Додаток
до вих. № 18/02-196
від 01.02.2019

ІНФОРМАЦІЯ
про здійснення Адміністрацією Держспецзв'язку державної регуляторної політики у 2018 році

I. Вступна частина

Державна регуляторна політика протягом 2018 року здійснювалася Адміністрацією Держспецзв'язку з метою виконання основних завдань стосовно забезпечення:

1) формування та реалізації державної політики у сферах:

функціонування, безпеки та розвитку державної системи урядового зв'язку та Національної системи конфіденційного зв'язку (далі - НСКЗ);

телекомунікацій і користування радіочастотним ресурсом України;

криптографічного та технічного захисту інформації;

захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури;

2) здійснення державного контролю у цих сферах.

Зазначені завдання виконувалися шляхом розроблення Адміністрацією Держспецзв'язку проектів регуляторних актів, відстеження результативності та перегляду регуляторних актів, розробником яких є Адміністрація Держспецзв'язку.

II. Загальна частина

1. Загальна характеристика здійснення Адміністрацією Держспецзв'язку державної регуляторної політики у 2018 році

З метою виконання Адміністрацією Держспецзв'язку вимог законодавства про державну регуляторну політику та планування відповідної діяльності на 2018 рік т.в.о. Голови Держспецзв'язку 15.12.2017 затверджено План діяльності Адміністрації Держспецзв'язку з підготовки проектів регуляторних актів на 2018 рік (№ 18/02-3397 від 15.12.2017), відповідно до якого заплановано вживати заходів щодо розроблення 24 проектів регуляторних актів (Законів України – 2, постанов Кабінету Міністрів України – 9, наказів Адміністрації Держспецзв'язку – 13).

Протягом звітного періоду видано 3 регуляторних акти Адміністрації Держспецзв'язку. Інші завдання, передбачені Планом, знято з розроблення або їх строк виконання перенесено на 2019 рік.

Усі проекти регуляторних актів Адміністрацією Держспецзв'язку розроблено із дотриманням єдиного підходу до їх підготовки. Зазначені акти в установленому порядку проходять процедуру оприлюднення з метою одержання зауважень і пропозицій від фізичних та юридичних осіб.

Повідомлення про оприлюднення проектів регуляторних актів та аналізи регуляторного впливу цих документів розміщуються на офіційному веб-сайті Держспецзв'язку.

Опрацювання одержаних від фізичних і юридичних осіб, їх об'єднань зауважень і пропозицій у процесі підготовки проектів регуляторних актів здійснюється відповідно до вимог законодавства.

Деякі проекти регуляторних актів розглядалися на засіданнях Громадської ради при Адміністрації Держспецзв'язку та доопрацьовувалися з урахуванням наданих пропозицій, а також з урахуванням пропозицій та зауважень Інтернет Асоціації України та Українського союзу промисловців та підприємців.

Відстеження результативності дії регуляторних актів здійснювалося відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності», Методики відстеження результативності регуляторного акта, затвердженої постановою Кабінету Міністрів України від 11.03.2004 № 308, а з 01.10.2018 також і на підставі та у строки, визначені План-графіком відстеження Адміністрацією Держспецзв'язку результативності регуляторних актів на 2018 рік, затвердженим Головою Держспецзв'язку та зареєстрованим 28.09.2018 за № 18/02-3041.

Про результати відстеження результативності в установленому порядку інформувалася Державна регуляторна служба України. Звіти про відстеження результативності регуляторних актів розміщувалися на офіційному веб-сайті Держспецзв'язку.

Відповідно до рекомендацій, наданих ДРС, протягом 2018 року удосконалювалась організація здійснення Адміністрацією Держспецзв'язку державної регуляторної політики.

В Адміністрації Держспецзв'язку визначено та з жовтня 2018 року розміщено на офіційному веб-сайті Держспецзв'язку Список посадових осіб Адміністрації Держспецзв'язку, відповідальних за стан реалізації державної регуляторної політики, проводиться систематизація регуляторних актів (відповідний перелік розміщено на офіційному веб-сайті Держспецзв'язку).

14.12.2018 затверджено План діяльності Адміністрації Держспецзв'язку з підготовки проектів регуляторних актів на 2019 рік (№ 18/02-3397), яким заплановано внесення змін до чинних регуляторних актів та розроблення нових, спрямованих на вдосконалення законодавства України.

На початку 2019 року структуру розділу «Регуляторна діяльність» офіційного веб-сайту Держспецзв'язку удосконалено відповідно до рекомендацій ДРС.

2. Ситуація, яка потребувала упорядкування державного регулювання господарських відносин у сферах формування та реалізації (участі у реалізації) Адміністрації Держспецзв’язку державної політики у 2018 році

2.1. Ситуація у сфері технічного та криптографічного захисту інформації потребувала удосконалення нормативно-правової бази стосовно державного регулювання господарських відносин у частині:

удосконалення механізмів проведення державної експертизи у сфері технічного та криптографічного захисту інформації;

удосконалення вимог до організації та забезпечення безпеки криптографічного захисту службової інформації;

уточнення положень Вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв’язку від 18.12.2012 № 739, зареєстрованих в Мін’юсті 14.01.2013 за № 108/22640, з метою їх однозначного тлумачення;

розробки Технічного регламенту на засоби криптографічного захисту інформації;

встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їх відокремлених пунктів реєстрації.

Також на сьогодні виникла потреба приведення нормативно-правових актів, які регламентують господарську діяльності у галузі криптографічного та технічного захисту інформації, у відповідність зі законодавства, а саме:

наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованого в Мін’юсті 16.05.2007 за № 820/14087 «Про затвердження Положення про державну експертизу в сфері технічного захисту інформації»;

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв’язку від 20.07.2007 № 141, зареєстрованого в Мін’юсті 30.07.2007 за № 862/14129;

наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.06.2008 № 100, зареєстрованого в Мін’юсті 16.07.2008 за № 651/15342 «Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації».

Слід зазначити, що 07.11.2018 набрав чинності Закон України «Про електронні довірчі послуги», який регулює відносини, що виникають між юридичними, фізичними особами, суб'єктами владних повноважень у процесі надання, отримання електронних довірчих послуг, процедури надання цих послуг, нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також основні організаційно-правові засади електронної ідентифікації.

Одночасно з набранням чинності Законом України «Про електронні довірчі послуги» втратив чинність Закон України «Про електронний цифровий підпис» та змінилася сфера державного регулювання електронного цифрового підпису на сферу електронних довірчих послуг.

У зв’язку з цим проводиться робота щодо визнання такими, що втратили чинність, низки нормативно-правових (у тому числі регуляторних) актів у сфері регулювання електронного цифрового підпису, розроблених Адміністрацією Держспецзв'язку.

Протягом звітного періоду внесено зміни до Положення про державну експертизу в сфері криптографічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.06.2008 № 100, зареєстрованого в Мін’юсті 16.07.2008 за № 651/15342 (наказ Адміністрації Держспецзв’язку від 06.02.2018 № 61, зареєстрований в Мін’юсті 22.02.2018 за № 220/31672), та до Вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв’язку від 18.12.2012 № 739, зареєстрованих в Мін’юсті 14.01.2013 за № 108/22640 (наказ Адміністрації Держспецзв’язку від 21.12.2017 № 712, зареєстрований в Мін’юсті 17.01.2018 за № 72/31524).

Регуляторні нормативно-правові акти у сфері технічного та криптографічного захисту інформації, якими буде удосконалено вимоги до організації та забезпечення безпеки криптографічного захисту службової інформації, затверджено технічний регламент на засоби криптографічного захисту інформації та встановлено вимоги з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їх відокремлених пунктів реєстрації, заплановано до розробки та затвердження на 2019 рік.

На 2019 рік заплановано приведення у відповідність із вимогами законодавства положення таких нормативно-правових актів:

наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованого в Мін’юсті 16.05.2007 за № 820/14087 «Про затвердження Положення про державну експертизу в сфері технічного захисту інформації»;

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв’язку від 20.07.2007 № 141, зареєстрованого в Мін’юсті 30.07.2007 за № 862/14129.

наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.06.2008 № 100, зареєстрованого в Мін’юсті 16.07.2008 за № 651/15342 «Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації».

2.2. Ситуація у сфері кіберзахисту

2.2.1. У зв’язку зі змінами законодавства у сфері захисту інформації та розвитком законодавчої бази у сфері кіберзахисту існує необхідність врегулювати процедури підключення інформаційно-телекомунікаційних систем, де обробляються державні інформаційні ресурси, необхідно забезпечити захист державних інформаційних ресурсів при підключенні інформаційно-телекомунікаційних систем органів виконавчої влади, інших державних органів, підприємств, установ та організацій до мережі Інтернет

відповідно до вимог сучасності та з урахуванням підвищення рівня загроз у кіберпросторі.

Кіберзахист державних електронних інформаційних ресурсів та захист інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, мають полягати у забезпеченні безпеки інформаційно-телекомунікаційних систем органів виконавчої влади, інших державних органів, підприємств, установ та організацій, які одержують, обробляють, поширюють і зберігають державні інформаційні ресурси під час підключення їх до мережі Інтернет.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки» комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, а також комунікаційні системи, які використовуються для реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронного документообігу є об’єктами кіберзахисту та, як наслідок, до них мають бути застосовані організаційні, правові, інженерно-технічні заходи, а також заходи захисту інформації, спрямовані на запобігання кіберінцидентам, виявлення та захист від кібератак. При цьому Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» визначено, що «державні інформаційні ресурси повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю».

Таким чином, для забезпечення захисту державних інформаційних ресурсів, які оброблюються в інформаційно-телекомунікаційних системах органів виконавчої влади, інших державних органів, підприємств, установ та організацій та які підключені до мережі Інтернет, у таких інформаційно-телекомунікаційних системах необхідно застосовувати комплексні системи захисту інформації з підтвердженою відповідністю.

Ці вимоги мають знайти своє відображення у нормативно-правових документах, якими регламентується порядок підключення до глобальних мереж передачі даних інформаційно-телекомунікаційних систем органів виконавчої влади, інших державних органів, підприємств, установ та організацій, які одержують, обробляють, поширюють і зберігають державні інформаційні ресурси.

Проблема не може бути розв’язана за допомогою ринкових механізмів, оскільки на сьогодні питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікацій, у яких немає документів про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації, не внормовано.

Проблема не могла бути розв’язана за допомогою чинних регуляторних актів, оскільки постанова Кабінету Міністрів України від 12.04.2002 № 522 «Про затвердження Порядку підключення до глобальних мереж передачі

даних» не врегульовує питання необхідності підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації операторами (провайдерами) телекомунікацій при наданні послуг з доступу до мережі Інтернет.

З огляду на зазначене Адміністрація Держспецзв'язку розробила проект постанови Кабінету Міністрів України «Про внесення змін до постанови Кабінету Міністрів України від 12.04.2002 № 522» (в редакції станом на сьогодні – «Про затвердження Порядку доступу до мережі Інтернет»), який доопрацьовується з урахуванням наданих державними органами зауваженнями та пропозиціями, а також з урахуванням пропозицій та зауважень Інтернет Асоціації України, Українського союзу підприємців та промисловців, Української асоціації операторів зв'язку «Телас» та Телекомунікаційної палати України.

2.2.2. Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, у тому числі шляхом порушення штатних режимів роботи систем управління технологічними процесами на об'єктах критичної інфраструктури.

Аналіз кіберзагроз свідчить, що кібератаки на комунікаційні системи та системи управління технологічними процесами об'єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість та інші може призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави.

Розбудова цілісної системи кібербезпеки вимагає чіткого окреслення об'єктів кібербезпеки, передусім шляхом визначення переліку тих об'єктів критичної інформаційної інфраструктури, щодо яких пріоритетно мають проводитися заходи з кіберзахисту, а також заходи з аудиту інформаційної безпеки.

На сьогодні перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави формується відповідно до постанови Кабінету Міністрів України від 23.08.2016 № 563 «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

Водночас набуття чинності Законом України «Про основні засади забезпечення кібербезпеки України» потребує внесення до переліку об'єктів критичної інформаційної інфраструктури держави систем управління технологічними процесами, що не мають виходу каналами електрозв'язку за межі контрольованої зони, але кібератака на які може призвести до негативних наслідків, зазначених у Порядку формування переліку об'єктів критичної інформаційної інфраструктури.

Крім того, забезпечення кіберзахисту об'єктів критичної інфраструктури в сучасних умовах інформаційних війн потребує особливої уваги до усіх

критично важливих об’єктів інфраструктури незалежно від форми власності з огляду на те значення, яке вони мають для економіки та промисловості, суспільства та безпеки населення. Виведення їх з ладу або порушення їх функціонування може негативно впливати на стан національної безпеки і оборони України, навколишнього природного середовища, а погіршення їх функціонування може заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей.

Тобто питання формування Переліку та підтримки його в актуальному стані є одним з першочергових кроків на шляху створення загальнодержавної системи захисту об’єктів критичної інфраструктури.

При цьому забезпечення належного функціонування Переліку потребує створення автоматизованої системи накопичення, обліку, обробки і зберігання відомостей про ті об’єкти критичної інформаційної інфраструктури, які внесені до Переліку - державного реєстру об’єктів критичної інформаційної інфраструктури.

Проблема не може бути розв’язана за допомогою ринкових механізмів, оскільки немає механізму залучення до формування Переліку не тільки суб’єктів критичної інформаційної інфраструктури будь-якої форми власності, але й уповноважених органів, які через ведення галузевих (секторальних) переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об’єктах критичної інфраструктури, щодо яких вони здійснюють владні повноваження.

Проблема не може бути розв’язана за допомогою чинних регуляторних актів, оскільки на сьогодні таких нормативно-правових актів немає.

У зв’язку з цим Адміністрація Держспецзв’язку розробила проект постанови Кабінету Міністрів України «Про затвердження порядків формування переліку об’єктів критичної інформаційної інфраструктури, порядку внесення об’єктів критичної інформаційної інфраструктури до державного реєстру об’єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування».

Надані за результатами громадського обговорення зауваження та пропозиції заінтересованих органів було в цілому враховано при доопрацюванні проекту Постанови, який подано до Кабінету Міністрів України (19.11.2018) з метою його подальшого опрацювання та винесення на розгляд профільного Урядового комітету та Уряду.

2.2.3. Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено загрози кібербезпеці об'єктів критичної інфраструктури, шляхи протидії їм та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв’язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Водночас Закон України «Про основні засади забезпечення кібербезпеки України» визначає, що до об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров’я; є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об’єктами потенційно небезпечних технологій і виробництв.

Тобто питання формування Переліку об’єктів критичної інфраструктури (далі - Перелік) та підтримки його в актуальному стані є одним з першочергових кроків на шляху створення загальнодержавної системи захисту об’єктів критичної інфраструктури. Важливим кроком при формуванні Переліку є визначення критеріїв та порядку віднесення об’єктів до об’єктів критичної інфраструктури.

На сьогодні результатом кібератак є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування об’єктів критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони. У зв’язку з цим існуючі кіберзагрози потребують впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. Тому важливим також є розроблення загальних вимог з кіберзахисту об’єктів критичної інфраструктури.

Проблема не може бути розв’язана за допомогою ринкових механізмів, оскільки на сьогодні немає критеріїв та порядку віднесення об’єктів до об’єктів критичної інфраструктури, а також немає загальних вимог з кіберзахисту таких об’єктів.

Проблема не може бути розв’язана за допомогою чинних регуляторних актів, оскільки на сьогодні таких нормативно-правових актів немає.

Тому Адміністрацією Держспецзв’язку розроблено проект постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури, критеріїв та порядку віднесення об’єктів до об’єктів критичної інфраструктури».

Надані зауваження та пропозиції заінтересованих органів було в цілому враховано при доопрацюванні проекту Постанови.

У зв’язку з наданими зауваженнями прийнято рішення щодо поділу проекту Постанови на два окремих проекти, а саме проекту постанови Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» та «Про затвердження критеріїв та порядку віднесення об’єктів до об’єктів критичної інфраструктури», які подано до Кабінету Міністрів України з метою їх подальшого розгляду та винесення на розгляд профільного Урядового комітету та Уряду.

2.2.4. Координація зусиль усіх суб’єктів забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури у ході виконання превентивних заходів, виявлення спроб та/або фактів вчинення кібератак та кіберінцидентів, стримування кібератак, припинення та усунення наслідків кібератак та кіберінцидентів, відновлення сталого функціонування об’єктів критичної інформаційної інфраструктури є запорукою забезпечення на належному рівні кіберзахисту об’єктів критичної інфраструктури України. Проблемним питання залишається відсутність нормативно-правової бази, яка б врегулювала основні аспекти спільної діяльності суб’єктів забезпечення кібербезпеки, суб’єктів кіберзахисту та власників (розпорядників) об’єктів критичної інформаційної інфраструктури, алгоритмів інформаційного обміну між ними, послідовності дій і розподілу їх функцій задля ефективної взаємодії під час запобігання, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків.

На сьогодні обмін інформацією під час вжиття заходів реагування на кіберінциденти та кібератаки здійснюється відповідно до Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого у Міністерстві юстиції України 07.07.2008 за № 603/15294.

Слід зазначити, що дія зазначеного наказу не поширюється на кіберінциденти, які не пов’язані з несанкціонованими діями щодо державних інформаційних ресурсів. При цьому сучасне визначення кіберінциденту, яке надано у Стратегії кібербезпеки України, затвердженій Указом Президента України від 15.03.2016 № 96, містить у собі не тільки спроби вчинення та/або вчинення несанкціонованих дій, але й має на увазі події ненавмисного (природного, технічного, технологічного, помилкового, зокрема людського фактора) характеру.

В умовах зростання за останні роки кількості кібератак і кіберінцидентів на об’єктах критичної інформаційної інфраструктури як державні, так і недержавні суб’єкти забезпечення кібербезпеки набули певного досвіду і розбудували організаційні і технічні системи кіберзахисту інфраструктурних об’єктів. Водночас ефективна протидія кібератакам і кіберінцидентам потребує координації та об’єднання зусиль усіх учасників діяльності у сфері кібербезпеки, спільних дій та взаємного інформування задля успішного протистояння кіберзагрозам та захисту інфраструктурних об’єктів.

Налагодження співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розроблення та запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі Стратегією

кібербезпеки України визнано як один з напрямів забезпечення кіберзахисту критичної інфраструктури. При цьому серед шляхів протидії загрозам кібербезпеці для об'єктів критичної інфраструктури - розроблення та впровадження протоколів спільних дій суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів.

Проблема не може бути розв’язана за допомогою ринкових механізмів, оскільки ця проблема стосується питань взаємодії в інтересах національної безпеки.

Проблема не може бути розв’язана за допомогою чинних регуляторних актів, оскільки на сьогодні питання взаємодії основних суб’єктів забезпечення кібербезпеки, суб’єктів кіберзахисту та власників (розпорядників) об’єктів критичної інформаційної інфраструктури під час запобігання, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків жодним нормативно-правовим актом не врегульовано.

У зв’язку з цим Адміністрація Держспецзв’язку розробляє проект постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій суб’єктів забезпечення кібербезпеки, власників (розпорядників) об’єктів критичної інформаційної інфраструктури під час запобігання, виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків».

Завершення розроблення зазначеного регуляторного акта заплановано на 2019 рік.

2.3. Ситуація у сфері розвитку державної системи урядового зв’язку та Національної системи конфіденційного зв’язку

2.3.1. У звітний період з метою виконання завдання 3 пункту 1а) Плану організації виконання Указу Президента України від 26 травня 2017 року № 146 «Про заходи, пов’язані із запровадженням Європейським Союзом безвізового режиму для громадян України» необхідним було вжиття Адміністрацією Держспецзв’язку заходів щодо нормативно-правового врегулювання питання зменшення вартості послуг конфіденційного зв’язку для надання адміністративних послуг, пов’язаних з оформленням документів, що дають право громадянину України на виїзд за кордон та містять безконтактний електронний носій.

З цією метою було розроблено та затверджено наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 09.03.2018 № 143 «Про внесення змін до Граничних тарифів на послуги конфіденційного зв’язку», який зареєстровано в Міністерстві юстиції України 26.03.2018 за № 360/31812 (далі - Наказ № 143).

2.3.2. Крім того, з метою приведення наказу Адміністрації Держспецзв’язку від 23.05.2016 № 346 «Про затвердження Порядку прийняття рішень щодо визначення операторів інформаційно-телекомунікаційних систем (мереж) Національної системи конфіденційного зв’язку», зареєстрованого в

Мін'юсті 05.08.2016 за № 1097/29227, у відповідність із вимогами статті 21 Закону України «Про ліцензування видів господарської діяльності» було розроблено та затверджено наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 19.12.2018 № 766 «Про внесення змін до наказу Адміністрації Держспецзв'язку від 23.05.2016 № 346» (подано на державну реєстрацію) (далі – Наказ № 766).

Прийняття Наказів № 143 та № 766 унормовує підстави для встановлення суб'єктами ринку телекомунікацій економічно обґрунтованої вартості послуг конфіденційного зв'язку згідно зі встановленою процедурою.

2.4. Ситуація у сфері телекомунікацій і користування радіочастотним ресурсом України

2.4.1. Відповідно до пункту 4 частини першої статті 15 Закону України «Про телекомунікації», Закону України «Про захист прав споживачів», Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411 (далі – Положення № 411), потребувало нормативно-правового врегулювання питання визначення вимог до рівня якості послуг фіксованого телефонного зв'язку.

З цією метою впродовж 2018 року проводилася розробка проекту наказу Адміністрації Держспецзв'язку «Про затвердження Вимог щодо рівня якості послуг фіксованого телефонного зв'язку», який подавався до Міністерства юстиції України для проведення державної реєстрації, однак його повернуто на доопрацювання.

Завершити виконання зазначеного завдання планується у 2019 році.

2.4.2. Відповідно до пункту 4 частини першої статті 15 Закону України «Про телекомунікації», Закону України «Про захист прав споживачів», Положення № 411, та на виконання пункту 1 Плану заходів щодо підвищення якості послуг рухомого (мобільного) зв'язку (далі – План), затвердженого розпорядженням Кабінету Міністрів України від 18 липня 2018 року № 540, у 2018 році проводилася розробка проекту наказу Адміністрації Держспецзв'язку «Про затвердження Вимог щодо рівня якості послуг рухомого (мобільного) зв'язку», який доопрацьовується в 2019 році з метою врахування пропозицій, наданих НКРЗІ.

2.4.3. Відповідно до пункту 4 частини першої статті 15 Закону України «Про телекомунікації», Закону України «Про захист прав споживачів», Положення № 411, приведення у відповідність із вимогами законодавства потребували Показники якості послуг із передачі даних, доступу до Інтернету та їх рівнів, затверджені наказом Адміністрації Держспецзв'язку від 28.12.2012 № 803, зареєстровані в Міністерстві юстиції України 21.01.2013 за № 135/22667.

У зв’язку з цим Адміністрація Держспецзв’язку розробила та у грудні 2018 року надіслала на зовнішнє погодження проект наказу Адміністрації Держспецзв’язку «Про затвердження Вимог щодо рівня якості послуг із передачі даних і доступу до Інтернету».

Прийняття зазначеного регуляторного акта заплановано у 2019 році.

2.4.4. З метою виконання пункту 3.5 витягу із протоколу від 26.04.2017 № 4 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України для вдосконалення механізму надання телекомунікаційних послуг, зокрема ідентифікації абонентів рухомого (мобільного) зв’язку, запровадження реєстрації кінцевого обладнання за міжнародним ідентифікатором у 2018 році було заплановано розроблення проекту Закону України «Про внесення змін до Законів України «Про телекомунікації» і «Про радіочастотний ресурс України».

За результатами опрацювання позицій заінтересованих органів, громадських організацій і об’єднань щодо проекту Закону у 2019 році вивчається питання щодо доцільності вжиття подальших заходів стосовно завершення розроблення зазначеного проекту регуляторного акта.

2.4.5. З метою виконання підпункту 3.1 протокольного рішення № 9 Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 08.06.2018 протягом 2018 року проводилася розробка проектів наказів Адміністрації Держспецзв’язку «Про затвердження Технічних вимог до складових системи оперативно-технічного управління телекомунікаційними мережами України» та «Про затвердження умов Типового договору та Типового договору взаємодії операторів телекомунікацій з Національним центром оперативно-технічного управління мережами телекомунікацій України».

Завершення виконання зазначених завдань заплановано у 2019 році.

2.4.6. Відповідно до частини шостої статті 29 Закону України «Про телекомунікації», пунктів 44–46 Порядку оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, затвердженого постановою Кабінету Міністрів України від 29.06.2004 № 812, проводилася розробка проекту наказу Адміністрації Держспецзв’язку «Про затвердження «Основних вимог до форм та строків подання інформації до Національного центру оперативно-технічного управління мережами телекомунікацій України».

Завершення розроблення проекту зазначеного регуляторного акта заплановано у 2019 році.

2.5. Ситуація у сфері державного контролю у сфері захисту інформації

З метою виконання абзацу четвертого пункту 1 Плану організації підготовки проектів актів, необхідних для забезпечення реалізації Закону

України «Про основні засади забезпечення кібербезпеки України», схваленого на засіданні Кабінету Міністрів України 22.11.2017 (протокол № 66), Адміністрація Держспецзв'язку розробила проект постанови Кабінету Міністрів України «Про затвердження Вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури», який заплановано подати на розгляд Кабінету Міністрів України в 2019 році.

III. Висновок

За результатами здійснення Адміністрацією Держспецзв'язку державної регуляторної політики у 2018 році спостерігається тенденція щодо зменшення рівня державного регулювання у сфері технічного та криптографічного захисту інформації, у тому числі дозвільної діяльності.

Водночас у зв'язку з набранням чинності Законом України «Про основні засади забезпечення кібербезпеки України» виникла необхідність у додатковому нормативно-правовому врегулюванні відносин у сфері захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, що також тягне за собою відповідно і додаткове врегулювання державного контролю у цій сфері.

Виходячи із запланованих та виконуваних у 2018 році заходів, спостерігаються також тенденції щодо планування збільшення кількості регуляторних актів у сфері телекомунікацій і користування радіочастотним ресурсом України, а також вдосконалення існуючих регуляторних актів у цій сфері.

Впродовж 2018 року продовжувалися вживатися заходи стосовно вдосконалення рівня організації здійснення Адміністрацією Держспецзв'язку державної регуляторної політики, зокрема у частині забезпечення прозорості всіх етапів її регуляторної діяльності.

Голова Державної служби спеціального
зв'язку та захисту інформації України Л.О. Євдоченко