Пропозиції
до проекту Закону України
«Про внесення змін до Закону України «Про електронні комунікації»
(щодо вимог при наданні електронних комунікаційних послуг
органам державної влади, органам місцевого самоврядування,
державним організаціям (установам, закладам) та на об'єкти
критичної інфраструктури)»
*(реєстр. № 8238 від 28.11.2022 р.)**

Проект Закону України «Про внесення змін до Закону України «Про електронні комунікації» (щодо вимог при наданні електронних комунікаційних послуг органам державної влади, органам місцевого самоврядування, державним організаціям (установам, закладам) та на об'єкти критичної інфраструктури)», як зазначено в пояснювальній записці, спрямований на захист та створення безпечних умов у діяльності органів державної влади, органів місцевого самоврядування, державних організацій (установ, закладів), об'єктів критичної інфраструктури та захист кіберпростору.

Сутність законодавчої ініціативи, на нашу думку, доцільно розглядати як складову комплексного вирішення проблем інформаційної та кібербезпеки. Пропонується внести зміни до Закону України «Про електронні комунікації», відповідно до яких встановити додаткові особливі вимоги до постачальників електронних комунікаційних мереж та/або послуг при наданні ними послуг, а саме: обов'язковість отримання статусу LIR та заборона здійснювати передачу (трансфери) IP-адрес в Україні або за її межі у період надання електронних комунікаційних послуг (пункт 15 частини третьої статті 18). Окрім того, пропонується доповнити категоріально-понятійний апарат дефініціями для визначення понять сфери електронних комунікацій, як-то: Локальна Інтернет-Реєстратура (Local Internet Registry, LIR), Регіональна Інтернет-Реєстратура (Regional Internet Registry, RIR) присвоєння та розподіл IP-адрес у мережі Інтернет.

Під час розгляду законопроекту до уваги також бралася позиція Інтернет Асоціації України (далі – ІнАУ), яку викладено в листі до Голови Комітету Верховної Ради України з питань цифрової трансформації від 1 грудня 2022 р. Позиція ІнАУ щодо впровадження пропонованих законодавчих новацій є негативною, оскільки, на їхнє переконання, наявність статусу LIR у постачальників комунікаційних послуг у разі, якщо серед їх абонентів є орган державної влади, місцевого самоврядування, державна організація (установа, заклад) або об'єкт критичної інфраструктури, не сприятиме безпеці кіберпростору. Як вважають фахівці ІнАУ, «такий підхід несе не лише небезпеку монополізації ринку на користь крупних гравців. У низці сільських регіонів представлені лише невеликі оператори, які не є LIRами, і покриття цих місцевостей крупними операторами потребуватиме часу і додаткових коштів».

Підтримуючи в цілому законодавчі ініціативи, спрямовані на забезпечення інформаційної та кібербезпеки, враховуючи наявність зобов'язань України за

Конвенцією Ради Європи про кіберзлочинність[1], положення законів України: «Про національну безпеку України»[2], «Про захист інформації в інформаційно-телекомунікаційних системах»[3], «Про основні засади забезпечення кібербезпеки України»[4], а також необхідність оперативного законодавчого реагування в умовах встановленого правового режиму воєнного стану, вважаємо за доцільне висловити такі міркування.

Щодо встановлення вимог до постачальників електронних комунікаційних мереж та/або послуг на отримання статусу LIR при наданні ними електронних комунікаційних послуг на об'єкти критичної інфраструктури.

Регулювання правових й організаційних засад створення та функціювання національної системи захисту критичної інфраструктури здійснюється відповідно до Закону України «Про критичну інфраструктуру»[5] (далі – Закон) від 16 листопада 2021 року № 1882-IX, який є складовою законодавства у сфері національної безпеки. Відповідно до частини першої статті 8 Закону віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України. Таким нормативно-правовим актом є Порядок віднесення об'єктів до об'єктів критичної інфраструктури, затверджений постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури»[6] ще у 2020 році до прийняття Закону.

Окрім того, відповідно до статті 11 Закону для цілей узгодження дій суб'єктів національної системи захисту критичної інфраструктури формується Реєстр об'єктів критичної інфраструктури (далі – Реєстр). Своєю чергою, збирання, узагальнення, попередній аналіз даних щодо об'єктів критичної інфраструктури та пропозиції щодо включення таких об'єктів до Реєстру в межах визначених секторів здійснюються Секторальними органами. Реєстр формується та ведеться Уповноваженим органом у сфері захисту критичної інфраструктури на основі пропозицій суб'єктів національної системи захисту критичної інфраструктури. Постановою Кабінету Міністрів України від 12 липня 2022 р. № 787 «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України»[7] визначено уповноважений орган у сфері захисту критичної інфраструктури – Державна

[1] Конвенція про кіберзлочинність, ратифіковано 07.09.2005 р., набуття чинності для України 01.07.2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 14.12.2022)

[2] Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 14.12.2022)

[3] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 14.12.2022)

[4] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.12.2022)

[5] Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 14.12.2022)

[6] Деякі питання об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 14.12.2022)

[7] Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України: постанова Кабінету Міністрів України від 12.07.2022 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text (дата звернення: 14.12.2022)

служба захисту критичної інфраструктури та забезпечення національної системи стійкості України (ДЗКІ). Окрім того 18 жовтня 2022 р. прийнято Закон України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України», відповідно до приписів якого Розділ IX «Прикінцеві та перехідні положення» Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» доповнено пунктом 2^1 такого змісту: «Установити, що під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування повноваження уповноваженого органу у сфері захисту критичної інфраструктури України, передбачені Законом України «Про критичну інфраструктуру», здійснюються Державною службою спеціального зв'язку та захисту інформації України».

Варто також зазначити, що об'єкти критичної інфраструктури не є однотипними. Адже, відповідно до рівня їх важливості для забезпечення окремих життєво важливих функцій держави в межах секторів критичної інфраструктури здійснюється їх категоризація. Згідно з частиною другою статті 10 Закону існують такі категорії критичності об'єктів: I категорія критичності – особливо важливі об'єкти, які мають загальнодержавне значення і значний вплив на інші об'єкти критичної інфраструктури, порушення функціонування яких призведе до виникнення кризової ситуації державного значення; II категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення; III категорія критичності – важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення; IV категорія критичності – необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

З огляду на викладене, нормативно-правове регулювання питань критичної інфраструктуру та її захисту перебуває на стадії формування, що може ускладнити процес визначення об'єктів критичної інфраструктури щодо яких встановлені вимоги до постачальників електронних комунікаційних мереж та/або послуг на отримання статусу LIR при наданні ними електронних комунікаційних послуг.

Щодо доцільності та обґрунтованості врегулювання означених у зверненні питань шляхом встановлення законодавчих норм.

Певною мірою варто погодитися з висновком ІнАУ про те, що «наявність статусу LIR у постачальників комунікаційних послуг у разі, якщо серед їх абонентів є орган державної влади, місцевого самоврядування, державна організація (установа, заклад) або об'єкт критичної інфраструктури, не сприятиме безпеці кіберпростору». Така позиція обґрунтовується, зокрема, аналізом положень Закону України «Про основні засади забезпечення кібербезпеки України». Так, відповідно до пункту 8 частини четвертої статті 5 зазначеного Закону суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та / або надають послуги,

пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом, віднесені до переліку суб’єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Водночас, органи державної влади, місцевого самоврядування, державна організація (установа, заклад), підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури, також є суб’єктами, що безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Зокрема, відповідно до частини четвертої статті 6 Закону відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об’єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об’єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури.

Отже, відповідальність за забезпечення захисту електронних інформаційних ресурсів є солідарною й покладається на постачальників електронних комунікаційних мереж та/або послуг при наданні ними електронних комунікаційних послуг, органи державної влади, місцевого самоврядування, державні організації (установи, заклади), власників та/або керівників підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури. Окрім того, здійснення господарської діяльності у сфері електронних комунікацій є гнучким, зарезервованим, конкурентоспроможним, ґрунтується на засадах мінімально необхідного правового регулювання, згідно з яким рішення, дії суб’єктів владних повноважень мають бути необхідними та мінімально достатніми для досягнення мети і вирішення завдань, а запровадження регуляторних зобов’язань до постачальників електронних комунікаційних мереж та/або послуг із значним ринковим впливом застосовується «…лише тією мірою, що необхідна для забезпечення ефективної та стійкої конкуренції в інтересах кінцевих користувачів та послаблення або скасування таких зобов’язань як тільки ця умова буде забезпечена» (пункти 1, 3 частини другої статті 3 Закону України «Про електронні комунікації»).

Дослідницька служба
Верховної Ради України

**Цей документ підготовлений Дослідницькою службою Верховної Ради України як довідковий інформаційно-аналітичний матеріал. Інформація та позиції, викладені в документі, не є офіційною позицією Верховної Ради України, її органів або посадових осіб. Цей документ може бути цитований, відтворений та перекладений для некомерційних цілей за умови відповідного посилання на джерело.*