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

1) у частині першій статті 1:

абзаци третій, сьомий і п'ятнадцятий викласти в такій редакції:

"виток інформації – результат дій або бездіяльності, внаслідок яких інформація, що обробляється в системі чи пристроєм обробки інформації, стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї";

"захист інформації в системі – діяльність, спрямована на запобігання порушенню цілісності, конфіденційності і доступності інформації в системі";

"обробка інформації в системі – виконання однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, що здійснюються в системі за допомогою технічних і програмних засобів 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 з безпеки – рішення щодо можливості функціонування (експлуатації) відповідної інформаційної, електронної комунікаційної, інформаційно-комунікаційної, технологічної системи з урахуванням

її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту, криптографічного захисту та кіберзахисту, що приймається у встановленому законодавством порядку";

"авторизована система з безпеки – інформаційна, електронна комунікаційна, інформаційно-комунікаційна, технологічна система або її окремі елементи, об'єкт критичної інформаційної інфраструктури, в яких запроваджені заходи та/або системи з безпеки інформації, що пройшли авторизацію з безпеки";

"комплекс технічного захисту інформації – сукупність заходів, засобів технічного захисту інформації, призначених для захисту інформації від витоку технічними каналами в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах";

"пристрої обробки інформації – технічні пристрої (засоби) обробки інформації, в яких технічно неможливо реалізувати програмні процедури розмежування доступу користувачів та інші функціональні послуги безпеки";

"перелік авторизованих систем з безпеки – єдина електронна база даних, що містить відомості про авторизовані системи з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, порядок ведення якої, порядок внесення даних щодо авторизованих систем з безпеки 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 з безпеки, що міститься в переліку, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом та інформації, доступ до якої обмежений відповідно до законодавства на період дії воєнного стану";

"технічний канал витоку інформації – взаємопов'язана сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки, спрямована на забезпечення витоку інформації";

2) статтю 8 викласти в такій редакції:

"Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі, об'єкті критичної інформаційної інфраструктури визначаються власником або розпорядником відповідної системи з урахуванням вимог щодо захисту інформації, визначених законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, у системах, об'єктах критичної

інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, мають оброблятися в авторизованих системах з безпеки або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності.

Авторизація з безпеки систем, об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, а також підтвердження дотримання вимог з безпеки щодо таких систем, об'єктів критичної інформаційної інфраструктури протягом їх життєвого циклу здійснюються в порядку, встановленому Кабінетом Міністрів України.

Складовою такого порядку авторизації з безпеки має бути встановлення повідомного (декларативного) принципу щодо прийняття власником або розпорядником системи, об'єкта критичної інформаційної інфраструктури (крім тих, в яких обробляється інформація, що становить державну таємницю) рішення про здійснення авторизації з безпеки з урахуванням відповідних профілів безпеки, а також строки та порядок підтвердження дотримання вимог відповідно до базового, цільового та галузевого (за наявності) профілів безпеки протягом життєвого циклу відповідної системи, об'єкта критичної інформаційної інфраструктури.

Підтвердження відповідності стандарту інформаційної безпеки за результатами процедури з оцінки відповідності національним стандартам України здійснюється органом з оцінки відповідності, який акредитовано національним органом України з акредитації чи національним органом з акредитації іноземної держави, якщо національний орган України з акредитації та національний орган з акредитації відповідної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

Процедура отримання сертифіката відповідності стандарту інформаційної безпеки не застосовується до систем, в яких обробляється інформація, що становить державну таємницю.

Авторизація з безпеки або отримання сертифіката відповідності стандарту інформаційної безпеки щодо систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, здійснюється за одночасного дотримання таких умов:

використання для захисту інформації в системах засобів технічного та/або криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або

криптографічного захисту інформації або документ про відповідність (крім систем, об'єктів критичної інформаційної інфраструктури, в яких обробляється службова інформація або інформація, що становить державну таємницю), виданий органом з оцінки відповідності, який акредитовано національним органом України з акредитації або національним органом з акредитації іноземної держави, якщо національний орган України з акредитації та національний орган з акредитації відповідної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

жодний з елементів системи, об'єкта критичної інформаційної інфраструктури не розташований на тимчасово окупованій території України, на території держави, визнаної Верховною Радою України державою-агресором, або на території держави, яка входить до митного або воєнного союзу з такими державами;

власник або розпорядник жодного з елементів системи, об'єкта критичної інформаційної інфраструктури не є юридичною або фізичною особою, зареєстрованою на тимчасово окупованій території України, резидентом держави, визнаної Верховною Радою України державою-агресором, резидентом держави, яка входить до митного або воєнного союзу з такими державами або щодо якої застосовано санкції відповідно до Закону України "Про санкції";

власник або розпорядник системи, об'єкта критичної інформаційної інфраструктури або його представник, який надає послуги з використанням системи, об'єкта критичної інформаційної інфраструктури, 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, має оброблятися в системі, об'єкті критичної інформаційної інфраструктури із застосуванням комплексу технічного захисту інформації з підтвердженою відповідністю та за умови використання засобів криптографічного захисту суб'єктів господарювання, які провадять ліцензовану діяльність відповідно до законодавства. Порядок атестації такого комплексу технічного захисту інформації визначається спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

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

Національний банк України визначає умови обробки інформації, використання засобів захисту інформації в системах у сфері надання платіжних, банківських та інших фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, валютного регулювання та валютного нагляду, а також у системі депозитарного обліку Національного банку України.

Власники або розпорядники систем, об'єктів критичної інформаційної інфраструктури для забезпечення їх належного функціонування та захисту інформації, що обробляється в них:

створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів, систем, об'єктів критичної інформаційної інфраструктури вимог щодо їх захисту, цілісності та конфіденційності;

забезпечують створення резервних копій державних інформаційних ресурсів, систем, об'єктів критичної інформаційної інфраструктури на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), під час дії воєнного стану в Україні та протягом шести місяців з дня його припинення чи скасування;

забезпечують в установленому законодавством порядку передачу (переміщення) державних інформаційних ресурсів та їх резервних копій для розміщення на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, під час дії воєнного стану в Україні та протягом шести місяців з дня його припинення чи скасування.

Розміщення систем, об'єктів критичної інформаційної інфраструктури або їх елементів та зберігання резервних копій державних інформаційних ресурсів на тимчасово окупованій території України, території держави, визнаної Верховною Радою України державою-агресором, або на території держави, яка входить до митного або воєнного союзу з такими державами, забороняється";

3) у статті 9:

частину першу після слова "власника" доповнити словами "або розпорядника";

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

4) у статті 10:

частину першу викласти в такій редакції:

"Мінімальні вимоги щодо заходів захисту як базовий профіль безпеки щодо систем, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, в яких обробляються державні інформаційні ресурси

або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом (крім вимог щодо забезпечення захисту інформації, встановлених законом у сфері надання платіжних, банківських та інших фінансових послуг), встановлюються Кабінетом Міністрів України";

у частині третій:

абзац шостий викласти в такій редакції:

"здійснює заходи щодо виявлення загроз державним інформаційним ресурсам від несанкціонованих дій та витоку інформації технічними каналами в інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних системах, надає рекомендації щодо запобігання таким загрозам";

після абзацу шостого доповнити трьома новими абзацами такого змісту:

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

затверджує порядок ведення переліку авторизованих систем з безпеки;

здійснює включення авторизованих систем з безпеки до переліку авторизованих систем з безпеки та виключення з такого переліку".

У зв'язку з цим абзац сьомий вважати абзацом десятим;

частини четверту і п'яту замінити чотирма новими частинами такого змісту:

"Органи державної влади, державні органи, органи місцевого самоврядування з урахуванням набору мінімальних вимог щодо заходів захисту (базового профілю безпеки), відповідних стандартів, політик безпеки, призначення системи, її структурно-функціональних характеристик, результатів аналізу ризиків безпеки та особливостей функціонування системи розробляють та затверджують цільові профілі безпеки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, власником або розпорядником яких вони є.

Органи державної влади, державні органи в межах своїх повноважень у відповідній сфері або галузі розробляють та за погодженням із Державною службою спеціального зв'язку та захисту інформації України затверджують галузеві профілі безпеки для відповідної сфери або галузі з урахуванням мінімальних вимог щодо заходів захисту (базового профілю безпеки), а також відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі.

Порядок затвердження цільових та галузевих профілів безпеки затверджується Кабінетом Міністрів України.

Національний банк України встановлює вимоги щодо забезпечення захисту інформації, вимоги щодо захисту якої встановлені законом у сфері надання платіжних, банківських та інших фінансових послуг (крім професійної діяльності на ринках капіталу та діяльності в системі накопичувального пенсійного забезпечення), державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, валютного регулювання та валютного нагляду, а також у системі депозитарного обліку Національного банку України".

У зв'язку з цим частину шосту вважати частиною восьмою;

5) у статті 13 "Прикінцеві положення":

назву викласти в такій редакції:

"Стаття 13. Прикінцеві та перехідні положення";

доповнити пунктом 1^1 такого змісту:

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

2. 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:

абзаци шостий і сьомий викласти в такій редакції:

"допуск до експлуатації – комплекс організаційно-технічних заходів щодо проведення тематичних досліджень засобів криптографічного захисту інформації, криптографічних алгоритмів, призначених для захисту службової інформації або інформації, що становить державну таємницю, та державної експертизи результатів таких досліджень з метою встановлення можливості використання відповідних засобів, алгоритмів за призначенням;

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

абзаци дев'ятий і десятий виключити;

абзац сімнадцятий викласти в такій редакції:

"тематичні дослідження – дослідження щодо встановлення відповідності засобів криптографічного захисту інформації, криптосистем, криптографічних алгоритмів, призначених 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";

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 або який спеціально розроблений для пошуку закладних пристроїв або контролю за ефективністю технічного захисту інформації";

"орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам – наукова (науково-дослідна, науково-технологічна, науково-технічна, науково-практична) установа або організація Державної служби спеціального зв'язку та захисту інформації України, до функцій якої належить 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 визначення поточного та/або цільового стану захищеності або перевірки їх відповідності вимогам законодавства щодо повноти запроваджених заходів захисту інформації чи 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 у сфері кібербезпеки";

"репозитарій інформації про кіберінциденти – електронна база даних, у якій накопичуються, зберігаються і систематизуються відомості про кіберінциденти у порядку, встановленому Державною службою спеціального зв'язку та захисту інформації України";

"спеціальна інформаційно-комунікаційна система – інформаційно-комунікаційна система, яка забезпечує обробку 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 досягнення оптимального ступеня впорядкованості 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 досягнення оптимального ступеня впорядкованості у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам";

"таксономія кіберінцидентів – схема понять та класифікації кіберінцидентів, призначена для застосування під час обміну, повідомлення, зберігання інформації та підготовки звітів про кіберінциденти";

2) частину першу статті 3 після абзацу дев'ятого доповнити новим абзацом такого змісту:

"здійснення стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам".

У зв'язку з цим абзац десятий вважати абзацом одинадцятим;

3) у частині першій статті 14:

у пункті 9 слова "засобів, комплексів та систем спеціального зв'язку" виключити;

пункти 13, 30 і 39 викласти в такій редакції:

"13) забезпечення функціонування державної системи урядового зв'язку, її безпеки, розвитку та готовності до роботи в особливий період і в разі виникнення надзвичайної ситуації";

"30) встановлення порядку організації та проведення державної експертизи у сфері криптографічного та технічного захисту інформації; забезпечення організації 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";

пункти 50, 67 і 72 викласти в такій редакції:

"50) встановлення:

технічних вимог до електронних комунікаційних мереж та об'єктів спеціального зв'язку;

порядку і забезпечення проведення експертизи інфраструктури електронних комунікацій проектів будівництва, реконструкції та модернізації електронних комунікаційних мереж, споруд спеціального зв'язку";

"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 криптографічного та технічного захисту інформації, кіберзахисту, електронних комунікацій та радіочастотного спектра";

доповнити пунктом 77^1 такого змісту:

"77^1) затвердження до використання 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 Міжнародної організації зі стандартизації (ISO), Європейського комітету зі стандартизації (CEN), Європейського інституту телекомунікаційних стандартів (ETSI), Міжнародного союзу електрозв'язку (ITU), Агентства Європейського Союзу з кібербезпеки (ENISA), Агентства з кібербезпеки та безпеки інфраструктури (CISA), Національного інституту стандартів та технологій (NIST), Організації Північноатлантичного договору (NATO), а також визнаних зазначеними організаціями процедур оцінки відповідності, у тому числі сертифікації, рекомендованої для застосування у сферах організації спеціального зв'язку, криптографічного та технічного 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, службова інформація та інформація, що становить державну таємницю, стану кіберзахисту об'єктів критичної інформаційної інфраструктури та об'єктів критичної інфраструктури";

пункт 91 виключити;

доповнити пунктами 96–115 такого змісту:

"96) встановлення вимог щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури.

Такі вимоги щодо запровадження заходів безпеки застосовуються до постачальників товарів, робіт, послуг лише в разі, якщо товари, роботи, послуги, які вони постачають, забезпечують функціонування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, 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 або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури рівня ризику, пов'язаного з критичністю таких товарів, робіт, послуг для забезпечення функціонування та заходів безпеки, що відповідають такому ризику; встановлює порядок підтвердження постачальниками товарів, робіт, послуг відповідності впроваджених заходів безпеки інформації встановленим вимогам відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт, послуг;

97) забезпечення реалізації та дотримання порядку пошуку та/або виявлення потенційних вразливостей в інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, та на об'єктах критичної інформаційної інфраструктури;

98) забезпечення організації та систематичного проведення консультацій (навчань) з питань захисту інформації та кіберзахисту та оцінювання стану кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи із захисту інформації або кіберзахисту в органах державної влади, державних органах, органах місцевого самоврядування, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, та в юридичних особах, які є власниками або розпорядниками об'єктів критичної інформаційної інфраструктури;

99) розроблення та забезпечення оновлення методичних рекомендацій щодо проведення інструктажів та тренінгів щодо кібергігієни на період призначення на посади державних службовців, працівників органів державної влади та державних органів, військовослужбовців, керівників та працівників державних підприємств, установ та організацій;

100) надання з урахуванням професійних стандартів методичних рекомендацій щодо типових вимог до підрозділів із кіберзахисту, загальних вимог до керівників із кіберзахисту в органах державної влади, державних органах, державних установах, організаціях, а також до осіб, які виконують функції та завдання керівників із кіберзахисту в юридичних особах щодо об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких вони є, та в органах місцевого самоврядування;

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

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

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

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

105) затвердження порядку ведення переліку авторизованих систем з безпеки, включення таких систем до переліку та виключення з нього, надання доступу до переліку та інформації з нього;

106) запровадження 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 органах, органах місцевого самоврядування, державних установах, організаціях та які рекомендуються до застосування на об'єктах критичної інфраструктури;

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

108) забезпечення функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;

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

110) забезпечення функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

111) забезпечення функціонування регіональних центрів кіберзахисту;

112) визначення для виконання завдання щодо функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози:

основних завдань, що можуть бути делеговані національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA галузевим та регіональним командам реагування на кіберінциденти, кібератаки, кіберзагрози, та порядку взаємодії команд реагування з CERT-UA;

вимог до організаційно-технічної спроможності, до сервісу, пов'язаного з реагуванням на кіберінциденти національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози, а також інших команд реагування в частині виконання ними завдань галузевої або регіональної команди реагування або в частині надання ними сервісу, пов'язаного з реагуванням на кіберінциденти, органам державної влади, державним органам, органам місцевого самоврядування, операторам критичної інфраструктури, власникам або розпорядникам об'єктів критичної інформаційної інфраструктури;

порядку ведення репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій;

порядку здійснення моніторингу за діяльністю національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози, а також інших команд реагування в частині виконання ними завдань галузевої або регіональної команди реагування або в частині надання ними сервісу, пов'язаного з реагуванням на кіберінциденти, органам державної влади, державним органам, органам місцевого самоврядування, операторам критичної інфраструктури, власникам або розпорядникам об'єктів критичної інформаційної інфраструктури, зокрема щодо додержання вимог закону в частині функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози відповідно до сфери їхніх повноважень та надання вимог про усунення порушень;

порядку здійснення заходів реагування у кризовій ситуації в кіберпросторі;

підстав для надання на основі отриманої від CERT-UA інформації вимог про реагування власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація,

що становить державну таємницю, об'єктів критичної інформаційної інфраструктури, операторам критичної інфраструктури, а також визначення строків та порядку реалізації визначених відповідною вимогою про реагування заходів реагування та подання звіту про їх виконання;

113) встановлення для виконання завдання щодо функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози:

порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, форм повідомлення, національної таксономії кіберінцидентів;

критеріїв визначення значного кіберінциденту, у тому числі для цілей виконання зобов'язань, визначених законодавством про здійснення повідомлень про кіберінциденти;

114) запровадження організаційно-технічних заходів щодо створення національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

115) забезпечення функціонування платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та встановлення порядку приєднання до такої платформи";

4) у частині першій статті 15:

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 кіберінциденти, кібератаки, кіберзагрози, національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, щодо виконання вимог законодавства за результатами моніторингу в порядку, визначеному законодавством щодо діяльності команд реагування на кіберінциденти, кібератаки, кіберзагрози;

1^2) у визначених законодавством випадках вживати заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози шляхом надання обов'язкових до виконання вимог про реагування власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, та власникам або розпорядникам об'єктів критичної інформаційної інфраструктури.

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

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

пункт 22 після слів "ключових документів" доповнити словами "та державних шифрів".

3. У частині другій статті 2 Закону України "Про стандартизацію" (Відомості Верховної Ради України, 2014 р., № 31, ст. 1058; 2019 р., № 29, ст. 117; 2023 р., № 14, ст. 37) слова "військові стандарти, стандарти медичної допомоги" замінити словами "військові стандарти, стандарти криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, стандарти медичної допомоги".

4. 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:

пункти 7 і 19 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, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки";

"19) об'єкт критичної інформаційної інфраструктури – інформаційна, електронна комунікаційна, інформаційно-комунікаційна або технологічна система, яка необхідна для стійкого та безперервного функціонування об'єкта критичної інфраструктури, істотно впливає на безперервність та стійкість процесу надання життєво важливих функцій та/або послуг та відсутній альтернативний об'єкт (спосіб) їх надання";

доповнити пунктами 24 і 25 такого змісту:

"24) кризова ситуація у сфері кібербезпеки – порушення або загроза порушення режиму функціонування інформаційних, електронних комунікаційних та/або 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 кіберінцидентом, кібератакою або кіберзагрозою, порушення функціонування яких може призвести до значних негативних наслідків для національної безпеки;

25) реагування на кіберінциденти – структурована сукупність дій, спрямованих на підготовку до кіберінцидентів, їх виявлення та аналіз, мінімізацію шкоди від кіберінциденту та запобігання їх повторенню 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 службова інформація та інформація, що становить державну таємницю, 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 затверджується 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 загальний контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, загальну координацію суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози; подає до Ради національної безпеки і оборони України пропозиції щодо оголошення кризової ситуації в кібербезпеці; координує реалізацію Стратегії кібербезпеки України, подає до Ради національної безпеки і оборони України пропозиції щодо формування та уточнення Стратегії, у тому числі з урахуванням положень Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2 Directive); визначає пріоритети, розробляє концептуальні засади та вносить Президентові України пропозиції щодо проведення кібероперацій стратегічного рівня в інтересах національної безпеки і оборони та забезпечує координацію суб'єктів сектору безпеки і оборони щодо їх проведення; координує стратегічні комунікації у сфері кібербезпеки.

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; затверджує порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (крім систем та об'єктів банків); встановлює порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, з правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності";

пункт 7 частини четвертої викласти в такій редакції:

"7) оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури";

5) доповнити статтею 5^1 такого змісту:

"Стаття 5^1. Підрозділи з кіберзахисту, керівники з 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 службова інформація та інформація, що становить державну таємницю, утворюються підрозділи з кіберзахисту та призначаються керівники з кіберзахисту, яким безпосередньо підпорядковуються такі підрозділи, а в органах місцевого самоврядування – особи, які виконують їхні функції та завдання.

Власники або розпорядники об'єктів критичної інформаційної інфраструктури призначають відповідальну особу, яка виконує функції та завдання керівника з кіберзахисту, та у разі потреби з метою забезпечення виконання вимог з кіберзахисту утворюють підрозділ з кіберзахисту.

Призначення керівника з кіберзахисту на посаду в органі державної влади здійснюється у порядку, затвердженому Кабінетом Міністрів України, за погодженням Державної служби спеціального зв'язку та захисту інформації України після перевірки, проведеної Службою безпеки України в межах її повноважень.

У разі ненадання Державною службою спеціального зв'язку та захисту інформації України протягом одного календарного місяця з дня отримання нею звернення вмотивованої відмови у погодженні призначення керівника

з кіберзахисту із зазначенням підстави, визначеної відповідним порядком, таке погодження вважається наданим.

2. Керівники з кіберзахисту або відповідальні особи, які виконують функції та завдання керівника з 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 службова інформація та інформація, що становить державну таємницю, у тому числі в разі введення воєнного стану.

3. Методичні рекомендації щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту в органах державної влади, а також до відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органах місцевого самоврядування, надаються Державною службою спеціального зв'язку та захисту інформації України";

6) статтю 6 викласти в такій редакції:

"Стаття 6. Кіберзахист критичної інфраструктури

1. Посадові особи операторів критичної інфраструктури, власників або розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечувати дотримання вимог з кіберзахисту, повідомляти в установленому порядку про кіберінциденти, кібератаки, кіберзагрози, 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 об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури проводиться добровільно або у випадках, визначених законодавством, обов'язково з урахуванням методичних рекомендацій щодо оцінювання стану кіберзахисту, загальних вимог до суб'єктів оцінювання стану кіберзахисту (крім оцінювання стану кіберзахисту щодо об'єктів критичної інфраструктури або 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 та 6 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, 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, активної протидії агресії в кіберпросторі, кіберзахисту критичної інфраструктури, здійснює державний контроль у зазначених сферах; здійснює стандартизацію у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам; забезпечує створення та функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, національної системи обміну інформацією про кіберінциденти, 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 кіберінциденти, кібератаки, кіберзагрози CERT-UA (національний CSIRT); 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 або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, та в юридичних особах, які є власниками або 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 службова інформація та інформація, що становить державну таємницю, 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, кримінальних правопорушень проти об'єктів критичної інформаційної інфраструктури; здійснює заходи з інформування громадян про безпеку в кіберпросторі;

3) Служба безпеки України відповідно до закону здійснює заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки України, миру і безпеки людства, а також кримінальних правопорушень терористичної спрямованості, що вчиняються у кіберпросторі або з його використанням; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом, кібердиверсіями та кібершпигунством; координує діяльність суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям; 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, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки";

"6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює Центр кіберзахисту Національного банку України (включаючи команду реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT-NBU), забезпечує функціонування системи кіберзахисту для 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; забезпечує функціонування системи оцінювання стану кіберзахисту в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг; встановлює вимоги до проведення аудиту інформаційної безпеки в банках, інших особах, 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";

доповнити пунктом 7 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 розвиток спроможностей національної системи кібербезпеки; забезпечує координацію

діяльності щодо співпраці з міжнародними партнерами для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці; забезпечує активну участь України в діяльності міжнародних організацій 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 і переслідувати кіберзлочинність та реагувати на кіберзагрози; координує процес 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";

у частині третій:

пункти 1 і 2 викласти в такій редакції:

"1) формування та 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) запровадження нормативно-правового регулювання у сфері кібербезпеки, кіберзахисту з урахуванням ризик-орієнтованого підходу, чіткого розподілу ролей, завдань, функцій та відповідальності публічного сектору, операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури, а також галузевої специфіки, гармонізації практик та стандартів з Європейським Союзом та НАТО";

пункт 3 виключити;

пункти 4–8 викласти в такій редакції:

"4) запровадження заходів стимулювання розвитку та конкурентоспроможності індустрії послуг та продуктів у сфері кібербезпеки в Україні;

5) залучення експертного потенціалу приватного сектору, наукових установ, професійних та громадських об'єднань до розроблення проектів щодо стратегічного планування, державної політики, проектів нормативно-правових актів, нормативних документів, стандартів та методичних рекомендацій у сфері кібербезпеки;

6) систематичного проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи з кіберзахисту в органах державної влади, органах місцевого самоврядування, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить

державну таємницю, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури;

7) функціонування системи оцінювання стану кіберзахисту в органах державної влади, державних органах, органах місцевого самоврядування, державних підприємствах, господарських товариствах, 50 і більше відсотків акцій (часток) яких належать державі, державних наукових установах та закладах вищої освіти, щодо об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури;

8) розвитку мережі команд реагування на кіберінциденти, кіберзагрози на національному, галузевому та регіональному рівнях, у тому числі із залученням приватних команд реагування";

пункт 10 виключити;

пункти 12, 15 і 17 викласти в такій редакції:

"12) функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози";

"15) впровадження організаційно-технічної моделі кіберзахисту національної системи кібербезпеки";

"17) застосування інструментів та механізмів державно-приватної взаємодії для виконання завдань у сфері кібербезпеки, включаючи, але не обмежуючись, функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, заходи кіберзахисту та захисту інформації; запровадження загальної системи або індивідуальних програм моніторингу, аналізу, координації дій, у тому числі під час реагування на кіберінциденти; усунення наслідків, здійснення заходів з відновлення; організації та здійснення заходів з підготовки кадрів, підвищення рівня знань і навичок, проведення навчань, розроблення та реалізації освітніх і просвітницьких програм; здійснення досліджень та нових розробок; забезпечення функціонування центрів кібербезпеки та їхніх сервісів; розроблення програмних документів та нормативно-правових актів у сфері кібербезпеки, а також для вирішення інших завдань у сфері кібербезпеки, що можуть бути вирішені шляхом державно-приватної взаємодії";

доповнити пунктами 26 і 27 такого змісту:

"26) планування витрат та фінансування органами державної влади, державними органами, органами місцевого самоврядування, операторами критичної інфраструктури, власниками або розпорядниками об'єктів критичної інформаційної інфраструктури заходів кіберзахисту, передбачених законодавством;

27) проведення інструктажів та систематичних тренінгів щодо кібергігієни для членів уряду України, народних депутатів України, працівників патронатних служб, депутатів місцевих рад, державних службовців, військовослужбовців,

працівників органів державної влади та державних органів, керівників та працівників державних підприємств, установ та організацій, систематичність та порядок проведення яких встановлюються Кабінетом Міністрів України";

частину п'яту викласти в такій редакції:

"5. Впровадження організаційно-технічної моделі кіберзахисту як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення, функціонування та розвиток:

1) системи захищеного доступу державних органів до мережі Інтернет;

2) Національного центру резервування державних інформаційних ресурсів;

3) Центру антивірусного захисту інформації;

4) системи виявлення вразливостей, а також здійснення для органів державної влади, державних органів, органів місцевого самоврядування, власників або розпорядників критичної інформаційної інфраструктури, операторів критичної інфраструктури моніторингу мереж, сканування мережевих, інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем з метою виявлення вразливостей, які можуть мати значний вплив;

5) системи реагування на кіберінциденти, кібератаки, кіберзагрози щодо об'єктів кіберзахисту.

Державний центр кіберзахисту проводить систематичні навчання з питань кіберзахисту, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань; проводить оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів державної влади, державних органів, органів місцевого самоврядування, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури";

пункт 4 частини шостої виключити;

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 здійснюються відповідно до порядку пошуку та/або виявлення потенційних вразливостей, встановленого Кабінетом Міністрів України.

Складовою 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 мають бути порядок розроблення та проведення програм пошуку і виявлення вразливостей за винагороду та порядок узгодженого розкриття вразливостей";

8) статтю 9 викласти в такій редакції:

"Стаття 9. Національна система реагування на кіберінциденти, кібератаки, кіберзагрози

1. В Україні створюється та забезпечується функціонування національної системи реагування на кіберінциденти, 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 забезпечує функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, є Державна служба спеціального зв'язку та захисту інформації України.

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

1) CERT-UA – національна команда реагування на кіберінциденти, 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 кіберінциденти, кібератаки, кіберзагрози на національному, галузевому, регіональному рівнях, динамічний аналіз ризиків та ситуаційної обізнаності;

отримання та опрацювання у встановленому порядку обов'язкових та інших повідомлень про кіберінциденти, здійснених у межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози відповідно до цього Закону, надання рекомендацій щодо можливих заходів реагування та технічної підтримки (у разі потреби);

здійснення у встановленому порядку заходів щодо надання попереджень про кіберзагрози, сповіщень, оголошень та інформування щодо кіберінцидентів, кібератак, кіберзагроз та вразливостей органів державної влади, державних органів, органів місцевого самоврядування, операторів критичної інфраструктури, власників та розпорядників критичної інформаційної інфраструктури у режимі, за можливості, наближеному до реального часу;

надання у встановленому порядку сервісу у зв'язку з реагуванням, рекомендацій з реагування на кіберінциденти, кібератаки, кіберзагрози власникам або 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, власникам або розпорядникам критичної інформаційної інфраструктури, іншим суб'єктам (у разі потреби);

виконання функції координатора з метою узгодженого розкриття вразливостей;

інформування у встановленому законодавством порядку Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України про кіберінциденти, кібератаки, кіберзагрози, виявлені або потенційні вразливості інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також об'єктів критичної інформаційної інфраструктури із зазначенням обов'язкових та/або рекомендованих заходів реагування для видання вимоги про реагування;

проведення аналізу ризиків у зв'язку з кіберінцидентом, кібератакою, кіберзагрозою та надання відповідних рекомендацій;

забезпечення у встановленому порядку функціонування репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій;

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

взаємодія у встановленому порядку із суб'єктами національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

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 2 Directive);

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

взаємодія у встановленому порядку із суб'єктами приватного сектору, у тому числі з іноземними суб'єктами господарювання, з питань реагування на кіберінциденти, кібератаки, кіберзагрози.

Порядок взаємодії національної команди реагування на кіберінциденти, кібератаки, кіберзагрози з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності затверджується Кабінетом Міністрів України;

2) галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (далі – галузеві, регіональні CSIRT) – створюються органами державної влади або органами місцевого самоврядування з метою посилення спроможності національної системи реагування на кіберінциденти, 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 правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності, іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України.

Альтернативою створення органами державної влади або органами місцевого самоврядування власних галузевих, регіональних CSIRT є залучення послуг приватних команд реагування, що можуть виконувати у повному обсязі або частково завдання галузевого, регіонального CSIRT відповідно до цього Закону та за умови дотримання ними встановлених законодавством вимог до таких галузевих, регіональних CSIRT.

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

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

отримання та опрацювання у встановленому порядку обов'язкових та інших повідомлень про кіберінциденти у відповідній галузі або відповідному регіоні, отриманих у межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози згідно з цим Законом, надання рекомендацій щодо можливих заходів реагування та технічної підтримки (у разі потреби);

здійснення у встановленому порядку заходів щодо надання попереджень про кіберзагрози, сповіщень, оголошень та інформування щодо кіберінцидентів, кібератак, кіберзагроз та вразливостей у відповідній галузі або відповідному регіоні у режимі, за можливості, наближеному до реального часу;

надання у встановленому порядку сервісу у зв'язку з реагуванням, рекомендацій з реагування на кіберінциденти, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні.

Галузеві, регіональні CSIRT або приватні команди реагування, що виконують їхні завдання, здійснюють у встановленому законодавством порядку обмін інформацією з іншими суб'єктами національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, координують свою діяльність та інформують CERT-UA і Ситуаційний центр забезпечення кібербезпеки Служби безпеки України про відповідні заходи реагування.

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

Команда реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT-NBU, що входить до складу Центру кіберзахисту Національного банку України, є галузевим CSIRT та діє у складі національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та національної системи реагування на кіберінциденти, 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 про кіберінциденти, кібератаки, кіберзагрози та національної системи реагування на кіберінциденти, 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 кіберінциденти, кібератаки, кіберзагрози з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України, з урахуванням вимог цього Закону та в межах повноважень, визначених законом.

Служба безпеки України забезпечує функціонування Ситуаційного центру забезпечення кібербезпеки Служби безпеки України та регіональних центрів забезпечення кібербезпеки регіональних органів Служби безпеки України для виконання завдань щодо протидії шпигунству, тероризму, диверсіям та в межах повноважень, визначених законом, протидії іншим кіберзагрозам у сфері державної безпеки;

4) приватні команди реагування – можуть залучатися для надання операторам критичної інфраструктури, власникам або розпорядникам критичної інформаційної інфраструктури, органам державної влади та органам місцевого самоврядування окремих послуг, пов'язаних з реагуванням на кіберінциденти, виконання окремих завдань галузевих, регіональних CSIRT, а також взаємодіяти з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, у тому числі щодо обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, за умови організаційно-технічної спроможності та в порядку, встановленому Державною службою спеціального зв'язку та захисту інформації України.

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

Державна служба спеціального зв'язку та захисту інформації України та Служба безпеки України з метою вжиття заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози в межах своїх повноважень можуть надавати обов'язкові до виконання вимоги про реагування власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури, операторам критичної інфраструктури.

Таке оперативне реагування шляхом надання вимоги про реагування на кіберінциденти, кібератаки, кіберзагрози є актом організаційно-розпорядчого характеру, не є заходом державного контролю за технічним захистом інформації та кіберзахистом та здійснюється з метою запобігання або мінімізації негативних наслідків у зв'язку з кіберінцидентом, кібератакою або кіберзагрозою.

Власники або розпорядники інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, оператори критичної інфраструктури, власники або розпорядники об'єктів критичної інформаційної інфраструктури зобов'язані вжити визначених вимогою про реагування на кіберінциденти, кібератаки, кіберзагрози заходів та подати звіт про результати вжитих заходів у строки та порядку, встановлені Державною службою спеціального зв'язку та захисту інформації України.

Підстави для надання вимоги про реагування на кіберінциденти, кібератаки, кіберзагрози, строки та порядок подання звіту про результати вжитих заходів встановлюються Державною службою спеціального зв'язку та захисту інформації України;

5) Національний координаційний центр кібербезпеки – здійснює загальну координацію функціонування суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.

Суб'єкти національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, крім приватних компаній, що не здійснюють функцій галузевих, регіональних CSIRT, забезпечують у порядку, визначеному для функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, невідкладне інформування Національного координаційного центру кібербезпеки про всі значні кіберінциденти, кібератаки.

Для забезпечення скоординованого, оперативного та ефективного реагування на кризову ситуацію у зв'язку з кіберінцидентом, кібератакою, кіберзагрозою у складі Національного координаційного центру кібербезпеки утворюється та функціонує постійно діюча Об'єднана група реагування на кіберінциденти, кібератаки, кіберзагрози, до складу якої входять представники Національного координаційного центру кібербезпеки, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України та представники інших основних суб'єктів національної системи кібербезпеки (за обґрунтованої необхідності).

Керівником Об'єднаної групи реагування на кіберінциденти, кібератаки, кіберзагрози, який затверджує її персональний склад та порядок роботи з урахуванням визначених законом компетенції та повноважень її учасників, є заступник керівника Національного координаційного центру кібербезпеки";

9) доповнити статтею 9^1 такого змісту:

"Стаття 9^1. Національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози

1. В Україні створюється та забезпечується функціонування національної системи обміну інформацією про кіберінциденти, 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 забезпечує функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, є Державна служба спеціального зв'язку та захисту інформації України (далі – Уповноважений орган).

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

3. Власники або розпорядники інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, зобов'язані в порядку, визначеному Уповноваженим органом для функціонування національної системи обміну інформацією про кіберінциденти, кіберзагрози, кібератаки, повідомляти відповідний CSIRT про всі кіберінциденти.

Власники або розпорядники об'єктів критичної інформаційної інфраструктури зобов'язані в порядку, визначеному Уповноваженим органом для функціонування національної системи обміну інформацією про кіберінциденти, кіберзагрози, кібератаки, повідомляти відповідний CSIRT про всі значні кіберінциденти.

Органи державної влади, державні органи, органи місцевого самоврядування, які не є власниками або розпорядниками критичної інформаційної інфраструктури та отримали інформацію про кіберінцидент щодо критичної інформаційної інфраструктури, зобов'язані в порядку, визначеному Уповноваженим органом для функціонування національної системи обміну інформацією про кіберінциденти, кіберзагрози, кібератаки, повідомляти відповідний CSIRT про такі кіберінциденти.

Встановлення законом для суб'єктів, що здійснюють обробку інших категорій інформації з обмеженим доступом, зобов'язань щодо надання обов'язкових повідомлень про кіберінциденти, кібератаки є підставою для приєднання у встановленому порядку до національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози згідно з цим Законом.

Суб'єкти, для яких законом не встановлені зобов'язання щодо надання обов'язкових повідомлень про кіберінциденти, кібератаки, мають право приєднатися до національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та здійснювати добровільний обмін відповідною інформацією згідно із національною таксономією кіберінцидентів у порядку, визначеному Уповноваженим органом.

4. Усі обов'язкові повідомлення про кіберінциденти, кібератаки, кіберзагрози подаються суб'єктами, визначеними цією статтею, у строки та порядку, встановлені Уповноваженим органом.

5. Уповноважений орган визначає критерії значного кіберінциденту для цілей надання операторами критичної інфраструктури, власниками або розпорядниками критичної інформаційної інфраструктури обов'язкових повідомлень про кіберінциденти, кібератаки, а також для цілей інформування Національного координаційного центру кібербезпеки командами реагування згідно з цим Законом.

6. Посадові особи власників або розпорядників інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, посадові особи операторів критичної інфраструктури, власників або розпорядників об'єктів критичної інформаційної інфраструктури несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов'язку щодо здійснення обов'язкових повідомлень про кіберінциденти, кібератаки.

7. Інформація про кіберінцидент, кібератаку щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури та про їхні наслідки є відкритою інформацією, крім інформації про характер, технічні характеристики, інші деталі кіберінциденту, кібератаки, що віднесена до інформації з обмеженим доступом.

Критерії віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки до інформації з обмеженим доступом, перелік підстав, порядок та мета розкриття такої інформації, у тому числі службової інформації для обміну в межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, порядок публічного інформування або звітування про реагування на кіберінциденти, кібератаки, порядок усунення їх наслідків затверджуються Кабінетом Міністрів України.

Інформація, одержана національним, галузевим, регіональним CSIRT або приватною командою реагування, що виконує завдання галузевих, регіональних CSIRT відповідно до цього Закону, використовується ними виключно в цілях та в порядку, що визначаються законодавством щодо функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та забезпечують належні умови обробки та захисту одержаної інформації";

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 законодавства.

Порядок здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту встановлюється Кабінетом Міністрів України".

5. Частину першу статті 11 Закону України "Про публічні електронні реєстри" (Відомості Верховної Ради України, 2023 р., № 11, ст. 27) доповнити пунктом 6^1 такого змісту:

"6^1) організаційно забезпечує створення, модернізацію, модифікацію, розвиток програмного забезпечення Платформи, здійснення заходів, необхідних для його адміністрування та забезпечення функціонування, можливість використання програмного забезпечення Платформи для створення, ведення та адміністрування реєстрів у порядку, встановленому Кабінетом Міністрів України".

ІІ. Прикінцеві положення

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування, крім підпункту 5 пункту 4 розділу І цього Закону, який набирає чинності через шість місяців з дня його опублікування.

2. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:

забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону;

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

3. Кабінету Міністрів України у 2025 році поінформувати Верховну Раду України про стан виконання цього Закону.

Президент України В. ЗЕЛЕНСЬКИЙ

м. Київ
27 березня 2025 року
№ 4336–IX