, ШВЕЦІЇ, ФІНЛЯНДІЇ ТА КРАЇНАХ БАЛТІЇ

Ксенія ВОЛКОВА
експерт ГО «ВАІБІТ»

грудень 2021

COMPARATIVE ANALYSIS OF 5G CYBERSECURITY REGULATION IN UKRAINE AND EUROPEAN COUNTRIES: GERMANY, SWEDEN, FINLAND AND THE BALTIC STATES

Annotation

Deploying 5G networks, along with unprecedented capabilities, potentiates the growth of existing cyber threats and creates new challenges. That is why this review examines the issues of cybersecurity regulation of the fifth generation network, at the level of the European Union (EU), individual EU member states, and the situation with the implementation of the network. The main focus is on cybersecurity legislation, in terms of 5G network protection, both at the level of EU institutions and EU member states: Germany, Sweden, Finland and the Baltic States (Estonia, Lithuania, Latvia), the situation in Ukraine is studied.

The set of EU cybersecurity instruments, jointly agreed between the EU Commission and the Member States, reflects a risk-oriented approach to cybersecurity, based on the general principles of EU law.

The risk assessment enshrined in EU acts is based on the criteria of objectivity, transparency, proportionality and technological neutrality. The defined set of tools recommends a well-balanced and coherent set of measures aimed at reducing risk, in particular the application of standardization and certification mechanisms in the EU.

Some EU Member States choose (rely on) political criteria to address the security of their 5G networks and do not take into account the EU's common approach.

The regulatory framework for the deployment of 5G networks remains the European Electronic Communications Code and the All-Union Best Practice Toolkit for Coverage, which was developed and approved by Member States on 25 March 2021 in accordance with Recommendation (EU) 2020/1307 of 18.09.2020. The process of their implementation in the EU Member States is still ongoing.

КОРОТКИЙ ОГЛЯД

Розгортання 5G мереж, поряд з безпрецедентними можливостями, потенціює зростанню існуючого рівня кіберзагроз і створює нові виклики. Саме тому в цьому огляді досліджуються питання регулювання кібербезпеки мережі п'ятого покоління, на рівні Європейського Союзу (ЄС), окремих держав-членів ЄС, та ситуації з впровадження мережі. Основний фокус зроблено на законодавство про кібербезпеку, у частині захисту мережі 5G, як на рівні інституцій ЄС, так держави-членів ЄС : Німеччині, Швеції, Фінляндії та країн Балтії (Естонії, Литви, Латвії), досліджується ситуація в Україні.

Набір інструментів ЄС з кібербезпеки, спільно узгоджений між Комісією ЄС та державами-членами, відображає орієнтовний підхід ризиків до кібербезпеки, який грунтується на загальних принципах права ЄС.

Закладена в актах ЄС оцінка ризику, базується на критеріях об'єктивності, прозорості, пропорційності та технологічній нейтральності. Визначений набір інструментів рекомендує добре збалансований і узгоджений набір заходів скирдований на зменшення ризику, зокрема застосування механізмів стандартизації та сертифікації в ЄС.

Деякі держави-члени ЄС обирають (спираються) політичні критерії для вирішення питань безпеки своїх мереж 5G та не враховують спільний підхід ЄС.

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.

Зміст

Вступ та методологія

Технологія 5G як нова і проривна технологія, що широко розповсюджується, домінуватиме у сфері цивільних телекомунікацій у майбутньому і стане основою суспільства. Як говорить: Антоніо Кальдерон, виконуючий обов'язки головного технологічного директора Агентства зв'язку та інформації НАТО (NCI)[1], - «5G може сприяти більш широкому використанню багатьох інших нових та революційних технологій, таких як штучний інтелект, машинне навчання, аналітика великих даних та Інтернет речей»

В основу технології 5G покладено Стандарт IMT-2020, що був винайдений Консорціумом розробників специфікації для мобільної телефонії 3GPP (The 3rd Generation Partnership Project)[2].

Україна має плани з впровадження технології 5G. Уряд[3] схвалив План заходів щодо впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління (розпорядження Кабінету Міністрів України від 11 листопада 2020 р. № 1409) [4].

На червень 2022 року призначено проведення аукціону або конкурсу про надання в користування радіочастотного спектра з використанням радіотехнології мобільного зв'язку п'ятого покоління.

Серпень 2022 року визначено як термін надання операторам права на користування радіочастотним спектром з використанням радіотехнології мобільного зв'язку п'ятого покоління із застосуванням процедур аукціону або конкурсу.

Хоча офіційне розгортання технології 5G в Україні відкладено, але 25 жовтня цього року[5], завдяки спільному проєкту Міністерства цифрової трансформації, мобільного оператора Vodafone Україна, компанії Huawei Ukraine та технологічного парку UNIT.City, все ж таки, тестування технології було розпочато.

Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, ратифіковано Законом від 16.09.2014 № 1678-VII

(далі – Угода про асоціацію), визначено зовнішньополітичний вектор України.

Практичні та регуляторні рішення Європейського Союзу у сфері впровадження технології 5G мають визначальне значення для України.

[1] https://www.ncia.nato.int/

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

Проведено аналіз 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.

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

Інформація та висновки, які надані в цьому дослідженні 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

На початку становлення технології 5G у державах ЄС, більше уваги зосереджувалося на інфраструктурі, звільненні та виділенні необхідних діапазонів радіочастот, пошук моделей та джерел фінансування для розгортання мережі 5G, то в останні роки головними темами дискусії є питання національної та Загальноєвропейської стратегії кібербезпеки.

26 березня 2019 року затверджена Рекомендація 2019/534 з кібербезки 5G мереж [2] , яка зобов'язує держави-члени вжити заходів з оцінки ризиків кібербезпеки та вироблення кращих практик захисту з метою управління такими ризиками на національному рівні та на рівні ЄС.З метою регулювання цього питання Європейською комісією

Серед іншого, у Рекомендації 2019/534 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 5G[3].

У січні 2020 року Європейська комісія та держави-члени ЄС домовилися про спільну Панель інструментів для кібербезпеки 5G (Інструментарій ЄС). Набір інструментів ЄС рекомендує підхід, що ґрунтується на оцінці ризику кібербезпека, заснована «виключно на міркуваннях безпеки»[4] та на об'єктивній оцінці виявлених ризиків, повній повазі до відкритості єдиного ринку ЄС.

---

[2] COMMISSION 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

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

[4] European Commission, "Secure 5G Networks, Questions and Answers on the EU Toolbox." https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

Отже, Інструментарій ЄС визначає об'єктивні та пропорційні заходи безпеки, гармонізацію стандартів безпеки та сертифікація в усьому ЄС, та не націлений на певного постачальника чи державу-члена ЄС.

Також, у ЄС оприлюднено пропозицію щодо нової директиви з кібербезпеки, яка, якщо її буде схвалена, забезпечить набагато суворіші та скоординовані рамки для держав-членів. Це спрямовано на впровадження Інструментарію ЄС на рівні держав-членів є послідовним і відповідає основним принципам права ЄС.

Хоча оператори в значній мірі відповідають за безпечне розгортання 5G, а держави-члени несуть відповідальність для національної безпеки мета Інструментарію ЄС полягає у визначенні скоординованого підходу ЄС на основі загального набору заходів, спрямованих на зменшення основних ризиків кібербезпеки мереж 5G, які визначено у скоординованому ЄС звіті про оцінку ризиків.

1.1 Визначення ризиків кібербезпеки 5G мереж

Інструментарій ЄС.

Набір інструментів ЄС містить рекомендації для країн-членів щодо того, як пом'якшити ризики, пов'язані з безпекою та цілісність поточних або майбутніх мереж 5G по всій Європі. Він виділяє кілька заходів, які держави-члени повинні визначити пріоритети в своїх планах дій з кібербезпеки і рекомендувати державам-членам провести ретельну оцінку ризику, щоб встановити відповідні та пропорційні заходи вирішувати конкретні ризики.

В Інструментарію ЄС запропонована стратегія пом'якшення ризику та детально описує перелік технічних і стратегічних заходів, яких країни-члени повинні дотримуватися.

Технічні заходи включають заходи щодо посилення безпеки мереж та обладнання 5G посилення безпеки технологій, процесів, людей і фізичних факторів:

- ✓ забезпечення застосування базових вимог безпеки (проект безпечної мережі та архітектури);
- ✓ забезпечення та оцінка впровадження заходів безпеки в існуючих стандартах 5G;
- ✓ забезпечення суворого контролю доступу;
- ✓ підвищення безпеки функцій віртуалізованої мережі;

https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

✓ забезпечення безпечного керування мережею 5G, її функціонування та моніторингу;
✓ посилення фізичної безпеки. Посилення цілісності програмного забезпечення, керування оновленнями та виправленнями;
✓ підвищення стандартів безпеки в процесах постачальників за допомогою визначення умови надійних закупівель;
✓ використання сертифікації ЄС для компонентів мережі 5G, обладнання клієнтів та/або постачальників процесів;
✓ використання сертифікації ЄС для інших інформаційних та комунікаційних технологій, які не стосуються 5G продукти та послуги (підключені пристрої, хмарні послуги);
✓ зміцнення планів стійкості та безперервності.

Стосовно стратегічних заходів, країни-члени повинні застосовувати цілісний підхід у своїй діяльності стратегії реалізації та враховують зовнішні фактори, такі як соціально-економічні витрати та екологічні міркування. Інструментарій ЄС також визначає цілі або заходи, такі як:

✓ посилення ролі національних органів влади;

✓ проведення аудиту операторів та отримання інформації;

✓ оцінка профілів ризиків постачальників та застосування обмежень дляпостачальників з високим ризиком, включаючи необхідні виключення для ефективного зменшення ризиків, для ключових активів;
✓ контроль за постачальниками послуг з адміністрування (MSPs) та постачальників обладнання третьої черги підтримки;
✓ забезпечення різноманітності постачальників для окремих операторів мобільних мереж через стратегії мультивендорів;

✓ посилення стійкості мереж на національному рівні;

✓ визначення ключових активів та сприяння розвитку різноманітної та стійкої екосистеми 5G в ЄС;

✓ підтримка та розбудова різноманітності та потенціалу ЄС у майбутніх мережевих технологіях.

Що стосується оцінки профілів високого ризику окремих постачальників, Європейська Комісія пропонує оцінити на основі низки факторів, не рекомендуючи категоричного виключення конкретних постачальників або продуктів, ймовірність того, що постачальник зазнає втручання з боку країни, яка не входить до ЄС. Це може сприяти, але не обмежуватись, наявності таких факторів:

✓ міцний зв'язок між постачальником та урядом даної третьої країни;

✓ законодавство третьої країни, особливо там, де немає законодавчих або демократичних стримувань і противаг, або за відсутності безпеки чи даних угоди про захист між ЄС та такою третьою країною;

✓ характеристики корпоративної власності постачальника;

✓ здатність третьої країни здійснювати будь-які форми тиску, у тому числі по відношенню до місця виготовлення обладнання;

✓ здатність постачальника забезпечити постачання;

Загальна якість продукції та методи кібербезпеки постачальника, включаючи:

✓ ступінь контролю над власним ланцюгом поставок чи є відповідним пріоритет, що надається практикам безпеки;

✓ оцінка профілю ризиків постачальника може також враховувати видані повідомлення органами влади ЄС та/або національними органами держав-членів.

Кожна держава-член вживає необхідних заходів для належного та пропорційного реагування щодо фактичних виявлених ризиків. Кожна держава-член повинна виконувати плани пом'якшення наслідків, враховуючи фактори реалізації, такі як вартість та економічний та/або соціальний вплив.

Реалізація Інструментарію ЄС має відповідати основним принципам ЄС; зокрема, вільний рух товарів і послуг, чесній конкуренції, а також загальним принципам права ЄС. Конкретні постачальники або продукти не є виключенням.

Нарешті, підтримуючи ці заходи державами-членами, Європейська Комісія має намір вжити власні заходи щодо підтримки різноманітного та стійкого ланцюга поставок 5G, щоб уникнути довгострокової залежності, в т.ч шляхом повного використання існуючих інструментів (відбір, інструменти торговий захист, конкурс). Подальше зміцнення потенціалу ЄС у технологіях 5G використовуючи релевантні програми ЄС; фінансування та сприяння координації між державами-членами щодо стандартизація для досягнення конкретних цілей безпеки; і розробка відповідної сертифікації в усьому ЄС схеми.

1.2. Загальний ландшафт сучасних кіберзагроз та 5G мережа

Відповідно до існуючий в ЄС регуляцій на операторів телекому можуть бути накладені також зобов’язання щодо забезпечення кібербезпеки. Держави-члени ЄС зобов'язані забезпечити цілісність і безпеку публічних та загальнодоступних мережах зв'язку, або вжиття заходів управління ризиками безпеки.

Розбудована конструкція також передбачає, що компетентні національні регулюючі органи мають повноваження для визначення видання обов'язкових інструкцій та забезпечення їх дотримання.

Європейський кодекс електронних комунікацій (далі – **ЕЕСС, Кодекс)**[5], Директива (ЄС) 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій підтримує та розширює положення про безпеку та запроваджує визначення безпеки мереж і послуг та інцидентів безпеки. Кодекс передбачає, що заходи безпеки повинні враховувати всі відповідні аспекти певних елементів у таких сферах, як безпека мереж і об'єктів, обробка інцидентів безпеки, безперервність бізнесу управління, моніторинг, аудит і тестування, а також відповідність міжнародним стандартам.

В частині створення умов для розгортання та використання 5G мережі слід звернути увагу на такі положення та принципи ЕСЕС: визначено поняття «мережі надвисокої пропускної здатності» (стаття 2);

- ✓ держави-члени ЄС 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;
- ✓ національні регуляторні та/або інші компетентні органи мають провести географічний огляд територіального охоплення електронних комунікаційних мереж, здатних забезпечувати широкосмуговий доступ 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 ЄС 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

[5] 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

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 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 ЄС повинні забезпечити право регулятора вимагати від операторів телекомунікаційних мереж (a) надавати інформацію, необхідну для оцінювання безпеки їхніх мереж і послуг, включаючи задокументовані правила безпеки; та (b) проводити незалежний аудит безпеки телекомунікаційних мереж.

✓ 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 ЄС[6].

До 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 ЕСЕС[7].

Станом на грудень 2021 року тільки 9 держав ЄС (Бельгія, Болгарія, Греція, Данія, Німеччина, Угорщина, Франція, Фінляндія, Чехія) імплементували ЕСЕС.

Директива EU 2016/1148 з безпеки мереж та інформаційних систем (NIS Directive)[8]. Директива EU 2016/1148 присвячена регулюванню таких питань:

✓ наявність в кожної держави-члена національної стратегії та системи відстежування та розслідування інцидентів кібербезпеки;

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

✓ запровадження кожною державою нагляду за операторами мереж, які мають критичну вагу на ринку, нагляду у сфері критичної інфраструктури

[6] 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

[7] 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

[8] 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

(енергетика, транспорт, водопостачання, охорона здоров'я, цифрові мережі, фінансовий сектор), нагляду у сфері постачальників онлайн послуг, що мають критичну вагу на ринку (маркет-плейси, хмарні послуги, пошукові браузери).

Пропозиція Директиви щодо заходів для високого загального рівня кібербезпеки (NIS 2 **).** У грудні 2020 року було запропоновано для розгляду нову редакцію Директиви EU 2016/114838 (NIS 2[9]) , яка передбачає: більш жорсткі заходи нагляду за безпекою мереж із застосуванням штрафних санкцій, утворення Європейського кризисного 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 кіберзагроз[10].

Пропозиція щодо директиви NIS 2 накладає ряд зобов'язань на держави-члени та приватні організації, що діють в ЄС. По-перше, держава-член повинна буде підготувати та підтримувати детальну стратегію кібербезпеки разом із набором політик щодо кібербезпеки в ланцюжку постачання продуктів і послуг ІКТ, розкриття вразливостей, специфікація вимог кібербезпеки для державних закупівель, розробки інструментів кібербезпеки науково-дослідними установами, обмін інформацією між компаніями, а також підвищення обізнаності та навичок. Держава-член ЄС також повинна була б повідомити Європейську Комісію про такі політики та стратегій. Ця політика буде ретельно перевірена державою-членом ЄС - системою експертної оцінки.

По-друге, держава-член ЄС має створить або призначить один (або кілька) компетентних національних органів для керувати потенційними кризами та інцидентами відповідно до плану реагування на кризові ситуації.

Національний орган також буде виконувати функцію зв'язку з органами влади інших держав-членів і контролювати застосування директиви у своїй державі. Національний орган влади також матиме широкий спектр повноважень для розслідування, щоб забезпечити виконання зобов'язань директиви не порушуються, включаючи можливість накладення адміністративних штрафів на приватних суб'єктів іменовані «важливими та важливими суб'єктами» (тобто постачальники цифрових послуг та цифрові інфраструктури включено до реєстру, який створюватиметься та зберігатиметься Агентством ЄС з кібербезпеки).

[9]Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union,repealing Directive 2016/1148 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

[10] 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

Обробка інцидентів буде здійснюватися за допомогою «реагування на інциденти комп'ютерної безпеки» кожної країни-члена команда» (CSIRT). Зокрема, на щоденній основі команда буде відстежувати загрози, завчасно надавати попередження зацікавленим сторонам, реагування на інциденти, проактивні оцінки та аналіз, і надавати допомогу CSIRT в інших державах-членах ЄС. CSIRT має створити стандартизовану практику для виконання вищезгаданих завдань.

Закон про кібербезпеку (the Cybersecurity Act[11]), який запровадив систему сертифікації кібербезпеки на рівні Європейського Союзу, посилив та остаточно утвердив позиції ENISA в новій системі сертифікації кібербезпеки.

Звіт ENISA щодо оцінки основних кіберзагроз 5G мережі. 14 грудні 2020 року ENISA оприлюднило оновлений Звіт щодо оцінки основних кіберзагроз 5G мережі[12], із тим застереженням, що його предметом є вивчення гіпотетичних загроз, які випливають із вразливостей архітектури та дизайну 5G мережі, оскільки у 2020 році не було зафіксовано реальних кібератак на 5G мережі.

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.

У Звіті ENISA надає рекомендації щодо збору інформації, пов'язаної з кібербезпекою, консолідації роботи зацікавлених сторін, постійному аналізі загрози кібербезпеці, розробці спільних заходів реагування та проведення аналізу недоліків на рівні ЄС, підвищенню рівень зацікавлених сторін і національний рівень.

16 грудня 2020 року ЄС оголосив про нову стратегію кібербезпеки, яка містить конкретні регуляторні пропозиції та інвестиційні та політичні ініціативи щодо підвищення стійкості та технологічний суверенітет; створення оперативного потенціалу для запобігання, стримування та реагування; і просування глобального та відкритого кіберпростору шляхом розширення співпраці. Зокрема, ця стратегія включає пропозиції щодо директив у сфері кібербезпеки.

Отже, впровадження рекомендацій та інструментів, огляд яких зроблено вище триває, а більш завершену інформацію та відповіді щодо їх ефективності

---

11 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

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

35 Там же: P. 124 - 250

36 Там же: P. 10 - 11.

можна буде отримати лише згодом, сформувавши відповідну практику застосування.

2. Аналіз ситуації в Україні та європейських країнах: Німеччині, Швеції, Фінляндії та країнах Балтії.

Вивчая особливості досвіду інших країн з провадження 5G було проведено дослідження як щодо досвіду впровадження заходів кібербезки та захисту, так і щодо рівня забезпечення та готовності використання мережі 5G. Зокрема ландшафту покриття 5G; винагороди за спектр; спектру (частот), стратегії, часового періоду обраного для впровадження технології, порядку та вартості ліцензування, найкращих практик та перспектив розвитку мережі, умов покриття економічно невигідних, вартості та строків дії ліцензії, застосування практик державно-приватного партнерства. Розпочнемо огляд з України.

2.1. Україна

11 листопада 2020 року схвалено План заходів щодо впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління (розпорядження від 11.11. 2020 р. № 1409 та від 04.08. 2021 року № 930):

- ✓ на червень 2022 року призначено проведення аукціону або конкурсу про надання в користування радіочастотного спектра з використанням радіо технології мобільного зв'язку п'ятого покоління;
- ✓ на серпень 2022 року призначено надання операторам права на користування радіочастотним спектром з використанням радіотехнології мобільного зв'язку п'ятого покоління із застосуванням процедур аукціону або конкурсу;
- ✓ вивільняються смуги радіочастот, діапазони яких займає телебачення, для впровадження радіотехнології LTE у діапазонах 790 – 862 МГц, 694 – 790 МГц. Зараз на цих частотах працює українське телебачення. Схвалений План передбачає вивільнення частот компаніями та налаштування обладнання на нижчі діапазони компаніями "Зеонбуд" та ТРК "Етер". Вивільнення частот – не завадить роботі телебачення, адже воно буде працювати у нижчих діапазонах.
- ✓ у сільській місцевості, віддалених територіях та вздовж автомобільних доріг буде використовуватися 4G;
- ✓ затвердили план використання радіочастотного ресурсу України до 2025 року. А також доповнено його новими базовими стандартами LTE/LAA, eLTE-U та PMP. Це дозволить користувачам отримувати більш стабільні та високі швидкості під час перегляду відео та прослуховування музики. А також дозволить збільшити покриття та надійність зв'язку, сприятиме автоматизації виробничих технологічних процесів.

✓ повноваженнями щодо надання фінансової підтримки місцевим бюджетам для розвитку широкосмугового доступу до інтернету в Україні наділено Міністерства цифрової трансформації;

25 жовтня цього року відкриття тестової зони технології 5G - 5G Lab - результат реалізації проекту Міністерства цифрової трансформації, Vodafone Україна, Huawei Ukraine та UNIT.City.

Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» (Указ Президента України від 26.08.2021 року № 447/202153). До викликів для України у сфері кібербезпеки віднесено змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо.

1 січня 2022 року набуде чинності Закон України від 16 грудня 2020 року № 1089-IX "Про електронні комунікації" [13] визначення правових та організаційних основ державної політики у сферах електронних комунікацій та радіочастотного спектра, а також прав, обов'язків та відповідальності фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами.

Дія цього Закону буде поширюватися на відносини у сферах електронних комунікацій та радіочастотного спектра щодо надання та отримання електронних комунікаційних послуг, постачання та доступу до електронних комунікаційних мереж, забезпечення конкуренції на ринках електронних комунікацій, а також щодо користування радіочастотним спектром, ресурсами нумерації та захисту прав користувачів послуг.

Цей Закон розроблено з урахуванням та метою імплементації до українського законодавства положень Кодексу електронних комунікацій, зокрема врегульовані базові питання розгортання високошвидкісних мереж, функціонування (створення) інфраструктури електронних комунікацій для розгортання високошвидкісних мереж.

2.2. Німеччина

Німецьке законодавство не передбачає виключення окремих постачальників 5G надавачів послуг. Натомість вимоги щодо безпеки, як правило, посилюються для всіх із застосуванням спеціальних правил щодо критичної інфраструктури.

[13] https://zakon.rada.gov.ua/laws/show/1089-20#n2128

Ці нові критерії визначені в новому каталозі безпеки для роботи телекомунікацій мереж, розроблених Федеральним мережевим агентством, і закон IT-безпеку. Закон про IT-безпеку 2.0 залишає німецькі мережі 5G відкритими для всіх виробників, і будь-яке таке виключення вимагало б серйозних доказів об'єктивний ризик.

Компетентні органи. Основним законом, що регулює німецькі телекомунікаційні мережі, є Закон про телекомунікації (Telekommunikationsgesetz або TKG)[14]. Розділ 109 TKG визначає певні цілі захисту та зобов'язань.

Розділ 109(1) TKG регулює питання захисту персональних даних та захисту конфіденційності телекомунікацій як загальні цілі захисту. Це відповідальність постачальника за кожну послугу для досягнення цих загальних цілей захисту.

Розділ 109(2) TKG визначає спеціальні цілі захисту, пов'язані із захистом телекомунікаційної інфраструктури від збоїв і ризиків, а також доступністю телекомунікаційних послуг. Погоня за тими особливим захистом цілі обмежуються операторами телекомунікаційних мереж загального користування та постачальників загальнодоступних телекомунікаційних послуг. Для досягнення цих загальних і спеціальних цілей захисту всі компанії повинні прийняти рішення щодо застосування технічних запобіжних та інших заходів. Запобіжні або інші заходи доцільні лише в тому випадку, якщо техніко-економічні зусилля, необхідні для цього, не є не пропорційними значущості телекомунікаційні мережі або послуги, які підлягають захисту (TKG, розділ 109(2), речення 5).

Компетентним органом з контролю за дотриманням розділу 109 TKG є Федеральне мережеве агентство, який є національним органом регулювання телекомунікацій. Федеральне управління досліджує та контролює ризики безпеки, пов’язані з використанням IT Управління інформаційної безпеки (Bundesamt für Informationssicherheit in der Informationstechnik або BSI), яке також розробляє превентивні заходи безпеки з цього приводу.

Завдання та повноваження BSI визначені у Законі про Федеральне відомство інформаційних технологій (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik або BSIG)[15]. Закон от 18 травня 2021 про IT-безпеку

[14] https://de.wikipedia.org/wiki/Telekommunikationsgesetz_(Deutschland)
https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/start.html

[15] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

2.0[16]виявлення та захист, BSI була збільшена компетенція у виявленні прогалин у безпеці та захисту від кібер-атак. Як центральний центр компетенції в галузі інформаційної безпеки BSI може розробити безпечне оцифрування і, серед іншого, встановити обов'язкові мінімальні стандарти для федеральної влади та більш ефективно контролювати їх. Кібербезпека в стільникових мережах: Закон містить ухвалу, яка забороняє використання критично важливих компонентів для захисту громадського порядку або безпеки в Німеччині. Оператори мережі також повинні відповідати високим вимогам безпеки, **а критично важливі компоненти повинні бути сертифіковані. Закон забезпечує інформаційну безпеку в мобільних мережах 5G.**

Захист прав споживачів, BSI буде незалежним та нейтральним консультаційним центром для споживачів з IT - безпеки питань на федеральному рівні. Захист споживачів тепер є завданням BSI. Введення єдиного знаку безпеки IT для громадян має зробити безпеку IT більш прозорою та відомою в майбутньому, продукти якої вже відповідають певним стандартам безпеки IT.

Безпека для компаній, коло критичних інфраструктур розширено за рахунок включення сектора утилізації побутових відходів. Крім того, інші компанії, що становлять особливий суспільний інтерес (наприклад, виробники озброєнь або компанії з особливо великим економічним значенням), повинні будуть вжити певних заходів безпеки IT та будуть включені в надійний обмін інформацією з BSI.

Національний орган сертифікації кібербезпеки: згідно з § 9a параграфа 1 BSI також відомий як Національний центр сертифікації кібербезпеки значенні параграфа 1 статті 58 Регламенту (EU) 2019/88 (CSA). Зокрема, відповідає за моніторинг та дотримання правил у рамках європейських схем сертифікації кібербезпеки. Дії з нагляду та сертифікації повинні бути суворо відокремлені одна від одної та здійснюватися незалежно.

Інформаційна безпека та оцифрування нероздільні. Це дві сторони однієї медалі та BSI. З IT – Sig 2.0, BSI, як потужний федеральний орган з кібербезпеки, необхідний для забезпечення успіху оцифровки. Тому що поради, інформування та попередження будуть все більш важливими в майбутньому.

Опис заходів кібербезпеки в рамках TKG

Оператори телекомунікаційних мереж загального користування та провайдери загальнодоступних телекомунікаційних служб повинні призначити офіцера безпеки та представити технічні та організаційні заходи захисту, які вони

16 https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1638976032416

вжили в концепції безпеки до Федерального мережевого агентства відповідно до розділу 109(4) TKG.

Дотримання цих вимог безпеки є обов'язковим для всіх компанії. Федеральне мережеве агентство регулярно перевіряє реалізацію концепцій безпеки(тобто принаймні кожні два роки).Основа концепції безпеки та технічних заходів та інших заходів, які необхідно вжити операторам є «Каталог вимог безпеки до функціонування телекомунікацій та даних системи обробки та обробки персональних даних відповідно до § 109 TKG» (Каталог Безпеки), який був розроблений Федеральним мережевим агентством за погодженням з BSI і Федеральним комісаром із захисту даних та свободи інформації.

Крім того, Федеральне мережне агентство може розпорядитися операторам телекомунікацій загального користування мережі або постачальники загальнодоступних телекомунікаційних послуг пройти перевірку кваліфікованим спеціалістом незалежного органу або компетентного національного органу (Стаття 109(7) TKG). Мета такого огляду полягає в тому, щоб визначити, чи були виконані вимоги розділу 109(1)–(3) TKG.

Безпека. Каталог також може стати основою для аудиту безпеки кваліфікованого незалежного органу відповідно до розділу 109(7) TKG.

Критичність Мережі. Концепція безпеки згідно з розділом 109(4) TKG має враховувати критичність мережі, тією мірою, в якій він повинен надати аналіз очікуваних небезпек.

Оцінка критичності враховує загальні інтереси, захищені розділами 109 (1) і (2) TKG:телекомунікаційну таємницю, захист даних та функціональність мережі.

Вирішальним фактором у визначенні критичності є важливість телекомунікаційної мережі або послуг, яку потрібно захистити.

Критичність стандарту, всі телекомунікаційні мережі та послуги загального користування.

Підвищена критичність : телекомунікаційні мережі та послуги загального користування понад 100 000 передплатників.

Підвищена критичність: Телекомунікаційні мережі загального користування та послуги зі спецзначення для загального блага. Це торка́ється загальнодоступної мобільної мережі якої можна припустити використання поперечного перерізу.

Що стосується загальнодоступного мобільного зв'язку 5G мережі, які обслуговуються з кількістю абонентів понад 100 000.

Після завершення аналізу ризиків компанія-зобов’язана вибрати та впровадити відповідні, необхідні та відповідні захисні заходи.

Оцінка окремих випадків завжди є вирішальною для відбору та визначення. Це не абстрактне приписування небезпечній ситуації, а завжди результат конкретного аналізу індивідуальної небезпеки, яка є вирішальною для визначення захисного засобу заходу.

По-перше, при визначенні міри необхідно враховувати стан техніки. По-друге, захисні заходи, які слід вживати в окремих випадках, доцільні лише за умови технічного та економічного зусилля відповідним чином пропорційні важливості прав, які підлягають захисту, і важливості об'єктів, які підлягають охороні для населення.

Не повинно бути різниці між зусиллями приносити користь широкій громадськості.

Базовий збірник захисту IT BSI (IT-Grundschutz Kompendium) пропонує допомогу у виборі конкретних заходів.

Загальні заходи згідно ТКГ.

Організаційне управління та управління ризиками включає управління постачальниками, далі до якого:

- ✓ надійність третьої сторони повинна бути оцінена на основі відповідної інформації введення в експлуатацію
- ✓ треті сторони повинні бути зв'язані контрактом, який включає вимоги безпеки;
- ✓ треті сторони зобов’язані діяти відповідно до закону про захист даних через відповідні договірні домовленості;
- ✓ дотримання вимог безпеки контролюється на регулярній основі;
- ✓ вимоги безпеки до управління персоналом, що включає перевірку безпеки, охорона експертизи та поінформованість, врегулювання кадрових змін та усунення порушень;
- ✓ безпека систем і засобів даних, наприклад безпечна обробка конфіденційних даних, інформації та зв'язку, метаданих, фізичного та елементарного захисту вимог, безпеки постачання, контролю доступу, захисту цілісності та наявності мережевих та інформаційних систем, захисту від вірусів, ін'єкцій коду та інше шкідливе програмне забезпечення;
- ✓ належне та безпечне управління, управління змінами та активами;
- ✓ виявлення, реакція та повідомлення про несправності та інциденти безпеки;
- ✓ відповідна стратегія управління аварійними ситуаціями або аварійними ситуаціями;

- ✓ моніторинг подій, пов’язаних із безпекою, надзвичайних навчань та процедур тестування мережа та IT-системи.

Конкретні заходи застосовуються до мереж і послуг з підвищеною критичністю.

Щодо впровадження мережі 5G.

Частоти 700 МГц надано в червні 2015 року.

«5G для Німеччини», осінь 2016

Шлях карта спектра 5G, 2018.

Остаточні умови аукціону 5G, листопад 2018

Аукціон 5G у діапазоні 4–3,7 ГГц (300 МГц) та 2 ГГц (2 × 60 МГц) завершився у червні 2019 року та зібрав 6,55 млрд євро (з яких 4,18 млрд євро за спектр 36 ГГц). Ліцензії включають зобов'язання щодо страхового покриття.

100 МГц зарезервовано для місцевих та регіональних цілей у спектрі 3,7–3,8 ГГц. Програми відкриваються на 21 листопада вул., 2019.

Очікується, що спектр 26 ГГц буде потенційно надано після подання заявки.

Vodafone та Deutsche Telekom запустили 5G у липні 2019 року, Telefonica – у жовтні 2020 року. Новий гравець 1&1 Drillisch ще не запустив 5G.

Ініціативи 5G

Bundesnetzagentur опублікував свій "Компас частот" у липні 2016 року з метою визначення областей для регуляторних дій щодо спектру для 5G. Докладніші орієнтири були опубліковані в грудні 2016 року.

Восени 2016 року уряд запустив свою «Ініціативу 5G для Німеччини»[17]. У документі, опублікованому у вересні 2017 року, федеральний уряд визначає національну стратегію 5G (контекст, дії, розгортання) на період до 2025 року. У ньому визначено п'ять областей дій, ключові етапи та виділено 80 млн євро на дослідницькі ініціативи 5G у дослідницьких центрах 5G.

На основі представлених думок NRA Німеччини опублікувало ключові елементи та в червні 2017 року оголосило офіційний запит на загальнонаціональні присвоєння в діапазонах 2 ГГц та 3,6 ГГц.

Січень 2018 року NRA Німеччини випустило проект консультації, в якому йдеться, що дефіцитний спектр у діапазонах 2 та 3,6 ГГц буде проданий з аукціону. Рішення I та II були опубліковані у травні 2018 року.

[17] https://www.bmvi.de/SharedDocs/EN/publications/5g-strategy-for-germany.pdf?__blob=publicationFile#:~:text=The%20conditions%20for%20the%20rollout,by%202020%20at%20the%20latest.&text=bre%20optic%20is%20required%20to,have%205G%20connectivity%20by%202025.

У смузі частот 2 ГГц, 2×40 МГц будуть доступні з 1-го січня 2021 Додатковий 2×20 МГц буде доступний з 1-го січня 2026 року.

У смузі частот 3,6 ГГц (3,4-3,7 ГГц), деякі з спектра не призначається де - факто на загальнонаціональній основі (до 2021/2022) буде доступний як з 1 - го січня 2022 року (раніше стадії , як з 2019 року). Інші громадські ініціативи нагородити умови та правила аукціонів 5G були випущені 26 листопада – го 2018 року.

Весна 2019 року продаж 5G спектру. Процедура кваліфікації відкрита з 26 листопада - го 2018 року до 25 січня - го , 2019 умови покриття були посилені , а розклад 5G , здається, були пом'якшені. Умови встановлюються у два етапи (2022 та 2024 роки). BNetzA тепер має підготувати процес подання заявок для вертикалей (переважно промислових об'єктів) для верхніх 100 МГц 3,6 ГГц (3,7–3,8 ГГц) протягом кількох тижнів.

Мінімальна швидкість передачі даних 100 Мбіт/с, буде доступна до кінця 2022 року в 98% домогосподарств у кожній з земель, на всіх федеральних автомагістралях, на всіх основних дорогах і вздовж основних залізничних маршрутів.

Правила мінімального покриття не застосовуватимуться до жодного нового учасника. Документ Bundesnetzagentur також включає вимогу, що оператори працюватимуть разом над забезпеченням покриття в областях, які є економічно невигідними для встановлення кожним з них власного обладнання.

Вимоги до покриття:

✓ не менше 100 Мбіт/с як мінімум для 98% домогосподарств у кожній з земель до кінця 2022 року,

✓ не менше 100 Мбіт/с та максимальна затримка 10 мс для всіх автомагістралей Німеччини до кінця 2022 року.

✓ не менше 100 Мбіт/с та максимальна затримка 10 мс для всіх федеральних доріг з рівнями функції підключення 0 або 1 до кінця 2022 року,

✓ не менше 100 Мбіт/с та максимальна затримка 10 мс для всіх інших федеральних доріг до кінця 2024 р.

✓ не менше 50 Мбіт/с для всіх державних доріг до кінця 2024 р.

✓ не менше 50 Мбіт/с для морських портів та опорної мережі внутрішніх водних шляхів до кінця 2024 р.

✓ не менше 100 Мбіт/с для залізничних маршрутів з більш ніж 2000 пасажирів на день до кінця 2022 року, не менше 50 Мбіт/с для решти залізничних маршрутів до кінця 2024 року,

До кінця 2022 року, експлуатація 1000 «базових станцій 5G» та Робота 500 базових станцій зі швидкістю передачі не менше 100 Мбіт/с у непотових зонах.

Аукціони з використання діапазону 3,6 ГГц розпочалися у березні 2019 року. 5 червня 2019 року регулятор збільшив мінімальні ставки, намагаючись завершити аукціон із продажу спектра 5G. Процес завершився 12 червня 2019 року та зібрав 6,55 млрд євро після 497 раундів. Deutsche Telekom запропонувала 2,17 мільярда євро за 130 МГц із 420 МГц спектра, розподіленого в частотах 2 та 3,6 ГГц. Vodafone отримала 130 МГц за 1,88 мільярда євро, а Telefonica – 90 МГц за 1,42 мільярда євро. Drillisch заплатила 1,07 млрд. євро за 70 МГц. Частоти будуть доступні з 2021 чи 2026 року.

У вересні 2019 року оновлено національну стратегію мобільного зв'язку Було оголошено план з п'яти пунктів та погоджено план на 1,1 млрд євро для покращення покриття мобільного зв'язку. Центральна тема стосується питань покриття (розширення покриття) і особливо способів і засобів зменшення білих плям в 4G і, як наслідок, в 5G.

Національні оператори мобільного зв'язку погодилися: надавати надійні послуги передачі голосу та даних у 99% домогосподарств по всій країні до кінця 2020 року та 99% домогосподарств у кожній з земель до 2021 року, особливо у сільській місцевості; 1) не менше 1400 щогл, доступних для будь-якого оператора; 2) забезпечити мінімальну швидкість 100 Мбіт/с на основних транспортних маршрутах; 3) встановити базові станції в «білих плямах» сільських районів, що не обслуговуються. Для муніципалітетів будуть відкриті спеціальні фонди, щоб допомогти їм зробити активний внесок у покращення покриття мобільного зв'язку. Оператори мобільного зв'язку погодилися розділити 6000 сайтів 5G у сільській місцевості та на транспорті.

2.3. Королівство Швеція

Шведське законодавство не містить жодних загальних положень, які регулюють, наприклад, «постачальників з високим ризиком», але визначає процедури (необхідність) їх попереднього затвердження. Останні зміни посилили критерії безпеки для електронних комунікацій з міркувань національної безпеки.

Усі постачальники, які мають намір брати участь у розгортанні мереж 5G у Швеції, мають пройти незалежну перевірку безпеки в Управлінні пошти та телекомунікації Швеції (PTS)[18], яке з цих діє у співпраці зі Збройними Силами та Військовою розвідкою та службою безпеки Швеції.

Послуга, яка проводиться за технічними критеріями та одним політичним критерієм. Відповідність одному з критеріїв є достатнім для того, щоб оператор

[18]Шведське агентство пошти та телекомунікації - це орган, який контролює галузь електронного зв'язку та пошти у Швеції https://www.pts.se/en-gb/

або постачальник були виключені з претендентів на отримання ліцензії або від постачання власники ліцензій.

Рішенням від 20 жовтня 2020 року PTS додав додаткову умову рішення щодо умов для власників ліцензій 5G, відповідно до яких вони не можуть використовувати продукти або послуги від Huawei або ZTE

Компетентні органи та відповідне законодавство. У Швеції PTS відповідає за регулювання та моніторинг електронних комунікацій та відповідних операторів. Таким чином, він також є основним органом для вирішення питань кібербезпеки.

Законодавство згідно з яким PTS розглядає потенційні ризики національної безпеки, є Закон про електронні комунікації 2003 [Sw: Lag (2003:389) om elektronisk kommunikation][19]. Очікується, що законодавство буде оновлено та відповідатиме Кодексу.

Опис заходів кібербезпеки. Закон про електронні комунікації 2003 року (ECA03) регулює використання електронних комунікацій у Швеції забезпечити доступ до безпечних та ефективних електронних комунікацій.

Відповідно до ECA03, оператори, які хочуть здійснювати радіопередачу та пов'язану діяльність у Швеції, повинні спочатку звернутися до PTS для отримання офіційного дозволу (глава 2, параграф 1 ECA03).

Ліцензії на використання радіопередавача (Розділ 3, параграф 6 ECA03). Ліцензії на використання радіопередавача повинні надаватися якщо:

- ✓ можна припустити, що радіопередавач буде використовуватися таким чином, що ризик для заборонених шкідливих перешкод не виникає;
- ✓ використання радіо означає ефективне використання радіочастот;
- ✓ можна припустити, що використання радіо не буде перешкоджати такому радіозв'язку особливо важливо з огляду на вільне формування думки;
- ✓ використання радіо не використовує радіочастоти, які необхідні для підтримки розумного, готовність до розвитку існуючих і нових видів використання радіо або частот, для яких використання радіо було гармонізовано відповідно до міжнародних угод, до яких Швеція приєдналася або прийняла положення Договору про заснування Європейського Союзу.

Можна припустити, що використання радіо не порушить необхідні радіочастоти для операцій, зазначених у главі 3. Беручи до уваги той факт, що у заявника раніше було відкликано ліцензію чи інші подібні обставини, немає обґрунтованих підстав вважати, що радіопередавач буде використовуватися з порушенням умов ліцензії. Також, можна припустити, що використання радіо не

[19] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003389-om-elektronisk-kommunikation_sfs-2003-389

завдасть шкоди безпеці Швеції. Ліцензія на використання радіопередавача може бути комбінована з умовами щодо: частоти, на які стосується ліцензія; електронні комунікаційні послуги чи тип електронних комунікаційних мереж або методи, до яких відноситься ліцензія; охоплення та розгортання в межах Швеції; географічний район, у якому може використовуватися мобільний радіопередавач; зобов'язання програми ділитися частотним спектром з іншою стороною. Таке питання, як згідно з рішенням про гармонізоване використання радіочастот повинні бути встановлені як умови, коли сторона, якій буде виділена радіочастота, була призначені відповідно до міжнародних угод або Договору про створення Європейського Союзу; зобов'язання, що виникають відповідно до чинних міжнародних угод щодо використання частот; зобов'язання, які були зроблені у зв'язку з наданням ліцензії, кількість ліцензій у частотному спектрі обмежена;

технічні вимоги та інші вимоги для забезпечення фактичного та ефективного використання частоти; і вимоги, важливі для безпеки Швеції.

Однак такі умови можуть бути встановлені лише у разі необхідності, наприклад, для уникнення шкідливих перешкод, забезпечення ефективне використання частот, захист життя і здоров'я людей, задоволення суспільних інтересів у наявності певні електронні комунікаційні послуги, доступні в Швеції.

Цей процес попереднього затвердження (у поєднанні з можливістю встановлення певних умов для ліцензіатів) загалом вважається достатнім для усунення будь-яких потенційних ризиків безпеки, пов’язаних з радіопослугами.

1 січня 2020 року поправки до Закону про електронні комунікації набули чинності, визначає, що ризики для національної безпеки враховуються до (і після) надання ліцензії.

Оновлена редакція Закону про електронні комунікації, передбачає:

- ✓ PTS має враховувати інтереси національної безпеки Швеції при розгляді заяви на дозвіл на використання радіопередавача ;
- ✓ дозвіл може залежати від вимог щодо забезпечення безпеки Швеції.

Ліцензія/дозвіл, видана до 1 січня 2020 року, може бути передана іншому оператору за згодою PTS, якщо можна вважати, що він не завдає шкоди безпеці Швеції.

Дозвіл може бути відкликано або умови можуть бути змінені з негайним вступом в силу, якщо радіопередача завдала шкоди Швеції або, як можна вважати, заподіяла шкоду безпеці держави.

До процесу перевірки мають бути залучені Поліція безпеки та Збройні Сили Швеції, які також можуть оскаржити рішення про видачу дозволів з мотивів національної безпеки.

Надійність експлуатації. Провайдер мереж зв'язку загального користування або загальнодоступні послуги електронного зв'язку повинні вживати «відповідних технічних та організаційних заходів», щоб переконатися, що бізнес відповідає «розумним вимогам» щодо операційної надійності.

Такі заходи має бути придатним для створення такого рівня безпеки, який, враховує наявні технології та витрати на реалізацію заходів, адаптований до ризику зриву та переривання.

Захист даних. Закон про електронні комунікації передбачає, що постачальники публічних електронних комунікаційних послуг повинні приймати«відповідні технічні та організаційні заходи» для забезпечення захисту даних, що обробляються у зв'язку з наданням послуги, а також «необхідні заходи» для її підтримки захисту у мережі (гл. 6, п. 3). Будь-які вжиті заходи мають бути спрямовані на забезпечення того рівня безпеки, який з урахуванням наявної технології та витрат на впровадження таких заходів, що адаптовані до ризику інцидентів із конфіденційністю.

Якщо трапиться інцидент, постачальник повинен без зайвої затримки повідомити PTS.

Інші нормативні акти. Оскільки PTS має провести оцінку ризику національної безпеки разом із військовою розвідкою та службою безпеки Збройних сил Швеції, відповідні зміни також були внесені до Закону про публічну конфіденційність для забезпечення обміну інформацією між цими державними органами.

Позиція Служби безпеки Швеції щодо консультацій з PTS перед наданням частотних ліцензій визначені технічні критерії, які слід враховувати при оцінки ризику здобувачів частотної ліцензії:

Оператор повинен показати, що центральні функції[20] працюють і доступні в Швеції у разі збою. Здобувач також повинен мати план обробки. У Швеції повинні зберігатися дані про інциденти або збої безпеки, а також системні або користувацькі дані .

Оператор повинен мати можливість легко і швидко від'єднувати точки підключення до сторонніх країни, не впливаючи на мережу. Відповідно, він повинен мати план забезпечення функціональності мережі у разі інциденту безпеки з-за кордону та продемонструвати, яким чином можна запобігти зовнішньому впливу. Оператор повинен надати специфікації щодо функцій, необхідних для забезпечення високої доступності та секретності мережі, а також

[20] Центральні функції визначаються широко як усі «функції в мережі радіодоступу, мережі передачі, ядрі мережі та мережі обслуговування та обслуговування, які необхідні для підтримки функціональності мережі та електронної послуги зв'язку, що надаються власником ліцензії.

продемонструвати наявні запобіжні заходи захисту цих функції. Оператор повинен мати налагоджені процеси для відстеження та ідентифікації мережевого трафіку та мінімізувати ризик використання компонентів для відстеження та маніпулювання. Це повинно також свідчити про прозорість та контроль над своїми постачальниками. Оператор повинен передбачити заходи для захисту центральних функцій від несанкціонованої маніпуляції.

Центральні функції мережі повинні знаходитися в Швеції і не можуть бути доступні із за кордону. Мережа повинна бути спроектована таким чином, щоб запобігти несанкціонованому відстеженню послуг, пропускної здатності, розташування або користувачів. Мережа повинна бути спроектована так, щоб запобігти несанкціонованим атакам (наприклад, кібератакам) і, де можливо, виявляти та запобігати ним.

Оператор повинен:

✓ встановити відповідні процедури авторизації для доступу до системи управління центральними функціями.

✓ активно допомагати галузевому органу у розумінні та контролю над сектором, шляхом встановлення процедур звітності та інформації

✓ розробляти, впроваджувати, експлуатувати та підтримувати відповідні заходи безпеки, та повинен відповідним чином повідомити відповідний орган та посилатися на кожен з вищезазначених принципів.

✓ мати встановлені процедури щодо входу, оцінки журналу та огляду безпеки обладнання, підключеного до центральних функцій. *Обладнання, персонал та служби для центральних функцій мережі повинні бути розташовані в Швеції. Інциденти безпеки повинні оброблятися в Швеції, а дані користувачів повинні зберігатися в Швеції.*

✓ постійно надавати інформацію призначеним галузевим органом одержувачам на щодо дій, вжитих у мережах зв'язку, які можуть вплинути на секретність, сила, доступність, проникливість або контроль.

✓ надавати інформацію вчасно, щоб галузевий орган міг визначити, які ризики пов'язані з заходами, що вживаються в мережах зв'язку, та чи потрібно вживати заходів.

✓ забезпечити персонал, який має доступ до даних, які можуть вплинути на конфіденційність, точність, міцність і доступність схвалені та пройшли навчання з безпеки захист та усвідомлення таємниці інформації

Остаточний політичний критерій спрямований на оцінку ймовірності впливу оператора або постачальника. Такий вплив/тиск може бути застосований, але не обмежується наявністю наступних факторів:

✓ зв'язки, *включаючи інтереси власності, а також інші зв'язки з урядом або органом третіх країн (країни, що не входять до ЄС);*

✓ законодавство третьої країни, *особливо в тих випадках, коли діють інші правові правові або демократичні принципи, або вони відсутні або там де не можуть застосовуватися угоди про безпеку чи захист даних*;
✓ посилання на країни чи організації, які беруть участь у наступальних кібероперацією чи інші антагоністична діяльність проти Швеції;
✓ інші можливості для третіх країн чинити тиск, у тому числі щодо географічного розташування виробничих фондів.

Проект Закону про електронні комунікації 2020 року (ECA20). У вересні 2019 року уряд Швеції оголосив про свій план заміни ECA03 на новий Закон про електронні комунікації 2020 року (ECA20). Метою Закону є гармонізація законодавства Швеції з законодавством ЄС шляхом впровадження положень Кодексу. Ці зміни спрямовані на врахування розвитку ринку та запровадження тотожною Кодексу структури закону. ECA03 набув чинності, а офіційна законодавча пропозиція (після завершення відповідних кроків законодавчому процесі, включаючи офіційні процеси запитів і консультацій) ще не подана.

Проте, згідно з запропонованою наразі формулюванням, загальна вимога враховувати безпеку Швеції щоразу, коли вводиться новий закон (глава 1, параграф 1) для врахування швидкого розвитку технології та збільшення обміну інформацією через електронні комунікації. Залежно щодо відгуків, отриманих на етапах консультацій, це формулювання може бути змінено або внесено уточнення додано до остаточної законодавчої пропозиції після внесення.

Станом на 2 грудня 2021 року, відсутня інформація статусу урядової пропозиції ECA20[21].

Оцінка ризику. У квітні 2020 року оновлено PTS керівництво з оперативної безпеки (PTS Guidance). Згідно до оновленого керівництва, постачальники послуг електронного зв'язку повинні виконувати роботи з безпеки експлуатації, які мають проводитися в довгостроковій перспективі, безперервно і систематично. Це включає аналіз потенціалу ризиків порушення або переривання роботи мережі або її послуг не рідше одного разу на рік, а також прийняття відповідних заходів для захисту від такого порушення/переривання.

Зокрема, слід враховувати наступне:

✓ вторгнення та інше зовнішнє втручання (як фізичне, так і логічне);
✓ загрози, пов'язані з погодою (природними явищами);
✓ заплановані зміни та оновлення мережі та сервісів.

Шведські оператори зобов’язані проводити повну оцінку ризиків (включаючи обидва ризики згадані вище та аналіз загрози мережевого саботажу)

[21] https://www.pts.se/en/english-b/regulations2/legislation/electronic-communications-act/

перед закупівлею нових продуктіві послуги (параграф 5) для подолання ризиків, які виникли під час запланованого в країні впровадження 5G.

Ці правила узгодженні із заходами, рекомендованими ЄС, а також запроваджені суворіші вимоги до документації операторів. Зокрема, вони вимагають від операторів зберігати будь-які документи, пов'язані з закупівлями, до п'яти років та відповідати на інформаційні запити від PTS щодо потенційних загроз для національної мережі.

20 жовтня 2020 року, на основі процедури ECA03, PTS, після відібрав відповідних учасників (Hi3G Access, Net4 Mobility, Telia Sverige та Teracom), та встановив додаткові умови аукціону ліцензії 5G, які накладають сувору заборону на використання обладнання від Huawei та ZTE майбутніми власниками ліцензій.

Це рішення ґрунтувалося на тій підставі, що вони нібито представляють загрозу національній безпеці Швеції. На практиці нові установки та нове впровадження центральних функції для використання радіо в діапазонах частот не повинні застосовуватись з продуктами з цих двох постачальників; і якщо існуюча інфраструктура для центральних функцій буде використана для надання послуг відповідні діапазони частот, продукти від Huawei та ZTE, які вже використовуються, мають бути припинені до, алене пізніше 1 січня 2025 року.

Підсумовуючи нормативний огляд Швеції зауважимо, що тимчасова судова заборона спочатку запуску аукціону 5G за умови застосування додаткових ліцензійних умов в листопаді 2020 року, але аукціон був санкціонований рішенням суду при оскарженні. Аукціони відбулися 19 січня 2021 року. Судова справа по суті триває. Швеція зараз також працює над створенням Національного центру кібербезпеки для посилення інформаційної безпеки та стійкості Швеції до кібератак.

10 грудня 2020 року уряд офіційно доручив Національній оборонній радіостанції (FRA, National Defence Radio Establishment, is a civil authority subordinated to the Ministry of Defence)[22], Збройним силам Швеції, Шведському агентству з надзвичайних ситуацій (MSB)[23] та Поліції створити цей центр призначено фінансування на його створення та функціонування до 2025 року. Діяльність цього центру буде розвиватися поступово з 2021 до 2023 року.

---

[22] FRA — це цивільний орган, підпорядкований Міністерству оборони, створено в 1942 р. Головний офіс FRA розташований у Ловені, на захід від Стокгольма. Діяльність із розвідки сигналів здійснюється з різних місць по всій країні. FRA надає розвідувальні дані уряду Швеції, шведським збройним силам та іншим зацікавленим органам.
FRA також надає послуги кібербезпеки для окремих державних органів і державних компаній. FRA займається виявленням та заходами проти кібератак, спрямованих на критично важливу національну IT-інфраструктуру Швеції. https://www.fra.se

[23] https://www.msb.se/en/

Щодо запровадження мережі.

Стратегія 5G Швеції - “Повністю підключена Швеція до 2025 року – стратегія широкосмугового зв’язку” (березнь 2017 р.) [24].

Пробні ліцензії були надані за принципом «перший прийшов першим обслужений» і дійсні з 2017 року до 31 грудня 2019 року. 200 МГц спектру було надано в діапазоні 3,4–3,6 ГГц і 1000 МГц у діапазоні 24,25–27,5 ГГц

У травні 2018 року Північні країни підписали лист про наміри щодо поглиблення співробітництва у сфері 5G.

Аукціон 700 МГц відбувся в грудні 2018.

Аукціон на частотах 3 і 3,5 ГГц, спочатку запланований на березень 2020 року, був перенесений на 10 листопада 2020 року, а заявки були запрошені до 30 червня 2020 року, а відновлено 19 січня 2021 року.

320 МГц буде продаватися в діапазоні 3,5 ГГц (3400-3720 МГц) у кількості до 15 ліцензій.

Одна ліцензія включатиме 40 МГц спектру, інші 14 лише 20 МГц. Резервна ціна встановлена на рівні 100 MSEK (9,5 MEUR) за блок. Частина 3720-3800 МГц буде доступна на локальній мережі

80 МГц буде продаватися на частотах 2300 МГц з 8 блоками по 10 МГц, проданими з резервом 20 MSEK (1,9 MEUR).

PTS відкрив додаткові пробні ліцензії для 5G в частотах 6 ГГц-3,8 ГГц, 3,8 ГГц-4,2 ГГц, 40,5 ГГц-43,5 ГГц, 45,5 ГГц-47,0 ГГц, 47,2 ГГц-48,0 ГГц і 66 ГГц-71 ГГц. Тестування вже проводиться з використанням спектру 3,4 ГГц-3,6 ГГц і 26,5 ГГц-27,5 ГГц.

Запуск 5G Tele2 і Telia у травні 2020 року, Tre в червні 2020 року і Telenor у жовтні 2020 року.

2,3 та 3,5 ГГц

Регулятор запропонував до 15 блоків принаймні 20 МГц на частотах 3400 МГц-3720 МГц (ліцензія матиме 40 МГц), а також до 8 загальнонаціональних ліцензій на 2,3 ГГц, з щонайменше 10 МГц спектром кожна.

Кожен учасник торгів може отримати щонайменше 80 МГц спектру в діапазоні 3,5 ГГц. Мінімальна ставка установлена на рівні 100 млн шведських крон (9,7 млн євро) за лот 3,5 ГГц (загалом 146 млн євро). Резервна ціна за ліцензію на частоту 2,3 ГГц встановлена на рівні 20 мільйонів шведських крон

[24] https://www.government.se/496173/contentassets/afe9f1cfeaac4e39abcdd3b82d9bee5d/sweden-completely-connected-by-2025-eng.pdf

(1,9 мільйона євро), що становить 160 мільйонів шведських крон (15,6 мільйона євро).

У квітні 2020 року PTS оголошено аукціон на 10 листопада 2020 року, заявки приймалися до 30 червня. У листопаді 2020 року аукціон знову відклали через оскарження пункту, що забороняє ліцензіатам використовувати обладнання Huawei.

Чотири компанії (Telia, Net4Mobility, Tre і Teracom отримали дозвіл на участь у продажу. Наприкінці грудня 2020 року PTS оголосила, що аукціон має відновився 19 січня 2021 року. Розгляд судової справи триває.

2.4. Фінляндська Республіка

Фінляндія має репутацію однієї з найбільш кібербезпечних держав у світі та передову законодавчу базу. Однак немає конкретного виключення окремих категорій постачальників. Законодавству у цій галузі властиві суворі вимоги безпеки, оцінки ризиків постачальників, і можливістю встановлення обмежень щодо використання певного обладнання.

Компетентні органи та відповідне законодавство. Фінське агентство транспорту та зв'язку (Traficom)[25] відповідає за моніторинг та просування ринків і послуг зв'язку у Фінляндії. З 2014 року Національний центр кібербезпеки (NCSC-FI)[26] працює в рамках Traficom. Це національний орган інформаційної безпеки та підтримує загальнонаціональну обізнаність про кібербезпеку.

Опис заходів кібербезпеки.

Закон "Про послуги електронного зв'язку"[27] (AECS). NCSC-FI контролює діяльність та кількість операторів, у тому числі традиційних телекомунікаційних операторів, провайдерів зв'язку мереж і послуг зв'язку, а також постачальників цифрової інфраструктури згідно з Директивою NIS.

Багато заходів, запропонованих в Інструментарії ЄС, вже діють або встановилися на практиці Фінляндія, наприклад:

- ✓ вимоги до якості мереж і послуг зв'язку (пункти 243-244 AECS , параграф 260 AECS);
- ✓ можливість застосування обмежень щодо обладнання, яке, як вважається, становить «ризик» для людей здоров'я, безпека чи інші суспільні інтереси (AECS, параграф 262);
- ✓ вимоги до якості комунікаційних мереж та послуг AECS надає детальну інформацію про те, як телекомунікаційні компанії та інші відповідні оператори

[25] https://www.traficom.fi/fi/ https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

[26] https://www.kyberturvallisuuskeskus.fi/en

[27] https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf

повинні діяти для забезпечення інформаційної безпеки в своїх мережах і сервісах. Зокрема, у пункті 243 AECS встановлено вимоги до якості комунікаційних мереж та послуг, які розроблені, побудований та обслуговування для забезпечення того, серед іншого;

- ✓ технічний стандарт електронних комунікацій має високий рівень інформаційно безпечний;
- ✓ вони можуть витримувати звичайні та передбачувані кліматичні, механічні, електромагнітні, та інші зовнішні втручання, а також загрози інформаційній безпеці;
- ✓ можна контролювати продуктивність, функціональність, якість та надійність;
- ✓ можуть бути виявлені значні порушення та загрози інформаційній безпеці (це також включає виявлення помилок і збоїв, які істотно порушують функцію мережі/послуги);
- ✓ захист даних, інформаційна безпека чи інші права не порушуються;
- ✓ вони є взаємосумісними (інтероперабельними), і комунікаційні мережі можуть бути підключені до іншої мережі зв'язку при необхідності;
- ✓ зміни, внесені до них, не викликають непередбачених перерв в інших комунікаціях мережі та послуги.

Оцінка ризику (п. 251 AECS), будь-яке радіообладнання, яке використовується у Фінляндії, повинно відповідати низці вимог, у тому числі пов’язані з:

- ✓ охороною безпеки і здоров'я людей і тварин, охорона майна;
- ✓ електробезпекою;
- ✓ адекватними рівнями електромагнітної сумісності; і
- ✓ ефективним використання радіочастот (у тому числі з метою уникнення шкідливих втручань).

У разі наявності у Traficom підстави вважати, що певне радіообладнання становить потенційний ризик для здоров’я людей або безпеці, або інші аспекти, що становлять суспільний інтерес, він повинен провести повну оцінку того, чи є це відповідністю встановленим вимогам законодавства.

Якщо зроблено висновок про невідповідність радіообладнання вимогам законодавства, Traficom може зобов'язати провайдера прийняти відповідні коригувальні дії для приведення його у відповідність, або вилучити обладнання з ринку (тобто переконатися, що більше не продається) або відкликати його (тобто забрати назад) протягом розумного часу (як це встановлено органом влади).

Однак, навіть якщо орган влади дійшов висновку, що дане обладнання відповідає вимогам, встановлені законом, все одно можливо зобов'язати

постачальника вжити відповідних заходів, вилучити обладнання або відкликати його (параграф 262), але лише там, де буде виявлено, що обладнання не відповідає (порушує) суспільні інтереси.

Інформаційна безпека.

Згідно з параграфом 247 AECS, постачальники комунікацій повинні забезпечити інформаційну безпеку послугам, повідомленням, даним про трафік та даним про місцезнаходження під час передачі повідомлень.

Заходи безпеки повинні бути спрямовані на забезпечення належного рівня безпеки, враховуючи серйозність загроз, рівень технічного розвитку для захисту від загроз і витрати, понесені заходами.

Закон також визначає, що постачальники комунікацій (і постачальники послуг із доданою вартістю) можуть вживати «необхідних» заходів для забезпечення інформаційної безпеки з метою, наприклад, виявлення, запобігання і розслідування перешкод, які можуть негативно вплинути на інформаційну безпеку в комунікаційних мережах або службах, підключених до них та в інформаційних системах, які створюють перешкоди, що підлягає попередньому дослідженню (п. 272).

Це включає такі заходи, як автоматичний аналіз повідомлення, запобігання надсилання/отримання повідомлень або автоматичне видалення шкідливої комп'ютерної програми.

Зміни до Закону про послуги електронного зв'язку. Уряд Фінляндії ввів нові положення до цього закону, який набули чинності з 1 січня 2021 року з метою імплементації положень Кодексу електронних комунікацій.

Зокрема, доповнено положеннями щодо можливості обмеження конкретного мережевого обладнання в критичних частинах комунікаційної мережі, «*якщо є серйозні підстави підозрювати, що використання обладнання може загрожувати національній безпеці або національній обороні».*

До загроз національній безпеці належать такі види діяльності, які загрожують життю чи здоров'ю людей чи життєдіяльності суспільства, а також діяльність іноземної держави чи компанії, що знаходиться під його тісним впливом, що може зашкодити міжнародним відносинам Фінляндії, економічним або іншим важливим інтересам, або іноземній розвідці.

Такі положення надають Traficom повноваження зобов'язати оператора видалити комунікації мережевого обладнання зі своєї мережі. У цьому відношенні «критичними частинами» вважаються ті, які використовується для централізованого управління мережею та комунікаціями, що проходять через неї («ядро»).

Також Traficom зобов'язаний провести консультації з власником комунікаційної мережі та дати їй можливість усунути недоліки безпеки, перш ніж приймати рішення (крім випадків, коли терміновість вимагає негайного реагування).

Запроваджено також нову Консультативну раду з мережевої безпеки для оцінки забезпечення національної безпеки в мережі зв'язку.

До цієї консультативної ради має входити як представники фінської адміністрації, так і представники ключових телекомунікаційних компаній. Наприклад, ця рада має контролювати розробку та адресувати/виробляти рекомендації щодо:

- ✓ розвитку комунікаційних мереж і технологій;
- ✓ визначення критичних частин комунікаційних мереж;
- ✓ сприяння та захисту національної безпеки в мережах зв'язку, зокрема критичні частини мережі;
- ✓ заходів з боротьби з ризиками, що впливають на безпеку мереж зв'язку та реалізації національної безпеки;
- ✓ внесення змін до законодавства для підвищення безпеки мережі.

Власник мережі зв’язку має право на компенсації (на основі фактичної вартості та фінансових втрат) від фінської держави за будь-яку мережу обладнання, яке має бути вилучено згідно з новими змінами.

Загалом, це право на компенсації застосовується лише до пристроїв комунікаційної мережі, які були введені в експлуатацію раніше.

Однак, де обладнання було введено на пізнішому етапі, але демонтаж ґрунтується на «значній істотній зміні обставин» або іншій причині, якої не могло бути якщо розумно передбачити, компенсація все одно може бути отримана.

Outlook.13 січня 2021 року Міністерство транспорту і телекомунікацій оприлюднило проект Програми розвитку кібербезпеки для громадського коментаря. Ця програма має на меті орієнтувати розвиток кібербезпеки на кількох рівнях суспільства, від приватних осіб до державних установ.

Зокрема, програма передбачає посилене навчання з кібербезпеки на різних рівнях інструкції, посилення готовності та моніторинг з боку державних органів, узгодження вимоги до кібербезпеки в ключових секторах та підтримка фінської галузі кібербезпеки. Програма передбачає фінансування цих цілей до 2025 року.

Щодо впровадження мережі. Фінляндія вже виставила на аукціон ліцензії на частоти 700 МГц (листопад 2016 року), 3,5 ГГц (вересень 2018 року), і діапазони 26 ГГц (червень 2020р.). В умовах аукціону передбачалося здійснення перевірки технологій перед впровадженням мережі.

Elisa, перша мережа 5G в Європі, запущена в червні 2018 року. Відтоді всі гравці запустили 5G.

Дострокове надання пробних ліцензій великій кількості компаній (жовтень 2015 – жовтень 2017).

Аукціон для спектру 26 ГГц (25,1-27,5 ГГц) завершився 8 червня 2020 року. Потужні оператори MNO отримали ліцензію 5G за 7 мільйонів євро, що дає їм право використовувати 800 МГц спектру.

5G Test Network Finland (5GTNF) — це консорціум промислових партнерів, дослідницьких організацій та державного сектору (включаючи постачальників Nokia і Ericsson, MNO Telia, DNA і Elisa, фінське транспортне та комунікаційне агентство Traficom, Business Finland, велика кількість фінських ІКТ -компанії, університети та науково-дослідні інститути), що забезпечують передове середовище для розробки 5G і вище, вертикальних індустріальних рішень, послуг, систем і продуктів на основі штучного інтелекту та кібербезпеки. Реалістичне середовище тестування телекомунікаційних технологій обслуговує велику кількість дослідницьких проектів і випробувань, заснованих на реальних потребах і вимогах вертикальної системи та послуг. Багатосайтове тестове середовище та мережа співпраці підтримує 5G та інші технології у дослідженні послуг і широкомасштабні польові випробування. Місцеві полігони знаходяться в Еспоо, Гельсінкі, Оулу, Тампере, Турку, Юлів'єска, Соданкюля та Куопіо.Наприкінці 2018 року Міністерство транспорту та зв'язку Фінляндії опублікувало нову стратегію цифрової інфраструктури під назвою «Перетворення Фінляндії у світового лідера в мережах зв'язку – стратегія цифрової інфраструктури 2025».

Детально описана стратегія сприяння впровадженню 5G та підтримки будівництва оптоволоконного кабелю у Фінляндії. Стратегія містить план розгортання 5G у Фінляндії і особливо стосується діапазонів 3,6 ГГц і 26 ГГц.

У січні 2020 року Фінляндія розпочала консультації щодо аукціону 26 ГГц, запланованого на літо 2020 року. Він включав спектр від 25,1 до 27,5 ГГц, за винятком найнижчої частини 850 МГц діапазону 26 ГГц, яка була зарезервована для локальних мереж 5G та досліджень і розробок або освітніх використання. Діапазон частот можна використовувати для мереж 5G з 1 липня 2020 року, а ліцензія дійсна на материковій частині Фінляндії до 31 грудня 2033 року.

3. КРАЇНИ БАЛТІЇ

В даний час в країнах Балтії вводяться правові рамки для усунення ненадійних постачальників, що не залишає жодних сумнівів у тому, що будь-які китайські технології[28] будуть допущені в мережах 5G.

Зважаючи на баланс можливостей та ризиків, пов'язаних з 5G, важливе значення набуває й активна співпраця між союзниками НАТО. Литва, Латвія та Естонія, разом відомі як країни Балтії, є прикладом та підтвердили відданість політиці НАТО - вжили заходів щодо безпеки 5G.

Ці три країни входять до списку країн, які відповідають вимогам Північноатлантичного альянсу щодо виділення щонайменше 2% національного ВВП на свої оборонні бюджети. У 2020 році Естонія виділила 2,33% свого ВВП, Латвія – 2,27%, а Литва – 2,13%.

У звіті за 2019 рік Міжнародна безпека та Естонія 2019 Служба зовнішньої розвідки Естонії вперше визначила Китай як загрозу національній безпеці, та підтверджується наявність «лазівки» у китайських IT-пристроях та кібероперації на користь КПК та збройних сил[29].

Всі три країни приєдналися до ініціативи «Чиста мережа» під керівництвом США, підписавши спільну декларацію про безпеку 5G (Естонія у жовтні 2019 року, Латвія у лютому 2020 року та Литва у вересні 2020 року), наголосивши на проблемі безпеки 5G та взявши на себе зобов'язання на «Ретельна оцінка постачальників і ланцюжків поставок»[30].

В Естонії знаходиться Центр передового досвіду в галузі спільного кіберзахисту НАТО (CCDCOE), який керує як мінімум двома ключовими дослідницькими проектами з безпеки 5G, включаючи безпеку мереж 5G для військової мобільності, що фінансуються Міністерством оборони США та Міністерством оборони Естонії[31]. Інший важливий проект спрямований на визначення безпечних методів використання приватних та комерційних мереж 5G силами НАТО[32].

Латвія стала однією з перших європейських країн, що запустили 5G для комерційного використання ще в липні 2019 року та відкрила перший військовий випробувальний полігон 5G у Європі на військовій базі Адажі у листопаді 2020

---

[28] Girard, Bonnie. "The Real Danger of China's National Intelligence Law". *The Diplomat.* February 23, 2019. https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/

[29] Lau, Stuart. "Lithuania pulls out of China's '17+1' bloc in Eastern Europe". Politico. May 21, 2021. https://www.politico.eu/article/lithuania-pulls-out-china-17-1-bloc-eastern-central-europe-foreign-minister-gabrielius-landsbergis/. ; "International security and Estonia". Estonian foreign intelligence service. February 28, 2019. https://www.välisluureamet.ee/pdf/raport-2019-ENG-web.pdf

[30] «Спільна декларація США та Естонії про безпеку 5G». 1 листопада 2019 р. https://ee.usembassy.gov/joint-declaration-on-5g/. ; «Спільна заява про Спільну декларацію США та Латвії про безпеку 5G». 27 люте 2020 р. https://2017-2021.state.gov/joint-statement-on-united-states-latvia-joint-declaration-on-5g-security/index.html .; «Меморандум про взаєморозуміння між США та Литовською Республікою про безпеку 5G». 17 вересня 2020 р. https://2017-2021.state.gov/united-states-republic-of-lithuania-memorandum-of-understanding-on-5g-security/index.html

[31] https://ccdcoe.org/news/2021/experts-concluded-that-nato-needs-a-multinational-effort-to-secure-supply-chain-and-networks-of-commercial-and-military-5g-networks/

[32] https://ccdcoe.org/news/2021/experts-concluded-that-nato-needs-a-multinational-effort-to-secure-supply-chain-and-networks-of-commercial-and-military-5g-networks/

року. Проект реалізується під керівництвом оператора мобільного зв'язку «Латвійський мобільний телефон» (LMT) у співпраці з Національними збройними силами з метою створення життєздатного середовища для розробки та тестування нових технологій захисту 5G. Середовище було створено для використовувати об'єднані можливості латвійських підприємств, дослідницьких центрів та експертів у галузі оборони для розробки нових датчиків, систем захисту та інших технологій на основі 5G для національних та союзних збройних сил[33].

Литва з її майбутнім розгортанням 5G може запропонувати цікаві проекти щодо можливостей кібербезпеки, які можуть задовольнити потреби співробітництва. **Литовський національний центр кібербезпеки (NCSC) відіграватиме важливу роль у процесі перевірки довіри до обладнання, де однією з функцій NCSC є надання оцінок кібербезпеці конкретних пристроїв та додатків на основі потреб приватного та державного секторів**.

Також у травні цього року у Литві розпочав роботу новий Регіональний центр кіберзахисту (RCDC) пілотну діяльність. Метою цієї двосторонньої американо-литовської ініціативи є створення платформи для обміну передовим досвідом у галузі кібербезпеки, створення постійного центру навчання кібербезпеки та проведення НДДКР. В області НДДКР RCDC може використовувати можливості місцевих компаній та дослідницьких інституцій. Ресурси, які можуть запропонувати країни Балтії, включають Ericsson в Естонії та її центр розробки в Естонії; LMT та партнери, які вже створюють середовище для тестування військових додатків 5G на військовій базі Адажі; група литовських виробників електроніки Teltonika IoT Group, яка нещодавно оголосила про плани інвестувати 2,5 мільярда євро (2,97 мільярда доларів) та побудувати литовський завод напівпровідників до 2030 року; і Балтійський інститут передових технологій, що базується в Литві, який розробляє апаратні компоненти широкосмугового радіочастотного та міліметрового діапазону для додатків 5G і збирається запустити проект разом з європейськими партнерами з розробки прототипу передавача 6G з покращеним штучним інтелектом[34].

3.1. Естонська Республіка

У січні 2019 року міністр підприємництва та інформаційних технологій підписав проект постанови, в якому закладено основу для того, щоб оператори електронного зв’язку могли розпочати розвиток мереж 5G в діапазоні 3,6 ГГц.

[33] https://www.mod.gov.lv/en/news/camp-adazi-becomes-first-innovative-5g-m military- test- site- europe https://cepa.org/how-can-the-baltic-states-support-5g-security-through-transatlantic-cooperation/#:~:text=.%20https%3A//jamestown.org/program/5g-technologies-in-latvia-advance-military-capabilities-and-national-economy/.

[34] https://cepa.org/how-can-the-baltic-states-support-5g-security-through-transatlantic-cooperation/

У березні 2019 року була опублікована дорожня карта спектру 5G з планами продати на аукціон спектр 700 МГц у першому семестрі 2020 року. Згадується потенціал спектру в діапазонах 40-44 ГГц і 66-71 ГГц.

Естонія провела консультації щодо 5G у квітні 2018 року. NRA, TJA, в травні 2018 року вказав, що буде організовано аукціон для діапазону 3,6 ГГц.

У 2020 році призначено 4 ліцензії на частотах 3,6 ГГц

Аукціон на 390 МГц спектру в діапазоні 3,6 ГГц був призупинений у квітні 2019 року через скаргу на правила тендеру. Levikom Eesti, постачальник послуг Інтернету речей та фіксованого бездротового Інтернету, заявив, що аукціон лише трьох ліцензій у діапазоні 3,6 ГГц сприятиме трійці існуючих стільникових операторів країни, а також перешкоджає конкуренції.

У жовтні 2019 року Міністерство економіки та зв’язку розпочало консультацію щодо публічного тендеру на послуги широкосмугового мобільного зв’язку на частотах 700 МГц та 26 ГГц (24,25–27,5 ГГц). Консультація тривала до середини грудня 2019 року.

У червні 2020 року на аукціоні 5G було додано четверту ліцензію.

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.

Зміни до Закону про електронні комунікації прийняті в травні 2020 року, та передбачено право уряду встановлювати для цілей національної безпеки та оборони вимагати від оператора та зобов'язати останнього надавати інформацію відносно мережевого обладнання та його програмного забезпечення. Обладнання та програмне забезпечення для потреб оборони використовуються за дозвільним

принципом [35]. Процедурні питання мають бути врегульовані підзаконними актами.

Проект постанови внесено на розгляд уряду на початку березня 2021 року, але не був прийнятий із занепокоєння щодо юридичної ясності. Новий аукціон спектру для 5G в діапазоні 3,6 ГГц (до чотирьох ліцензій) оголошено, з кінцевим терміном подачі заявок у листопаді 2021 (тендери на діапазони частот 700 МГц і 26 ГГц не оголошено).

3.2. Латвійська Республіка

Регламент Латвії про планування та реалізацію заходів безпеки для критично важливої IT-інфраструктури набув чинності у січні 2021 року. Регламент передбачає, що критична інфраструктура потребує найвищого рівня безпеки, та встановлює вимоги для постачальників обладнання та програмного забезпечення, а також бенефіціарів, які мають бути зареєстровані у державі-члені НАТО, ЄС або Європейській економічній зоні (ЄЕЗ).

У 2019 році відбувся запуск перших двох мереж 5G та планів для внутрішнього виробництва маршрутизаторів 5G. Латвія серед попередників 5G в Європі[36].

У лютому 2020 р. уряд Латвії затвердив національну дорожню карту для Розгортання загальнодоступної мережі мобільного зв'язку 5G. Документ містить огляд розподілу спектру, розгортання комерційних мереж у великих міських центрах та зобов'язання щодо покриття, заплановані для розподілу 700 МГц для залізниць та автомобільних доріг.

100 МГц спектру 3,5 ГГц для 5G продано на аукціон у листопаді 2017 року. Решта 50 МГц спектру 3,5 ГГц для 5G продано на аукціон у вересні 2018 р.

Запуск 5G Tele2 на двох сайтах у січні 2020 року

700 МГц. Латвійський регулятор видав консультацію щодо призначення спектру 700 МГц для 5G у березні 2020 року.

Три лоти 2×10 МГц +1×5 МГц спектру (703-713 МГц, 738-743 МГц і 758-768 МГц – 713-72 МГц, 743-748 МГц і 768-778 МГц – 723-733 МГц, 748-758 МГц і 778-788 МГц).

---

[35] Electronic Communications Act, § 11 subsection 41, 87 subsection 21 and 22, Riigi Teataja [State Courier], https://www.riigiteataja.ee/en/eli/517122020006/consolide.

[36] 3 Andris Tauriņš, Gunvaldis Leitens, and Lūcija Strauta, 'The Technology, Media and Telecommunications Review: Latvia', Law Reviews, 3 February 2021, https://thelawreviews.co.uk/title/the-technology-media-and-telecommunications-review/latvia.

Резервна ціна встановлюється на рівні 1 млн євро за кожен лот.

Термін дії ліцензій – 20 років з початку 2022 року.

1500 МГц. На початку 2019 року SRPK анулював права Lattetelecom на фіксоване використання частот 1427-1452 та 1492-1517 МГц з 2021 року. SRPK має намір надавати послуги мобільного зв'язку 5G на частотах 1427-1517 МГц.

У серпні 2019 року регулюючий орган Латвії опублікував консультацію щодо своїх планів виставити на аукціон смугу частот 1432-1492 МГц до січня 2021 року. Консультації завершились 4 вересня 2019 року.

3,4-3,8 ГГц. 100 МГц на частотах 3,4–3,8 ГГц частково продано з аукціону у листопаді 2017 року. LMT придбала два блоки по 50 МГц (3400-3450 МГц та 3650-3700 МГц) за початковою ціною 250 000 євро за штуку. Термін дії концесії – 10 років, з січня 2019 року до грудня 2028 року.

50 МГц, що залишилися, зі спектру 3,5 ГГц продані з аукціону у вересні 2018 року. SPRK продала з аукціону 50 МГц спектра для послуг 5G у діапазоні 3550–3600 МГц компанії Tele2 Латвія у вересні 2018 року. На аукціоні було зібрано 6,5 мільйона євро за 10-річну ліцензію, що діє з 1 січня 2019 року.

3.3. Литовська Республіка

У березні 2021 року внесено до поправки до існуючої нормативно-правової бази, які дозволяють уряду перешкоджати участі ненадійних постачальників на ринку електронних комунікацій. Одним із основних критеріїв щодо визначення надійного виробника є те, чи зареєстрований він (або його бенефіціар) у країні НАТО, Європейському союзі, ЄЕЗ та/або Організації економічного співробітництва та розвитку (ОЕСР). Цей критерій застосовується до телекомунікаційної компанії, постачальника обладнання та постачальника послуг з обслуговування обладнання, що означає, що жодні так звані сторонні компанії не можуть брати участь на ринку електронних комунікацій.

Генеральний план для 5G, затверджений 3 червня 2020 року, включаючи зобов'язання з покриття: принаймні, одне з 5 найбільших міст буде охоплено до 2022 року, усі 5 – до 2023 року та основні маршрути – до 2025 року.

700 МГц. Регулятор планує виділити одну ділянку спектра FDD 2 x 10 МГц, дві ділянки спектра FDD 2 x 5 МГц і три ділянки спектра 5 МГц для додаткової лінії зв'язку (SDL). Буде організовано SMRA (одночасний аукціон у кілька раундів), але учаснику торгів буде дозволено брати участь лише в одному блоці спектру FDD та одному блоці спектру SDL.

3,4-3,8 ГГц / 3,8-4,2 ГГц. RRT відкрила громадські консультації щодо використання частот 3,4–3,8 ГГц та 3,8–4,2 ГГц з квітня по травень 2018 р. Другі консультації з громадськістю щодо використання частот 3,4–3,8 ГГц були

проведені в період з жовтня до листопада 2018 р. Консультації завершилися в квітні 2019.

Спектр смуги 3,5 ГГц був виділений на тимчасовій і некомерційній основі компанії Telia Lietuva.

RRT у відповідь на громадську реакцію та поширення дезінформації про 5G надало роз'яснення щодо цієї технології на своєму веб-сайті.

2020 року уряд Литви затвердив план впровадження 5G. Керівні принципи вказують, що як мінімум одна мережа 5G повинна охоплювати одне з найбільших міст країни (Вільнюс, Каунас, Клайпеда, Шяуляй або Паневежис) до 2022 року і що мінімум одна мережа 5G повинна бути доступна у всіх 5 містах до 2023 року.

Встановлено зобов'язання щодо покриття всіх міських територій та основних транспортних маршрутів та вузлів (автомагістралей, залізниць, аеропортів) до 2025 року.

ВИСНОВКИ:

Для України настав найкращий час, для вжиття превентивних заходів та амбітних кроків у напрямку розгортання високошвидкісних мереж та максимального використання їх можливостей, оскільки на сьогодні увесь світ знаходиться на етапі переходу від одного технологічного покоління до іншого.

І саме тому зміцнення та технологічної незалежності буде слугувати як захисту критично важливої інфраструктури, так і ствердженню наукового та технологічного потенціалу, конкурентоспроможності технологічних рішень України.

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 ідентичність[37]. Проект програми «Цифровий компас 2030» демонструє глобальні цілі держав-членів ЄС для досягнення цифрового майбутнього.

До 2030 року, зокрема:

- ✓ всі домогосподарства повинні мати гігабітний зв'язок;
- ✓ всі населені пункти повинні мати 5G;
- ✓ 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.

Нижче наведено набір рекомендацій, які потенційно може підтримати та прискорити зусилля щодо побудови більш безпечного майбутнього 5G, активізувати процес імплементації нормативної бази для розгортання 5G мереж:

«практична реалізація прогресивного законодавства вбачається неможливою без вирішення безпекових аспектів пов'язаних з 5G мережею. На користь цього свідчать всі матеріали та приклади цього дослідження».

[37] 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

І тому, обираючи найкращий безпечний та дієвий шлях слід підвести такі підсумки:

1) розгортання високошвидкісних мереж повинно йду у спільному та тісному розвитку та розгортання системи безпекових питань. У зв'язку з цим, розробка та внесення на розгляд Верховної Ради України нової редакції проекту Закону "Про кібербезпеку", у тому числі положень NIS 2, Інструментарію ЄС, відповідності вимогам безпеки та національним інтересам постачальникам обладнання як для високошвидкісних мереж, так і на інших об'єктах критичної інформаційної інфраструктури, вимоги до зберігання відомостей про функціонування мережі та її інциденти, користувачів виключно на території України ;

2) врегулювання практичних аспектів розгортання високошвидкісних мереж, у тому числі та не обмежуючись питаннями строку дії ліцензії, вартості ліцензії, вимог до обладнання та його постачальників, строків розгортання, розгортання мережі в економічно невигідних регіонах, вздовж автомагістралей, залізничних та авіо-трасс. Окремим та базовим питанням є обрахування вартості запровадження розгортання високошвидкісних мереж в Україні є їх вартість, тобто необхідно як доопрацювання законодавства про електронні комунікації, так і розробка урядових та відомчих актів, підготовки доповідних записок до уряду із пропозиціями щодо проведення науково-дослідної роботи та проведення переговорів з донорами для отримання технічної допомоги;

3) впровадження найкращих практик державно-приватного партнерства для ефективного розгортання високошвидкісних мереж як для реалізації проектів, так і базово для підготовки проведення досліджень з обрахування вартості, строків, особливостей доопрацювання законодавства про державно-приватне партнерство та законодавства про електронні комунікації, законодавства про науково-технічну діяльність;

4) запровадження механізмів перевірки обладнання для розгортання високошвидкісних мереж - використання можливостей національного законодавства у сфері стандартизації, сертифікації та оцінки відповідності.