ПРОЄКТ

Вноситься вноситься народними депутатами України
Олександр ФЕДІЄНКО (№89) та інші

ЗАКОН УКРАЇНИ

Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури

Верховна Рада України **п о с т а н о в л я є**:

І. Внести зміни до таких законів України:

1. У пункті 4 частини першої статті 8 Закону України «Про державну таємницю» (Відомості Верховної Ради України, 1999 р., № 49, ст. 428 із наступними змінами):

абзац п’ятий викласти в такій редакції:

«про систему спеціального зв’язку та національну систему урядових електронних комунікацій»;

доповнити абзацами тринадцятим, чотирнадцятим та п’ятнадцятим такого змісту:

«про організацію, стан, плани розвитку, заходи і порядок здійснення кіберрозвідки, кібероборони, забезпечення кібербезпеки, протидії кібертероризму та кібершпигунству в суб’єктах сектору безпеки та оборони;

про організацію, зміст, стан і плани забезпечення захисту об’єктів критичної інфраструктури;

про створення матеріально-технічного резерву для реагування на кризові ситуації та ліквідації їх наслідків на об’єктах критичної інфраструктури».

2. У Законі України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України, 2005 р., № 26, ст. 347 із наступними змінами):

1) назву доповнити словами «та на об’єктах інформаційної діяльності»;

2) преамбулу доповнити словами «та на об’єктах інформаційної діяльності»;

3) у частині першій статті 1:

абзаци третій і сьомий викласти в такій редакції:

«виток інформації – результат дій, внаслідок яких інформація, що обробляється в системі чи пристроєм обробки інформації або озвучується на об’єкті інформаційної діяльності, стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї»;

«захист інформації в системі або на об’єкті інформаційної діяльності – діяльність, спрямована на запобігання витоку інформації, що обробляється в системі чи пристроєм обробки інформації або озвучується на об’єкті інформаційної діяльності»;

абзац п’ятнадцятий доповнити словами «або автономно (без підключення до інших засобів обробки інформації, ліній зв’язку або мереж передачі даних) пристроями обробки інформації»;

доповнити з урахуванням алфавітного порядку термінами такого змісту:

«авторизація системи з безпеки – рішення щодо можливості функціонування (експлуатації) системи безпеки відповідної інформаційної, електронно комунікаційної та інформаційно-комунікаційної систем, з урахуванням відповідності її вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту, криптографічного захисту та кіберзахисту»;

«авторизована система з безпеки – інформаційна, інформаційно-комунікаційна, електронна комунікаційна, технологічна система або їх окремі компоненти, об’єкт критичної інформаційної інфраструктури, в яких запроваджені заходи та/або системи з безпеки інформації, що пройшли авторизацію з безпеки»;

«власник об’єкта інформаційної діяльності – юридична особа, якій належить право власності на об’єкт інформаційної діяльності»;

«комплекс технічного захисту інформації – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів технічного захисту інформації, призначених для захисту інформації від витоку технічними каналами в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності»;

«об’єкт інформаційної діяльності – інженерно-технічна споруда (будівля, приміщення тощо), відокремлена територія (зона), транспортний засіб, намет, в яких провадиться діяльність, пов’язана з обробкою державних інформаційних ресурсів та інформації з обмеженим доступом в органах

державної влади, державних органах, державних підприємствах, установах, організаціях, органах місцевого самоврядування»;

«озвучування інформації на об’єкті інформаційної діяльності – процес формування голосовим апаратом людини або відтворення (підсилення) акустичними технічними засобами і поширення на об’єкті інформаційної діяльності акустичного сигналу (акустичного поля), що несе інформацію»;

«пристрої обробки інформації – технічні пристрої (засоби) обробки інформації, в яких технічно неможлива реалізація програмних процедур розмежування доступу користувачів та інших функціональних послуг безпеки»;

«перелік авторизованих систем з безпеки – єдина електронна база даних, що містить відомості про авторизовані системи безпеки інформаційних, електронно комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об’єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, порядок ведення якої, включення авторизованих систем до якої та порядок доступу і надання інформації з якої визначаються спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації. Інформація про авторизовані системи, що міститься в переліку, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом та обмежень, встановлених законодавством на період дії правового режиму воєнного стану»;

«технічний канал витоку інформації – взаємопов’язана сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки, спрямовані на забезпечення витоку інформації»;

4) статтю 2 викласти в такій редакції:

«Стаття 2. Об'єкти захисту в системі та на об’єкті інформаційної діяльності

Об'єктами захисту в системі та на об’єкті інформаційної діяльності є інформація, що обробляється або озвучується, програмне забезпечення, призначене для обробки такої інформації»;

5) у статті 3:

у частині першій:

абзац перший після слів «в системах» доповнити словами «та на об’єктах інформаційної діяльності»;

після абзацу третього доповнити новим абзацом такого змісту:

«власники об’єкта інформаційної діяльності».

У зв'язку з цим абзаци четвертий - шостий вважати відповідно абзацами п'ятим - сьомим;

частину третю після слів «власник системи» доповнити словами «(або власник об’єкта інформаційної діяльності)», після слів «розпоряджатися системою» - словами «(або об’єктом інформаційної діяльності)», а після слів «розпоряднику системи» - словами «(або розпоряднику об’єкта інформаційної діяльності), слово «фізичній» виключити»;

6) у статті 8:

частини другу – четверту викласти в наступній редакції:

«Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом в системах, об’єктах критичної інформаційної інфраструктури, власниками/розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації, або шляхом авторизації системи з безпеки, або шляхом отримання сертифікату відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності.

Для створення комплексної системи захисту інформації використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, та засоби технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або сертифікат відповідності, виданий органом з оцінки відповідності, який акредитовано:

національним органом України з акредитації;

чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

Процедури авторизації систем безпеки інформації та отримання сертифікату відповідності стандарту інформаційної безпеки не застосовуються до публічних електронних реєстрів, а також для обробки інформації категорії державна таємниця.

Підтвердження відповідності комплексної системи захисту інформації забезпечується власником/розпорядником системи з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому Кабінетом Міністрів України.

Авторизація системи безпеки інформації здійснюється в порядку, встановленому Кабінетом Міністрів України.

Підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України здійснюється органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іноземної держави, якщо і національний орган України з акредитації, і національний орган з акредитації іноземної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

Авторизація систем безпеки або отримання сертифікату підтвердження відповідності стандарту інформаційної безпеки щодо систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктах критичної інформаційної інфраструктури, власниками/розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, здійснюється за одночасного дотримання таких додаткових умов:

- використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації або документ про відповідність, виданий за результатами сертифікації таких засобів відповідно до Закону України "Про технічні регламенти та оцінку відповідності";

- жодний з елементів системи не розташований, а власник такої системи або його офіційний представник не є юридичною особою (її представником), зареєстрованою на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на території держави, визнаної Верховною Радою України державою-агресором, на території держави, щодо якої застосовані санкції відповідно до Закону України "Про санкції", або на території держави, яка входить до митного союзу з такими державами;

- власник системи або його представник, який надає послуги з використанням системи, елементи якої розміщуються поза межами України, є юридичною особою, зареєстрованою в Україні, або має свого офіційного представника в Україні;

- виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.

Інформація, що становить державну таємницю, повинна оброблятися в системі, до складу комплексної системи захисту інформації якої входить комплекс технічного захисту інформації від витоку технічними каналами з підтвердженою відповідністю. Підтвердження відповідності комплексу технічного захисту інформації здійснюється за результатами проведеної атестації такого комплексу. Порядок атестації комплексу технічного захисту інформації визначається спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, обробляється на об’єкті інформаційної діяльності автономно пристроями обробки інформації за умови забезпечення режимними (організаційними) заходами захисту від витоку такої інформації, а в разі обробки інформації, що становить державну таємницю - за умови застосування комплексу технічного захисту інформації від витоку технічними каналами з підтвердженою відповідністю.

Програмне забезпечення, що забезпечує функціонування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляється інформація, що становить державну таємницю, використовуються за умови проведення державної експертизи у сфері захисту інформації, здійсненої в порядку, встановленому Кабінетом Міністрів України.

Національний банк України визначає умови обробки інформації в системах у сфері надання банківських, інших фінансових та платіжних послуг, інформації з обмеженим доступом, що є складовою системи депозитарного обліку депозитарію Національного банку України, та використання засобів захисту такої інформації в системах Національного банку України, банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг»;

7) доповнити статтею 8^1 такого змісту:

«Стаття 8^1. Умови озвучування інформації на об’єкті інформаційної діяльності

Інформація, що становить державну таємницю, повинна озвучуватися на об’єкті інформаційної діяльності із застосуванням комплексу технічного захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексу технічного захисту інформації здійснюється за результатами проведеної атестації такого комплексу. Порядок атестації комплексу технічного захисту інформації визначається спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації. Для створення комплексу

технічного захисту інформації використовуються засоби технічного захисту інформації, що мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або документ про відповідність, виданий органом з оцінки відповідності, який акредитовано національним органом України з акредитації.

Озвучування на об’єкті інформаційної діяльності іншої інформації з обмеженим доступом із застосуванням комплексу технічного захисту інформації з підтвердженою відповідністю може здійснюватися за рішенням володільця інформації.

Порядок створення, проведення атестації та експлуатації комплексів технічного захисту інформації визначається спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації»;

8) у статті 9:

назву доповнити словами «та на об’єкті інформаційної діяльності»;

у частині першій після слова «власника» доповнити словами «або розпорядника»;

у частині другій слова «службу захисту інформації» замінити словами «підрозділ із кіберзахисту»;

Доповнити абзацами третім та четвертим такого змісту:

«Відповідальність за забезпечення захисту інформації, що автономно озвучується та/або обробляється пристроями обробки інформації на об’єкті інформаційної діяльності, покладається на власника або розпорядника об’єкта інформаційної діяльності.

Власник або розпорядник об’єкта інформаційної діяльності, на якому автономно обробляється та/або озвучується пристроями обробки інформації інформація, що становить державну таємницю, утворює підрозділ з технічного захисту інформації або призначає осіб, на яких покладаються обов'язки щодо забезпечення захисту інформації від витоку технічними каналами та здійснення контролю за ним. За рішенням власника або розпорядника об’єкта інформаційної діяльності зазначені обов’язки можуть покладатися на підрозділ із кіберзахисту або осіб, на яких покладаються обов'язки здійснювати забезпечення захисту інформації та контролю за ним»;

9) у статті 10:

назву доповнити словами «та на об’єктах інформаційної діяльності»;

частину першу викласти в такій редакції:

«Вимоги захисту в системах, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та

організації, органи місцевого самоврядування та в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом (крім вимог щодо забезпечення захисту інформації, встановлених законами у сфері надання банківських, інших фінансових послуг, крім професійної діяльності на ринках капіталу та діяльності у системі накопичувального пенсійного забезпечення, та платіжних послуг), та на об’єктах інформаційної діяльності, встановлюються Кабінетом Міністрів України»;

у частині третій:

абзаци п’ятий і шостий викласти в такій редакції:

«здійснює державний контроль за додержанням вимог законодавства у сфері технічного захисту інформації (крім об'єктів критичної інфраструктури банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг, а також єдиної системи технічних засобів, яка призначена для зняття інформації з електронних комунікаційних мереж);

здійснює заходи щодо виявлення загроз державним інформаційним ресурсам від несанкціонованих дій та від витоку інформації технічними каналами в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, а також від витоку інформації технічними каналами на об’єктах інформаційної діяльності, та надає рекомендації щодо запобігання таким загрозам";

доповнити абзацами сьомим – десятим такого змісту:

«забезпечує реалізацію та здійснює методичне керівництво підтвердження відповідності комплексної системи захисту інформації, авторизацією з безпеки, порядок проведення яких затверджується Кабінетом Міністрів України;

визначає порядок ведення переліку авторизованих систем;

здійснює включення систем з безпеки до переліку авторизованих систем та виключення з такого переліку»;

розробляє та затверджує базовий профіль безпеки як мінімальний набір заходів захисту, встановлених для відповідної категорії інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси;

частину п’яту викласти в такій редакції:

Органи державної влади, державні органи, органи місцевого самоврядування, в порядку, встановленому Кабінетом Міністрів України, з

урахуванням набору мінімальних вимог заходів захисту встановлених для відповідних систем, розробляють та затверджують галузевий та/або цільові профілі безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, власником (розпорядником) яких вони є.

«Національний банк України встановлює вимоги щодо забезпечення захисту інформації (вимоги щодо захисту якої встановлені законами у сфері надання банківських, інших фінансових, крім професійної діяльності на ринках капіталу та діяльності у системі накопичувального пенсійного забезпечення, та платіжних послуг) у системах Національного банку України, банків, інших осіб, що здійснюють діяльність на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг»;

10) назву та частину першу статті 11 після слів «в системах» доповнити словами «та на об’єктах інформаційної діяльності».

11) у статті 13:

назву викласти у такій редакції:

«Стаття 13. Прикінцеві та перехідні положення»;

доповнити підпунктом 1^1 такого змісту:

«1^1. Установити, що комплексні системи захисту інформації, системи управління інформаційною безпекою з підтвердженою відповідністю, що були створені та застосовувалися до набрання чинності Законом України «Про внесення змін до деяких законів України щодо посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури», залишаються чинними відповідно до умов їх створення та не потребують повторного підтвердження відповідності (авторизації)».

3. В абзаці четвертому частини другої статті 5 Закону України «Про функціонування паливно-енергетичного комплексу в особливий період» (Відомості Верховної Ради України, 2006 р., № 52, ст. 526 із наступними змінами) слова «державної системи урядового зв’язку» замінити словами «національної системи урядових електронних комунікацій».

4. Частину другу статті 2 Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» (Відомості Верховної Ради України, 2007 р., № 29, ст. 389 із наступними змінами) після слів «(у частині нагляду (контролю) за суднами)» доповнити словами «державного контролю за додержанням вимог законодавства у сферах технічного захисту інформації та кіберзахисту, що здійснюється Державною службою спеціального зв'язку та захисту інформації України».

5. У Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» (Відомості Верховної Ради України, 2014 р., № 25, ст. 890 із наступними змінами):

1) у частині першій статті 1:

абзац другий виключити;

абзаци шостий і сьомий викласти в такій редакції:

«допуск до експлуатації - комплекс організаційно-технічних заходів з проведення тематичних досліджень засобів криптографічного захисту інформації, криптографічних алгоритмів, які призначені для захисту службової інформації або інформації, що становить державну таємницю, та державної експертизи їх результатів з метою встановлення можливості їх використання за призначенням;

експертні дослідження – дослідження та аналіз конкретних властивостей засобів криптографічного захисту інформації, криптографічних алгоритмів з метою перевірки їх відповідності вимогам нормативно-правових актів, оцінки ступеня захищеності інформації або їх науково-технічного рівня»;

абзаци дев’ятий і десятий виключити;

абзаци сімнадцятий і вісімнадцятий викласти в такій редакції:

«тематичні дослідження – дослідження щодо встановлення відповідності засобів криптографічного захисту інформації, криптосистем, криптографічних алгоритмів, які призначені для захисту службової інформації або інформації, що становить державну таємницю, вимогам тактико-технічних завдань на їх створення, нормативно-правових актів у сфері криптографічного захисту інформації, а також вимогам із захисту від витоку інформації каналами побічних електромагнітних випромінювань і наведень;

урядовий зв’язок – спеціальний зв’язок, надання якого забезпечується національною системою урядових електронних комунікацій»;

доповнити з урахуванням алфавітного порядку термінами такого змісту:

«верифікація – комплекс заходів щодо перевірки відповідності програмних і технічних засобів вимогам, встановленим нормативними документами»;

«засіб технічного захисту інформації – технічний або програмний засіб, у якому передбачено функції технічного захисту інформації, технічний або програмний засіб, спеціально розроблений для пошуку закладних пристроїв або контролю ефективності технічного захисту інформації»;

«національна система урядових електронних комунікацій – загальнодержавна спеціальна інформаційно-комунікаційна система, створена на базі державної системи урядового зв'язку, яка функціонує в інтересах

здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період із забезпеченням передавання, приймання та оброблення інформації, що становить державну таємницю, та іншої інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом»;

«орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам – установа або організація Державної служби спеціального зв'язку та захисту інформації України, до функцій якої віднесено розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення, запровадження та застосування стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам»;

«оцінювання стану кіберзахисту – процес перевірки обраних та/або запроваджених методів, заходів, засобів захисту інформації або кіберзахисту з метою встановлення поточного та/або цільового стану захищеності або їх відповідності вимогам законодавства щодо повноти запроваджених заходів захисту інформації або кіберзахисту, або відповідності національним стандартам у сфері захисту інформації або кіберзахисту або стандартам, настановам, рекомендаціям, аналітичним оглядам та іншим документам, розробленим та прийнятим іноземними та міжнародними організаціями»;

«репозитарій інформації про інциденти кібербезпеки – електронна база даних, в якій накопичуються, зберігаються і систематизуються відомості про інциденти кібербезпеки у порядку, встановленому Державною службою спеціального зв'язку та захисту інформації України»;

«спеціальна інформаційно-комунікаційна система – інформаційно-комунікаційна система, яка забезпечує оброблення інформації, що становить державну таємницю, та іншої інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, із застосуванням технічних засобів електронних комунікацій і засобів криптографічного захисту інформації»;

«стандарт криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам – стандарт, прийнятий органом стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, що встановлює для загального і неодноразового використання правила та настанови щодо діяльності у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам і спрямований на впорядкування у зазначених сферах»;

«стандартизація криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам – діяльність із встановлення для загального і неодноразового використання правил та настанов щодо наявних чи потенційних завдань, спрямована на впорядкування у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам»;

«таксономія інцидентів кібербезпеки – схема понять та класифікації інцидентів кібербезпеки, призначена для застосування при обміні, повідомленні, зберіганні інформації та підготовці звітів про кіберінциденти»;

2) у частині першій статті 2:

слова «державної системи урядового зв’язку» замінити словами «національної системи урядових електронних комунікацій»;

доповнити абзацом другим такого змісту:

«Державна служба спеціального зв’язку та захисту інформації України є центральним органом виконавчої влади, що забезпечує здійснення повноважень регулятора комунікаційних послуг при наданні хмарних послуг»;

3) у статті 3:

в абзаці другому слова «державної системи урядового зв’язку» замінити словами «національної системи урядових електронних комунікацій»;

абзац сьомий викласти в наступній редакції: «формування та реалізація державної політики у сфері державного контролю за додержанням вимог законодавства у сферах технічного захисту інформації та кіберзахисту об'єктами державного контролю у сферах технічного захисту інформації та кіберзахисту;

доповнити новим абзацем восьмим-дев’ятим такого змісту:

«формування та реалізація державної політики у сфері кіберзахисту щодо обміну інформацією про інциденти кібербезпеки, кібератаки та кіберзагрози, реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, оцінювання стану кіберзахисту;»

«здійснення стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;»

4) частину четверту статті 5 доповнити абзацом такого змісту:

«В особливий період загальна чисельність Державної служби спеціального зв’язку та захисту інформації України збільшується на кількість особового складу, призваного на військову службу до Державної служби спеціального зв’язку та захисту інформації України на виконання указів Президента України про мобілізацію, затверджених законами»

5) абзац третій частини першої статті 9 викласти в такій редакції:

«забезпечення функціонування, безпеки та розвитку підсистеми польового урядового зв’язку як складової національної системи урядових електронних комунікацій»;

6) у частині першій статті 14:

пункт 1 викласти в такій редакції:

«1) формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, захисту державних інформаційних ресурсів та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності, протидії технічним розвідкам, активної протидії агресії у кіберпросторі; у сфері державного контролю за додержанням вимог законодавства у сферах технічного захисту інформації та кіберзахисту; у сфері кіберзахисту щодо обміну інформацією про інциденти кібербезпеки, кібератаки та кіберзагрози; у сфері оцінювання стану кіберзахисту, а також щодо реагування на кіберінциденти, кібератаки, кіберзагрози»;

у пункті 9 слова «засобів, комплексів та систем спеціального зв’язку» виключити;

пункт 13 викласти в такій редакції:

«13) забезпечення в порядку, встановленому Кабінетом Міністрів України, функціонування національної системи урядових електронних комунікацій, її безпеки, розвитку та готовності до роботи в особливий період і в разі виникнення надзвичайної ситуації»;

пункт 19 викласти в такій редакції:

«19) вирішення в межах повноважень питань забезпечення зв’язку для потреб національної системи урядових електронних комунікацій, Національної системи конфіденційного зв’язку, відповідних органів державної влади згідно із законодавством»;

в абзаці п’ятому пункту 29 слова «та обладнання спеціального зв’язку» виключити;

пункти 30 і 39 викласти в такій редакції:

«30) встановлення порядку організації та проведення державної експертизи у сфері криптографічного та технічного захисту інформації; забезпечення реалізації проведення державної експертизи щодо відсутності у програмному забезпеченні недокументованих функцій; проведення експертних та тематичних досліджень у сфері криптографічного захисту інформації; визначення криптографічних алгоритмів як рекомендованих; надання допуску до експлуатації засобів криптографічного захисту інформації; видача експертних висновків за результатами державної експертизи у сфері криптографічного захисту інформації, свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації; реєстрація експертних висновків за результатами державної експертизи у сфері технічного захисту інформації, декларацій та атестатів відповідності комплексних систем захисту інформації»;

«39) забезпечення функціонування CERT-UA»;

пункт 48 після слів «ключових документів» доповнити словами «та державних шифрів»;

у пункті 50:

абзац другий викласти в такій редакції:

«технічних вимог до електронних комунікаційних мереж та комплексів спеціального зв’язку»;

в абзаці третьому слова «і засобів спеціального зв’язку» виключити;

пункти 67 і 72 викласти в такій редакції:

«67) організація та забезпечення служби з охорони об’єктів, приміщень, систем, мереж урядового і спеціального зв’язку, ключових документів та державних шифрів до засобів криптографічного захисту інформації»;

«72) здійснення відповідно до законодавства підготовки, перепідготовки та підвищення кваліфікації осіб у сферах кіберзахисту, криптографічного та технічного захисту інформації, електронних комунікацій та радіочастотного спектра»;

доповнити пунктом 77^1 такого змісту:

«77^1) затвердження переліків стандартів, настанов, рекомендацій, аналітичних оглядів та інших документів, розроблених та прийнятих іноземними та міжнародними організаціями з питань, що належать до повноважень Державної служби спеціального зв’язку та захисту інформації України, у тому числі документів The International Organization for Standartization (ISO), The European Committee for Standartization (CEN), The European Telecommunications Standart Institute (ETSI), International Telecommunications Union (ITU), The European Union Agency for Cybersecurity (ENISA), The Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), The North Atlantic Treaty Organization (NATO), а також визнаних цими організаціями процедур оцінки відповідності, включаючи, сертифікацію, рекомендованих для застосування у сферах організації спеціального зв’язку, захисту інформації, кіберзахисту»;

пункт 90 викласти в такій редакції:

«90) методичне регулювання оцінювання стану кіберзахисту, стану захищеності інформації, проведення оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури»;

пункт 91 виключити;

доповнити пунктами 96-117 такого змісту:

«96) встановлення вимог щодо впровадження постачальниками (їхніми субпідрядниками) заходів безпеки інформації відповідно до рівня ризику, пов’язаного з постачанням товарів, робіт і послуг власникам/розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, а також об'єктів критичної інформаційної інфраструктури.

Такі вимоги щодо впровадження заходів безпеки інформації застосовуються до постачальників (їх субпідрядників) лише у разі, якщо товари, роботи, послуги, які вони постачають, забезпечують функціонування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, а також об'єктів критичної інформаційної інфраструктури.

З метою встановлення таких вимог Державна служба спеціального зв’язку та захисту інформації України визначає критерії критичності таких товарів, робіт, послуг; встановлює порядок визначення власниками/розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, а також об'єктів критичної інформаційної інфраструктури, рівня ризику, пов’язаного з критичністю таких товарів, робіт і послуг для забезпечення функціонування та заходів безпеки інформації, що відповідають такому ризику; встановлює порядок підтвердження постачальниками (їх субпідрядниками) відповідності впроваджених заходів безпеки інформації встановленим вимогам відповідно до рівня ризику, пов’язаного з постачанням товарів, робіт і послуг.

97) забезпечення формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання відповідно до порядку, затвердженого Кабінетом Міністрів України;

98) забезпечення реалізації порядку організації та проведення державної експертизи у сфері захисту інформації щодо відсутності у програмному забезпеченні недокументованих функцій, надання висновків за результатами такої державної експертизи;

99) створення та забезпечення функціонування лабораторії з пошуку недокументованих функцій у програмному забезпеченні;

100) забезпечення реалізації порядку пошуку та/або виявлення потенційних вразливостей в інформаційно-комунікаційних системах, в яких

обробляються державні інформаційні ресурси або інформація з обмеженим доступом, а також на об'єктах критичної інформаційної інфраструктури;

101) забезпечення організації та систематичного проведення навчань з питань вимог до технічного захисту та кіберзахисту об'єктів державного контролю у сферах технічного захисту інформації та кіберзахисту та оцінювання стану кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи з технічного захисту або кіберзахисту в органах державної влади, державних органах, органах місцевого самоврядування, що є власниками/розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, та в юридичних особах, які є власниками/розпорядниками об’єктів критичної інформаційної інфраструктури;

102) визначення типових вимог до підрозділів із кіберзахисту, загальних вимог до керівників із кіберзахисту в органах державної влади, державних органах, державних установах, організаціях та до осіб, що виконують функції та завдання керівників із кіберзахисту в юридичних особах щодо об'єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких вони є, та органах місцевого самоврядування;

103) забезпечення нормативно-правового регулювання відносин у сферах стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;

104) забезпечення розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам в порядку, встановленому Кабінетом Міністрів України;

105) призначення органу стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам з числа установ і організацій Державної служби спеціального зв’язку та захисту інформації України;

106) забезпечення реалізації та методичне керівництво авторизацією систем з безпеки, порядок проведення якої затверджується Кабінетом Міністрів України;

107) встановлення порядку ведення переліку авторизованих систем, включення таких систем до переліку та виключення з нього, надання доступу до переліку та інформації з нього;

108) впровадження та забезпечення функціонування системи професійної кваліфікації за групами кваліфікації у сферах захисту інформації та кіберзахисту, системи оцінювання та визнання таких кваліфікацій на основі відповідних професійних стандартів, затвердження у встановленому порядку

відповідних професійних стандартів, дотримання яких є обов’язковим в органах державної влади, державних органаз, органах місцевого самоврядування, державних установах, організаціях, та які рекомендуються до застосування на об'єктах критичної інфраструктури;

109) створення та забезпечення функціонування кваліфікаційного центру за групами кваліфікацій у сферах безпеки інформації та кіберзахисту;

110) забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;

111) координація діяльності об’єктів критичної інфраструктури з питань кіберзахисту у разі введення надзвичайного стану або воєнного стану;

112) забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози;

113) проведення у встановленому законом порядку судових експертиз та експертних досліджень у сферах криптографічного захисту інформації, технічного захисту інформації, протидії технічним розвідкам, кібербезпеки, кіберзахисту та надання електронних довірчих послуг щодо:

верифікації програмних та технічних засобів;

аналізу наявності у програмних та технічних засобах механізмів криптографічного захисту інформації (застосованих криптографічних алгоритмів і криптопротоколів та їх криптографічної стійкості);

програмного забезпечення на наявність/відсутність недокументованих функцій;

комплексних систем захисту інформації інформаційно-комунікаційних систем та засобів технічного і криптографічного захисту інформації;

аналізу наявності відомостей, що можуть становити державну таємницю, у матеріальних носіях, що містять відомості у сферах технічного та криптографічного захисту інформації, спеціального зв’язку;

аналізу належності програмних та технічних засобів захисту інформації до товарів подвійного використання;

114) визначення для виконання завдання щодо функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози:

основних завдань, що можуть бути делеговані національною командою реагування галузевим та регіональним командам реагування, та порядку взаємодії таких команд з національною командою реагування;

вимог до організаційно-технічної спроможності, до сервісу з управління інцидентами кібербезпеки національної команди реагування, галузевих, регіональних команд реагування, а також приватних команд реагування в

частині виконання ними завдань галузевої або регіональної команди реагування або в частині надання ними послуг з управління інцидентами кібербезпеки органам державної влади, державним органам, органам місцевого самоврядування та юридичним особам щодо об’єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких вони є;

порядку ведення репозитарію інформації про інциденти кібербезпеки, таксономій інцидентів кібербезпеки та їх версій;

порядку здійснення моніторингу за діяльністю національної команди реагування, галузевих та регіональних команд реагування, а також приватних команд реагування в частині виконання ними завдань галузевої або регіональної команди реагування або надання послуг з управління інцидентами кібербезпеки органам державної влади, державним органам, органам місцевого самоврядування та юридичним особам щодо об'єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких вони є, зокрема щодо додержання вимог закону в частині функціонування національних систем реагування та обміну інформацією відповідно до сфери своїх повноважень та надання вимог про усунення порушень;

порядку здійснення заходів реагування у кризовій ситуації в кіберпросторі;

підстав надання на основі отриманої від CERT-UA інформації вимог про реагування власникам/розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об’єктів критичної інформаційної інфраструктури, а також порядку, строків реалізації визначених відповідною вимогою про реагування заходів реагування та подання звіту про їх виконання;

115) встановлення для виконання завдання щодо функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози:

порядку обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози, форм повідомлення, національної таксономії інцидентів кібербезпеки;

критеріїв для визначення значності впливу інциденту кібербезпеки, кібератаки, у тому числі для цілей визначення обов'язку здійснення повідомлення оператором критичної інфраструктури;

116) впровадження організаційно-технічних заходів щодо створення національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози;

117) забезпечення функціонування платформи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози та встановлення порядку приєднання до такої платформи»;

7) у частині першій статті 15:

пункт 1 викласти в такій редакції:

«1) вимагати у випадках, передбачених законодавством України і у встановлені строки шляхом направлення письмового запиту надання органами державної влади, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, підприємствами, установами і організаціями незалежно від форми власності інформації, документів і матеріалів, необхідних для виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань»;

доповнити пунктами 1^1 і 1^2 такого змісту:

«1^1) надавати обов'язкові до виконання вимоги про усунення встановлених відповідно до закону порушень законодавства щодо функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози, щодо невиконання вимог законодавства за результатами моніторингу в порядку, визначеному законодавством за діяльністю команд реагування.

1^2) у визначених законодавством випадках вживати заходів оперативного реагування на кіберзагрози та інциденти кібербезпеки, кібератаки шляхом надання обов'язкових до виконання вимог про реагування власникам/розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури.

Таке оперативне реагування шляхом надання вимоги про реагування є актом організаційно-розпорядчого характеру і не є заходом державного контролю за технічним захистом інформації та кіберзахистом, та здійснюється з метою унеможливлення або мінімізації негативних наслідків у зв'язку з інцидентом кібербезпеки, кібератакою або кіберзагрозою»;

в абзаці третьому пункту 8 слова «засобів, комплексів та систем спеціального зв'язку» виключити;

у пункті 10 слова «державної системи урядового зв'язку» замінити словами «національної системи урядових електронних комунікацій»;

у пункті 21 слова «державної системи урядового зв'язку» замінити словами «національної системи урядових електронних комунікацій»;

пункт 22 після слів «ключових документів» доповнити словами «та державних шифрів»;

8) доповнити статтею 15^1 такого змісту:

Стаття 15^1. Основні засади здійснення державного контролю за станом технічного захисту інформації та кіберзахисту

1. Державна служба спеціального зв'язку та захисту інформації України здійснює державний контроль за додержанням вимог законодавства у сферах технічного захисту інформації та кіберзахисту об'єктами державного контролю у сферах технічного захисту інформації та кіберзахисту (далі – державний контроль за технічним захистом інформації та кіберзахистом), а також у сфері протидії іноземним технічним розвідкам.

2. Державний контроль за технічним захистом інформації та кіберзахистом здійснюється щодо власників, розпорядників інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об’єктів критичної інформаційної інфраструктури (крім систем банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг, а також єдиної системи технічних засобів, яка призначена для зняття інформації з електронних комунікаційних мереж) (далі – об'єкти контролю).

3. Предметом державного контролю за технічним захистом інформації та кіберзахистом є дотримання вимог законодавства щодо технічного захисту інформації, кіберзахисту об’єктами контролю.

4. Державний контроль за технічним захистом інформації та кіберзахистом здійснюється Державною службою спеціального зв'язку та захисту інформації України шляхом здійснення відповідних заходів контролю, зокрема у формі планових та позапланових перевірок об'єктів контролю.

5. У разі виявлення за результатами державного контролю порушень вимог законодавства у сферах технічного захисту інформації та кіберзахисту надаються обов'язкові до виконання вимоги про усунення порушень законодавства. Вимоги про усунення порушень є обов'язковими для виконання об'єктами контролю.

6. Посадові особи Державної служби спеціального зв'язку та захисту інформації України, уповноважені на здійснення заходів державного контролю за технічним захистом інформації та кіберзахистом, під час здійснення таких заходів мають право:

1) встановлювати особу керівника об'єкта контролю (особу, яка виконує його обов’язки) шляхом перевірки документа, що засвідчує особу;

2) отримувати доступ (з дотриманням вимог нормативно-правових актів щодо охорони державної таємниці в Україні) до території, будівель, споруд, приміщень, інших об'єктів об'єкта контролю за умови, якщо це необхідно для дослідження питань, безпосередньо пов’язаних із об’єктом та предметом державного контролю за технічним захистом інформації та кіберзахистом;

3) ознайомлюватися з усіма документами та матеріалами, необхідними для здійснення заходів державного контролю за технічним захистом інформації та кіберзахистом;

4) отримувати інформацію, у тому числі інформацію з обмеженим доступом з дотриманням відповідних зобов'язань щодо її охорони, копії необхідних документів, письмові та усні пояснення посадових осіб з питань, що безпосередньо пов’язані із об’єктом та предметом державного контролю за технічним захистом інформації та кіберзахистом;

5) отримувати та безпосередньо фіксувати інформацію, у тому числі інформацію з обмеженим доступом з дотриманням вимог щодо її охорони, про порушення вимог законодавства у сферах технічного захисту інформації та кіберзахисту шляхом створення знімків екрана та використання засобів фото-, відеозйомки;

6) надавати за результатом здійснення заходів державного контролю обов'язкові до виконання вимоги про усунення порушень законодавства, здійснювати контроль за їх виконанням;

7) складати протоколи про адміністративні правопорушення, отримувати персональні дані та інші дані, необхідні для складання такого протоколу, та надсилати до суду матеріали про адміністративні правопорушення.

7. У разі виявлення за результатом здійснення заходів державного контролю порушень законодавства у сферах технічного захисту інформації та кіберзахисту або у разі недотримання законних вимог винні особи притягаються до відповідальності відповідно до закону.

8. Порядок здійснення державного контролю за технічним захистом інформації та кіберзахистом, періодичність проведення планових перевірок з урахуванням рівня ризику об’єкту контролю, підстави проведення позапланових перевірок, порядок надання та виконання вимог про усунення порушень, з урахуванням обмежень щодо обігу розвідувальної інформації, затверджуються Кабінетом Міністрів України».

6. Частину другу статті 2 Закону України «Про стандартизацію» (Відомості Верховної Ради України, 2014 р., № 31, ст. 1058) після слів «військові стандарти» доповнити словами «стандарти криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам».

7. У Законі України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради України, 2017 р., № 45, ст. 403 із наступними змінами):

1) у частині першій статті 1:

пункт 7 викласти в такій редакції:

«7) кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки та стійкості, цілісності, доступності і конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки»;

у пункті 17 слова «спеціальних телекомунікаційних систем (мереж)» замінити словами «спеціальних електронних комунікаційних систем (мереж)», а слова «інших комунікаційних систем» – словами «інших електронних комунікаційних систем»;

доповнити пунктами 24 і 25 такого змісту:

«24) кризова ситуація у сфері кібербезпеки – порушення або загроза порушення режиму функціонування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури у зв'язку з інцидентом кібербезпеки, кібератакою або кіберзагрозою, переривання яких може призвести до значних негативних наслідків для національної безпеки;

25) реагування на інциденти кібербезпеки – структурована сукупність дій, спрямованих на підготовку до інциденту кібербезпеки, виявлення та аналіз інциденту, мінімізацію шкоди від інциденту та запобігання повторенню інциденту у майбутньому»;

2) пункт 2 частини першої статті 2 виключити;

3) у статті 4:

у пунктах 1 і 3 частини другої слова «комунікаційні системи» замінити словами «інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи»;

в абзаці першому частини третьої слова «перелік таких об’єктів» виключити;

доповнити частиною четвертою такого змісту:

«4. Обов’язковою умовою використання програмного забезпечення та комунікаційного (мережевого) обладнання в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких

обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, а також на об’єктах критичної інформаційної інфраструктури є відсутність таких продуктів та обладнання у відкритому переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання.

Порядок формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання затверджуються Кабінетом Міністрів України.

Повноваження щодо забезпечення формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання покладаються на Державну службу спеціального зв’язку та захисту інформації України.»;

4) у статті 5:

частини другу і третю викласти в такій редакції:

«2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, координацію суб'єктів національної системи реагування, зокрема під час функціонування національної системи обміну інформацією, оголошує кризову ситуацію у сфері кібербезпеки, координує реалізацію Стратегії кібербезпеки України, надає Раді національної безпеки і оборони України пропозиції щодо її формування та уточнення.

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; затверджує національний план реагування; затверджує загальні вимоги з кіберзахисту об’єктів критичної інфраструктури; забезпечує функціонування системи оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури (крім об’єктів критичної інфраструктури у банківській системі України), зокрема шляхом прийняття постанов та розпоряджень; встановлює порядок взаємодії суб'єктів національної системи реагування, їх взаємодії із суб'єктами забезпечення кібербезпеки, з правоохоронними органами та суб'єктами оперативно-розшукової діяльності»;

пункт 7 частини четвертої викласти в такій редакції:

«7) оператори критичної інфраструктури та власники/розпорядники критичної інформаційної інфраструктури»;

5) доповнити статтею 5^1 такого змісту:

«Стаття 5^1. Підрозділи з кіберзахисту, керівники із кіберзахисту

1. В органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, утворюються підрозділи з кіберзахисту та призначаються керівники із кіберзахисту, яким безпосередньо підпорядковуються такі підрозділи, а в органах місцевого самоврядування особи, що виконують їх функції та завдання.

Власники/розпорядники об’єктів критичної інформаційної інфраструктури призначають відповідальну особу, яка виконує функції та завдання керівника із кіберзахисту, та з метою забезпечення виконання вимог з кіберзахисту, створюють підрозділ із кіберзахисту (за необхідності).

2. Керівники із кіберзахисту або відповідальні особи, які виконують функції та завдання керівника із кіберзахисту, здійснюють керівництво, координацію та контроль з питань кіберзахисту відповідного об’єкта критичної інформаційної інфраструктури або органу державної влади, органу місцевого самоврядування, що є власником або розпорядником інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, у тому числі у разі введення воєнного стану.

3. Типові вимоги до підрозділів з кіберзахисту, загальні вимоги до керівників із кіберзахисту (або осіб, що виконують їх функції та завдання) в органах державної влади, а також до відповідальних осіб, які виконують завдання та функції керівника із кіберзахисту в юридичних особах, що є власниками/розпорядниками об’єктів критичної інформаційної інфраструктури I і II категорій критичності та органах місцевого самоврядування, визначаються Державною службою спеціального зв'язку та захисту інформації України. Загальні вимоги до відповідальних осіб, які виконують завдання та функції керівника із кіберзахисту на об’єктах критичної інфраструктури III і IV категорій критичності, визначаються Державною службою спеціального зв'язку та захисту інформації України і мають рекомендаційний характер.»;

6) статтю 6 викласти в такій редакції:

«Стаття 6. Кіберзахист критичної інфраструктури

1. Посадові особи операторів критичної інфраструктури, власників/розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечити дотримання вимог з кіберзахисту, повідомляти про інциденти кібербезпеки, кібератаки, виконувати інші зобов'язання щодо захисту інформації та кіберзахисту відповідно до законодавства, а також несуть відповідальність за невиконання таких вимог згідно із законом.

2. Оцінювання стану кіберзахисту щодо об'єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури проводиться добровільно або, у випадках визначених законодавством, обов’язково, з урахуванням методичного регулювання оцінювання стану кіберзахисту, загальних вимог до суб'єктів оцінювання стану кіберзахисту (крім оцінювання стану кіберзахисту щодо об’єктів критичної інформаційної інфраструктури III і IV категорій критичності), визначених Державною службою спеціального зв'язку та захисту інформації України.

7) у статті 8:

у частині другій:

абзац перший, пункти 1-3 викласти в такій редакції:

2. Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи України, Національний банк України, Міністерство закордонних справ України, Міністерство цифрової трансформації України, які відповідно до Конституції і законів України виконують у встановленому порядку такі основні завдання:

1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики з кіберзахисту державних інформаційних ресурсів та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інфраструктури; здійснює державний контроль за додержанням вимог законодавства у сферах технічного захисту інформації та кіберзахисту об'єктами державного контролю у сферах технічного захисту інформації та кіберзахисту; здійснює стандартизацію у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам; забезпечує створення та функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної електронної комунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, національної команди реагування на інциденти кібербезпеки, кібератаки (національний

CSIRT) CERT-UA; систематично організовує та проводить навчання з питань технічного захисту та кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи з кіберзахисту в органах державної влади, органах місцевого самоврядування, що є власниками/розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, та в юридичних особах, які є власниками/розпорядниками об'єктів критичної інфраструктури або об'єктів критичної інформаційної інфраструктури; забезпечує функціонування системи професійної кваліфікації за групами кваліфікацій у сферах захисту інформації та кіберзахисту; здійснює методичне регулювання оцінювання стану кіберзахисту, встановлює вимоги до суб'єктів оцінювання стану кіберзахисту щодо оцінювання інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури, виконує інші завдання та здійснює інші повноваження відповідно до закону;

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів; здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти об'єктів критичної інформаційної інфраструктури; здійснює заходи з інформування громадян про безпеку в кіберпросторі;

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, що вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством; негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів та інформації з обмеженим доступом категорій службова інформація та державна таємниця, критичної інформаційної інфраструктури; здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень щодо об'єктів критичної інформаційної інфраструктури, вчинених під час розвідувально-підривної діяльності проти України; забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки»;

доповнити пунктами 7 і 8 такого змісту:

«7) Міністерство закордонних справ України сприяє розвитку євроінтеграційних процесів щодо підходів, методів, засобів забезпечення

кібербезпеки, здійсненню узгоджених із ключовими міжнародними партнерами заходів, спрямованих на посилення кіберстійкості України та розвитку спроможностей національної системи кібербезпеки; забезпечує координацію відносин, спрямованих на практичну співпрацю з міжнародними партнерами, для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці; забезпечує активну участь України у міжнародних організаціях щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної міжнародної нормативно-правової бази; сприяє проведенню спільних з Європейським Союзом заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози; координує запровадження гармонізованого з євроатлантичною спільнотою підходу до застосування санкцій у відповідь на підривну діяльність у кіберпросторі, узгодження з міжнародними партнерами механізму спільних дипломатичних дій і заходів у відповідь на деструктивну кіберактивність, виконує інші завдання відповідно до закону;

8) Міністерство цифрової трансформації України здійснює стратегічне планування та програмно- цільове забезпечення заходів, спрямованих на посилення відмовостійкості та запобігання загрозам технологічної залежності від іноземних виробників і постачальників продукції, технологій та послуг, що забезпечують функціонування публічних електронних та державних інформаційних ресурсів, інформаційно-комунікаційних систем та електронних комунікаційних мереж; бере участь у формуванні державної політики у сфері кіберзахисту електронних публічних та державних інформаційних ресурсів, інформаційно-комунікаційних систем та електронних комунікаційних мереж, що забезпечують надання адміністративних, електронних публічних послуг та послуг електронного урядування; забезпечує формування та реалізацію державної інноваційної політики у сфері розвитку цифрових технологій, сприяє формуванню конкурентного середовища, державно-приватного партнерства і залученню інвестицій для розвитку інфраструктури, послуг і технологій у сфері кібербезпеки; бере участь спільно з іншими основними суб’єктами національної системи кібербезпеки у забезпеченні захисту стратегічних національних інтересів у кіберпросторі, розвитку відносин з міжнародними партнерами у сфері кібербезпеки, забезпечує посилення інтеграції з Європейським Союзом, його членами та євроатлантичної інтеграції у сфері кібербезпеки; координує і сприяє залученню міжнародної технічної допомоги для розвитку та посилення спроможностей національної системи кібербезпеки; забезпечує формування та реалізацію державної політики у сфері безпечного користування Інтернетом та цифровими технологіями для захисту користувачів, у тому числі дітей, у кіберпросторі»;

у частині третій:

викласти пункти 1-2 в такій редакції:

«1) формуванням і оперативної адаптації державної політики у сфері кібербезпеки, кіберзахисту, з урахуванням наявних або потенційних ризиків, впровадження кращих практик та досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правового регулювання в сфері кібербезпеки, кіберзахисту, що враховує ризик орієнтований підхід, чіткий розподіл ролей, завдань, функцій та відповідальності публічного сектору, операторів критичної інфраструктури та власників/розпорядників об'єктів критичної інформаційної інфраструктури, галузеву специфіку, гармонізацію практик та стандартів з Європейським Союзом та НАТО;»

пункт 3 виключити;

викласти пункт 4-8 в такій редакції:

«3) впровадження стимулювання розвитку індустрії послуг та продуктів в сфері кібербезпеки в Україні;

4) залучення експертного потенціалу приватного сектору, наукових установ, професійних та громадських об'єднань до розробки проектів концептуальних документів у сфері кібербезпеки;

5) систематичне проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи з кіберзахисту в органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси категорій службова інформація та державна таємниця, а також на об'єктах критичної інфраструктури

6) функціонування системи оцінювання стану кіберзахисту публічного сектору та критичної інфраструктури;

7) розвитку мережі команд реагування на інциденти кібербезпеки, кіберзагрози на національному, галузевому та регіональному рівнях, в тому числі, із залученням приватних команд реагування;»

пункти 9 вважати пунктом 8;

пункт 10 виключити;

пункт 11 вважати пунктом 9;

пункт 12 викласти в такій редакції:

«10) функціонування національних систем реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та обміну інформацією про інциденти кібербезпеки;»

пункт 17 викласти в такій редакції:

«15) впровадження державно-приватної взаємодії у сфері кібербезпеки, кіберзахисту з метою впровадження кращих практик та рішень при розбудові організаційно-технічної моделі кіберзахисту, включаючи реагування та обмін інформацією про інциденти кібербезпеки, кібератаки та кіберзагрози, усуненні їх наслідків;»

пункти 18-25 вважати пунктами 16-23 та доповнити пунктом 24 такого змісту:

«24) планування витрат та здійснення відповідного фінансування органами державної влади, органами місцевого самоврядування, операторами об'єктів критичної інфраструктури, власниками/розпорядниками об’єктів критичної інформаційної інфраструктури заходів кіберзахисту, передбачених законодавством»;

у частині п’ятій виключити слова «аудиту інформаційної безпеки та стану кіберзахисту об’єктів критичної інформаційної інфраструктури», а слова «кіберінциденти та кібератаки» замінити словами «інциденти кібербезпеки, кібератаки та кіберзагрози»;

доповнити частиною сьомою такого змісту:

«7. Розроблення та застосування платних, безоплатних умов пошуку та/або виявлення потенційних вразливостей в інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також на об'єктах критичної інформаційної інфраструктури повинні здійснюватися відповідно до порядку пошуку та/або виявлення потенційних вразливостей, встановленого Кабінетом Міністрів України.

Однією із складових такого порядку пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також на об'єктах критичної інформаційної інфраструктури має бути порядок розроблення та проведення програм пошуку та виявлення вразливостей за винагороду (Bug Bounty), а також порядок узгодженого розкриття вразливостей»;

8) статтю 9 викласти в такій редакції:

«Стаття 9. Національна система реагування на інциденти кібербезпеки, кібератаки, кіберзагрози

1. В Україні створюється та забезпечується функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси

або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури.

2. Уповноваженим органом, що здійснює забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози є Державна служба спеціального зв'язку та захисту інформації України.

3. До складу національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози входять:

1) CERT-UA, що є національною командою реагування на інциденти кібербезпеки, кібератаки, кіберзагрози (національний CSIRT), діяльність якої забезпечується Державною службою спеціального зв'язку та захисту інформації України та завданнями якої є:

моніторинг, накопичення та проведення аналізу даних про інциденти кібербезпеки, кібератаки, кіберзагрози на національному, секторальному, регіональному рівнях;

отримання та опрацювання у встановленому порядку обов'язкових та інших повідомлень, здійснених у межах національної системи обміну інформацією відповідно до цього Закону;

здійснення заходів із запобігання та інформування щодо інцидентів кібербезпеки, кібератак, кіберзагроз та вразливостей;

надання у встановленому порядку сервісу з реагування та рекомендацій з реагування власникам/розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторам критичної інфраструктури, та іншим суб'єктам (за необхідності);

інформування у встановленому порядку Державної служби спеціального зв'язку та захисту інформації України про інциденти кібербезпеки, кібератаки, кіберзагрози, виявлені або потенційні вразливості в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, а також на об'єктах критичної інформаційної інфраструктури із зазначенням обов'язкових та/або рекомендованих заходів реагування для видання вимоги про реагування;

здійснення аналізу ризиків у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою та надання рекомендацій щодо їх усунення;

забезпечення у встановленому порядку функціонування репозитарію інформації про інциденти кібербезпеки, таксономій інцидентів кібербезпеки та їх версій;

взаємодія у встановленому порядку з іншими суб'єктами національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;

взаємодія у встановленому порядку з суб'єктами національної системи обміну інформацією про інциденти кібербезпеки, кібератаки;

взаємодія у встановленому порядку з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності в межах, необхідних для виконання ними повноважень, визначених законом;

виконання функцій національного контактного центру відповідно до Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS Directive);

взаємодія з іноземними та міжнародними організаціями з питань реагування, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

взаємодія у встановленому порядку з суб'єктами приватного сектору, у тому числі з іноземними суб'єктами господарювання, з питань реагування;

2) галузеві та регіональні команди реагування на інциденти кібербезпеки, кібератаки, кіберзагрози (далі - галузеві та регіональні CSIRT), що створюються органами державної влади або органами місцевого самоврядування з метою посилення спроможності національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози у відповідній галузі, сфері або відповідному регіоні з урахуванням вимог до організаційно-технічної спроможності, встановлених Державною службою спеціального зв'язку та захисту інформації України, та взаємодіють з іншими суб'єктами національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України.

Альтернативою створення органами державної влади або органами місцевого самоврядування власних галузевих або регіональних CSIRT є залучення послуг приватних команд реагування, що виконують завдання та дотримуються вимог, встановлених для таких галузевих та регіональних CSIRT відповідно до законодавства.

Галузевим та регіональним CSIRT у порядку, визначеному Державною службою спеціального зв'язку та захисту інформації України, делегуються від національного CSIRT відповідні завдання щодо:

моніторингу та проведення аналізу даних про інциденти кібербезпеки, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні;

отримання та опрацювання у встановленому порядку обов'язкових та інших повідомлень у відповідній галузі або відповідному регіоні, здійснених у національній системі обміну інформацією згідно з цим Законом;

здійснення заходів із попередження та інформування щодо інцидентів кібербезпеки, кібератак, кіберзагроз та вразливостей;

надання у встановленому порядку сервісу з реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;

здійснення аналізу ризиків у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою та надання рекомендацій щодо їх усунення.

Галузеві та регіональні CSIRT, або приватні команди реагування що виконують їх завдання, здійснюють у встановленому порядку обмін інформацією з іншими суб'єктами національної системи обміну інформацією, координують свою діяльність та інформують CERT-UA щодо заходів реагування.

Державна служба спеціального зв'язку та захисту інформації України має право надавати вимоги про усунення порушень у діяльності галузевого або регіонального CSIRT у разі невідповідності вимогам щодо наявності організаційно-технічної спроможності або порушення встановленого порядку функціонування національної системи обміну інформацією або національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози.

Центр кіберзахисту Національного банку України (CSIRT-NBU) є галузевим CSIRT та діє у складі національної системи обміну інформацією та національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози з урахуванням постанов Національного банку України в частині, що не суперечить цьому Закону.

Центр кіберзахисту Міністерства оборони України (MIL.CERT-UA) є галузевим CSIRT та діє у складі національної системи обміну інформацією та національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози з урахуванням організаційно-розпорядчих актів Міністерства оборони України в частині, що не суперечить цьому Закону;

3) Національна поліція України, Служба безпеки України взаємодіють у рамках національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози з іншими суб'єктами національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України, з урахуванням вимог цього Закону та в межах своїх повноважень, визначених законами України.

Служба безпеки України визначає особливості здійснення реагування на кіберінциденти, кібератаки, кіберзагрози у сфері державної безпеки.

4) Об'єднана група реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, що функціонує на постійній основі з метою реагування на кризові ситуації та складається з представників Національного координаційного центру кібербезпеки, Державної служби спеціального зв'язку

та захисту інформації України, Національної поліції України, Служби безпеки України.

Персональний склад Об'єднаної групи реагування затверджується керівником Національного координаційного центру кібербезпеки за пропозиціями керівників відповідних органів.

За посадою Об'єднану групу реагування очолює заступник керівника Національного координаційного центру кібербезпеки.

До завдань Об'єднаної групи реагування належать:

взаємодія з власниками/розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторами критичної інфраструктури щодо об'єктів критичної інформаційної інфраструктури, щодо яких відбувся інцидент кібербезпеки, кібератака або існує кіберзагроза, що стали підставою для оголошення кризової ситуації, а також з постачальниками (їхніми субпідрядниками), товари, роботи, послуги яких можуть бути пов'язані з такими інцидентами кібербезпеки, кібератаками, кіберзагрозами та які можуть залучатися для належного здійснення заходів реагування;

здійснення заходів для координованого аналізу кризової ситуації, розроблення рекомендацій щодо реагування для всіх суб'єктів національної системи реагування, власників/розпорядників інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторів критичної інфраструктури з урахуванням порядку здійснення заходів реагування у кризовій ситуації у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою, встановленого Державною службою спеціального зв'язку та захисту інформації України;

залучення (за необхідності) додаткових сил та ресурсів суб'єктів національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози або інших суб'єктів забезпечення кібербезпеки.

У випадках та порядку, встановлених Кабінетом Міністрів України, для виконання завдань, визначених цим Законом, і з метою локалізації кібератак і інцидентів кібербезпеки, наслідки яких можуть призвести чи призвели до кризової ситуації, членам Об’єднаної групи реагування надається право безперешкодного доступу до інформаційно-комунікаційних і технологічних систем незалежно від розміщення їх компонентів:

органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до закону;

операторів критичної інфраструктури будь-якої категорії критичності, якщо органам державної влади, органам місцевого самоврядування прямо чи опосередковано належить частка у статутному капіталі такого оператора критичної інфраструктури у розмірі понад 50 відсотків або такі органи прямо чи опосередковано володіють більшістю голосів у вищому органі такого оператора критичної інфраструктури чи правом призначати більше половини складу виконавчого органу або наглядової ради такого оператора критичної інфраструктури;

інших операторів критичної інфраструктури I і II категорій критичності;

5) приватні команди реагування можуть залучатись для надання послуг з управління інцидентами кібербезпеки, кібератаками, кіберзагрозами власникам/розпорядникам критичної інформаційної інфраструктури, органам державної влади та органам місцевого самоврядування, виконання завдань галузевих та регіональних CSIRT, а також взаємодіяти з іншими суб'єктами національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, у тому числі щодо обміну інформацією про інциденти кібербезпеки, кібератаки, з урахуванням вимог до організаційно-технічної спроможності та в порядку, встановленому Державною службою спеціального зв'язку та захисту інформації України.

Суб'єкти національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози відповідно до законодавства забезпечують захист інформації з обмеженим доступом, отриманої під час здійснення своєї діяльності, та несуть кримінальну, адміністративну, цивільно-правову відповідальність за неправомірне розголошення, неправомірне розкриття, неправомірне використання та інші неправомірні дії з такою категорією інформації відповідно до закону.

Державна служба спеціального зв'язку та захисту інформації України, на основі отриманої від CERT-UA інформації з метою вжиття заходів оперативного реагування на кіберзагрози та інциденти кібербезпеки, кібератаки, може надавати обов’язкові до виконання вимоги про реагування власникам/розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об’єктів критичної інформаційної інфраструктури.

Таке оперативне реагування шляхом надання вимоги про реагування є актом організаційно-розпорядчого характеру і не є заходом державного контролю за технічним захистом інформації та кіберзахистом, та здійснюється з метою унеможливлення або мінімізації негативних наслідків у зв’язку з інцидентом кібербезпеки, кібератакою або кіберзагрозою.

Власники/розпорядники інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні

інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об’єктів критичної інформаційної інфраструктури, зобов’язані вжити визначених відповідною вимогою заходів реагування та подати звіт про вжиті заходи реагування у строк і порядку, встановлені Державною службою спеціального зв’язку та захисту інформації України.

Підстави надання вимог про реагування, строк і порядок подання звіту про вжиті заходи реагування встановлюються Державною службою спеціального зв'язку та захисту інформації України;

6) Національний координаційний центр кібербезпеки, що здійснює загальну координацію функціонування суб'єктів національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, для виконання своїх завдань має такі повноваження:

а) отримання від інших суб'єктів національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози з метою:

проведення аналізу стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури;

визначення наявності ознак кризової ситуації у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою;

здійснення координації між суб'єктами національної системи обміну інформацією та національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;

обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози між суб'єктами забезпечення кібербезпеки на базі технологічної платформи Національного координаційного центру кібербезпеки;

впровадження механізмів взаємодії основних суб'єктів національної системи кібербезпеки;

б) прийняття рішення про оголошення кризової ситуації у зв'язку з інцидентом кібербезпеки, кібератакою або кіберзагрозою;

в) прийняття рішення про задіяння Об'єднаної групи реагування;

г) здійснення координації між суб'єктами національної системи обміну інформацією та національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози у разі оголошення кризової ситуації»;

9) доповнити статтею 9^1 такого змісту:

«Стаття 9[1]. Національна система обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози

1. В Україні створюється та забезпечується функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури.

2. Уповноваженим органом, що здійснює забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози є Державна служба спеціального зв'язку та захисту інформації України (далі – Уповноважений орган).

Уповноважений орган визначає порядок, форми здійснення повідомлень про інциденти кібербезпеки, кібератаки, кіберзагрози з урахуванням обмежень, що унеможливлюють розкриття розвідувальної інформації, національну таксономію інцидентів кібербезпеки, впроваджує організаційно-технічні заходи щодо створення системи обміну інформацією, забезпечує функціонування платформи обміну інформацією та порядку приєднання до такої платформи.

3. Власники/розпорядники інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, зобов'язані повідомляти про всі інциденти кібербезпеки, кібератаки.

Власники/розпорядники об’єктів критичної інформаційної інфраструктури зобов'язані повідомляти про всі значні інциденти кібербезпеки, кібератаки.

Встановлення законами України зобов'язання для суб'єктів, що обробляють інші категорії інформації з обмеженим доступом, надавати обов'язкові повідомлення про інциденти кібербезпеки, кібератаки, є підставою для приєднання у встановленому порядку до національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози згідно з цим Законом.

Суб'єкти, для яких не встановлені зобов'язання надавати обов'язкові повідомлення про інциденти кібербезпеки, кібератаки мають право приєднатися до національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози та здійснювати добровільний обмін інформацією про інциденти кібербезпеки, кібератаки відповідно до встановленої національної таксономії інцидентів кібербезпеки та в порядку, визначеному Уповноваженим органом.

4. Усі обов'язкові повідомлення подаються суб'єктами, визначеними цією статтею, у строки та порядку, визначені Уповноваженим органом.

5. Уповноважений орган визначає критерії значності впливу інцидентів кібербезпеки, кібератаки, що призводить до обов'язку надавати обов'язкові повідомлення для власників/розпорядників критичної інформаційної інфраструктури згідно з цим Законом.

6. Посадові особи власників/розпорядників інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об’єктів критичної інформаційної інфраструктури несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов'язку надання обов'язкових повідомлень про інциденти кібербезпеки, кібератаки.

7. Інформація про інцидент кібербезпеки, кібератаку щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури є інформацією з обмеженим доступом, крім випадків, якщо порядком обміну такою інформацією або на підставі інших вимог законодавства передбачається обов'язок щодо її розкриття з визначеною метою»;

10) статтю 15 доповнити частиною четвертою такого змісту:

«4. Державна служба спеціального зв'язку та захисту інформації України здійснює державний контроль за додержанням вимог законодавства у сфері кіберзахисту відповідно до закону.

Основні засади здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту встановлюються Законом України «Про Державну службу спеціального зв'язку та захисту інформації України».

8. У частині першій статті 22 Закону України «Про національну безпеку України» (Відомості Верховної Ради України, 2018 р., № 31, ст. 241 із наступними змінами) слова «державної системи урядового зв’язку» замінити словами «національної системи урядових електронних комунікацій».

II. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через три місяці з дня його опублікування, крім пункту 2 цього розділу, який набирає чинності з дня його опублікування, крім підпункту 5 пункту 7 розділу I цього Закону, який набирає чинності з 1 січня 2025 року.

2. Кабінету Міністрів України вжити заходів щодо прийняття та/або оновлення нормативних актів органів виконавчої влади, що випливають з цього Закону, забезпечивши набрання ними чинності одночасно з набранням чинності цим Законом.

3. Кабінету Міністрів України у 2024 році поінформувати Верховну Раду України про стан виконання цього Закону.

Голова Верховної Ради України