Порівняльна таблиця до проекту Закону України **Реєстраційний № 11290**

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

Автор(и): Голова Комітету Верховної Ради України Завітневич О. М. **(Повторне друге)**

Автори остаточної редакції: Народні депутати України - члени Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки

Дата розгляду в комітеті: 25.03.2025

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
1	Проект			Проект
	З А К О Н У К Р А Ї Н И			**З А К О Н У К Р А Ї Н И**
2	**Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури**			**Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури**
3	Верховна Рада України п о с т а н о в л я є:			Верховна Рада України п о с т а н о в л я є:
4	І. Внести зміни до таких законів України:			І. Внести зміни до таких законів України:
5		**-1- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** 1. Розділ І після абзацу першого доповнити новим абзацом такого змісту: «1. Внести до Кримінального кодексу України (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131) такі зміни: 1) у статті 359: абзац другий частини першої викласти у наступній редакції: «караються штрафом від двохсот п’ятдесяти до тисячі двохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк»;	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		абзац другий частини другої викласти у наступній редакції: «караються позбавленням волі на строк від п’яти до восьми років»; абзац другий частини третьої викласти у наступній редакції: «караються позбавленням волі на строк від восьми до десяти років»; 2) у статті 360: абзац другий частини першої викласти у наступній редакції: «караються штрафом від двох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до ста двадцяти годин, або обмеженням волі на строк від одного до трьох років, або пробаційним наглядом на строк до двох років, або обмеженням волі на той самий строк»; абзац другий частини другої викласти у наступній редакції: «караються штрафом від чотирьох тисяч до дванадцяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до п’яти років»; абзац другий частини третьої викласти у наступній редакції: «караються штрафом від двадцяти тисяч до двадцяти п’яти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від шести до восьми років»; 3) у статті 361: абзац другий частини першої викласти у наступній редакції: «карається штрафом від двох тисяч до пяти тисяч неоподатковуваних мінімумів доходів громадян або пробаційним наглядом на строк до трьох років, або обмеженням волі на той самий строк»; абзац другий частини другої викласти у наступній редакції:		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«караються штрафом від п’яти тисяч до восьми тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк»; абзац другий частини третьої викласти у наступній редакції: «караються штрафом від в восьми тисяч до дванадцяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого»; абзац другий частини четвертої викласти у наступній редакції: «караються позбавленням волі на строк від дев’яти до тринадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого»; абзац другий частини п’ятої викласти у наступній редакції: «караються позбавленням волі на строк від десяти до п’ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до п’яти років»; 4) у статті 361^1: абзац другий частини першої викласти у наступній редакції: «караються штрафом від трьох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років»; абзац другий частини другої викласти у наступній редакції: «караються позбавленням волі на строк до шести років»; 5) у статті 361^2: абзац другий частини першої викласти у наступній редакції:		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«караються штрафом від трьох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років»; абзац другий частини другої викласти у наступній редакції: «караються позбавленням волі на строк від трьох до п'яти років»; 5) у статті 362: абзац другий частини першої викласти у наступній редакції: «караються штрафом від трьох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років»; абзац другий частини другої викласти у наступній редакції: «караються позбавленням волі на строк до чотирьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк»; абзац другий частини третьої викласти у наступній редакції: «караються позбавленням волі на строк від чотирьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років»; 6) у статті 363: абзац третій викласти у наступній редакції: «караються штрафом від трьох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або пробаційним наглядом на строк до трьох років, або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк»; 6) у статті 363^1: абзац другий частини першої викласти у наступній редакції: «карається штрафом від трьох тисяч до п’яти тисяч неоподатковуваних мінімумів		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		доходів громадян або обмеженням волі на строк до трьох років»; абзац другий частини другої викласти у наступній редакції: «караються обмеженням волі на строк до шести років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років».		
6	1. У Законі України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України, 2005 р., № 26, ст. 347 із наступними змінами):	**-2- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Частину 1 вважати частиною 2	Відхилено	1. У Законі України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України, 2005 р., № 26, ст. 347 із наступними змінами):
		-3- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Бобровська С. А. (р.к. №217), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Чернєв Є. В. (р.к. №26)	Відхилено	
		1. Пункт 1 Розділу І проекту Закону викласти в такій редакції: «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»;	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«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 їх окремі компоненти, 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»;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено 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 із застосуванням комплексної системи захисту інформації або шляхом авторизації з безпеки, або шляхом отримання сертифіката 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 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. Авторизація з безпеки та процедура отримання сертифіката відповідності		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		стандарту інформаційної безпеки не застосовуються до систем, в яких обробляється інформація, що становить державну таємницю. Підтвердження відповідності комплексної системи захисту інформації забезпечується власником або розпорядником системи в порядку, встановленому Кабінетом Міністрів України. Підтвердження відповідності стандарту інформаційної безпеки 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 національний орган України з акредитації та 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 з безпеки здійснюється в порядку, встановленому Кабінетом Міністрів України. Авторизація з безпеки або отримання сертифіката відповідності стандарту інформаційної безпеки щодо систем, в яких обробляються державні інформаційні ресурси або службова інформація, 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації або документ про відповідність, 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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, до складу комплексної системи захисту інформації якої входить комплекс 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 в системах у сфері надання банківських, інших фінансових та платіжних послуг, інформації з обмеженим доступом, що є складовою системи депозитарного обліку 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг. Власники або розпорядники систем, об'єктів критичної 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 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 банківських, інших фінансових послуг, крім професійної діяльності на ринках капіталу та діяльності в системі накопичувального пенсійного забезпечення, та платіжних 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, що 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.		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 банківських, інших фінансових послуг, крім професійної діяльності на ринках капіталу та діяльності в системі накопичувального пенсійного забезпечення, та платіжних послуг, у системах Національного банку України, включаючи системи депозитарного обліку 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». 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)».		
		-4- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д.	Враховано	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Касай Г. О. (р.к. №280), Н.д. Ковальов О. І. (р.к. №262), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Хоменко О. В. (р.к. №68), Н.д. Чернєв Є. В. (р.к. №26) Пункт 1 розділу І проекту Закону викласти в такій редакції: «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»;	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 їх 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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**		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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** здійснюється 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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**		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, що 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 в системі депозитарного обліку Національного банку України».** У зв'язку з цим частину шосту вважати частиною восьмою;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		5) у статті 13 «Прикінцеві положення»: назву викласти в такій редакції: «Стаття 13. Прикінцеві та перехідні положення»; доповнити пунктом 1^1 такого змісту: «11. 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)».		
7	1) у частині першій статті 1:			1) у частині першій статті 1:
8	абзаци третій, сьомий та п'ятнадцятий викласти в такій редакції:			абзаци третій, сьомий і п'ятнадцятий викласти в такій редакції:
9	«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»;			«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»;
10	«захист інформації в системі – діяльність, спрямована на запобігання витоку інформації, що обробляється в системі чи пристроєм обробки інформації»;	**-5- Н.д. Пузійчук А. В. (р.к. №182)** Абзац четвертий підпункту 1 пункту 1 розділу I викласти в такій редакції: «захист інформації в системі - діяльність, спрямована на запобігання витоку інформації, що обробляється в системі чи пристроєм обробки інформації та несанкціонованим діям щодо такої інформації;».	Відхилено	«захист інформації в системі – діяльність, спрямована на запобігання порушенню цілісності, конфіденційності і доступності інформації в системі»;
		-6- Н.д. Мокан В. І. (р.к. №99) В абзаці сьомому частини першої статті 1 Закону в редакції законопроєкту після слів "пристроєм обробки інформації" додати розділовий знак і слова: ", запобігання несанкціонованій зміні даних у відповідних	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		системах та порушення їх цілісності зі сторони авторизованих користувачів". ***Обґрунтування.*** Як вказує ГНЕУ, запропоновані зміни в редакції до 1 читання звужуватимуть сферу такої діяльності лише до запобігання доступу до відповідної інформації особами, що не мають права доступу до неї. При цьому, поза увагою захисної діяльності залишатимуться випадки несанкціонованої зміни даних у відповідних системах та порушення їх цілісності зі сторони авторизованих користувачів.		
		-7- Н.д. Мамка Г. М. (р.к. №147), Н.д. Макаренко М. В. (р.к. №153), Н.д. Борт В. П. (р.к. №152), Н.д. Ларін С. М. (р.к. №132), Н.д. Чорний В. І. (р.к. №151), Н.д. Іоффе Ю. Я. (р.к. №136), Н.д. Німченко В. І. (р.к. №130)	Відхилено	
		захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;		
		-8- Н.д. Штепа С. С. (р.к. №283)	Відхилено	
		Абзац четвертий підпункту 1 пункту 1 розділу І законопроєкту викласти у такій редакції: “захист інформації в системі або на об’єкті інформаційної діяльності – діяльність, спрямована на забезпечення конфіденційності, цілісності та доступності інформації та/або запобігання витоку інформації, що обробляється в системі чи на об’єкті інформаційної діяльності;”.		
		-9- Н.д. Федієнко О. П. (р.к. №89)	Відхилено	
		захист інформації в системі – діяльність, спрямована на запобігання **випадків витоку, несанкціонованого доступу, порушення цілісності, конфіденційності і доступності інформації в системі;**		
		-10- Н.д. Бурміч А. П. (р.к. №144)	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Абзац четвертий пункту 1 частини першої розділу I законопроекту викласти у такій редакції: «захист інформації в системі – діяльність, спрямована на запобігання витоку інформації, що обробляється в системі чи пристроєм обробки інформації, та на запобігання незаконній обробці інформації в системі;»		
		-11- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)	Відхилено	
		Абзац четвертий підпункту 1) пункту 1 Розділу I викласти в такій редакції: «захист інформації в системі – діяльність, спрямована на запобігання несанкціонованого доступу, втручанню в процеси обробки, зміни, знищення чи витоку інформації, що обробляється в системі чи пристроєм обробки інформації, а також будь-яких інших дія, спрямованим на нанесення шкоди даним чи середовищу, в якому вони обробляються;»		
		-12- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Абзац четвертий підпункту 1 пункту 1 розділу I проекту Закону викласти в такій редакції: «захист інформації в системі – діяльність, спрямована на запобігання порушення цілісності, конфіденційності і доступності інформації в системі»	Народні депутати України - члени Комітету	
11	«обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які 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»;			«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»;
12	доповнити з урахуванням алфавітного порядку термінами такого змісту:			доповнити з урахуванням алфавітного порядку термінами такого змісту:
13	«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, що приймається у встановленому законодавством порядку»;	**-13- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	«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»;
		авторизація системи з безпеки – рішення щодо можливості функціонування (експлуатації) **системи безпеки інформації** 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, що приймається у встановленому законодавством порядку;		
		-14- Н.д. Цимбалюк М. М. (р.к. №176)	Відхилено	
		Не зрозуміло використання у зазначеному законопроєкті терміну «електронно комунікаційна система», який наразі відсутній у законах України. Наприклад, в Законі України «Про електронні комунікації» присутній лише термін «електронна комунікаційна мережа».		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
14	«авторизована система з безпеки – інформаційна, інформаційно-комунікаційна, електронно 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»;	**-15- Н.д. Федієнко О. П. (р.к. №89)** авторизована **системи безпеки інформації** – інформаційна, інформаційно-комунікаційна, електронно 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;	Відхилено	«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»;
15	«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»;	**-16- Н.д. Пузійчук А. В. (р.к. №182)** Абзац дев'ятий підпункту 1 пункту 1 розділу I після слів «захисту інформації від» доповнити словами «несанкціонованих дій та». **-17- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163)** У частині 1 статті 1, з урахуванням алфавітного порядку, викласти абзац в наступній редакції: «комплекс технічного захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів технічного захисту інформації, призначених для захисту інформації від витоку втручань та інших порушень цілісності та конфіденційності даних за допомогою технічних каналів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» Обгрунтування: В пропонованій редакції до повторного другого читання комплекс технічного захисту інформації концентрується лише на захисті від витоків, тоді як основну небезпеку становлять не безпосередні витоки даних, а віддалена та/чи несанкціонована маніпуляція даними. В той же час в цій же статті визначення захисту	Відхилено Відхилено	«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»;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		інформації включає в себе запобігання порушення цілісності та конфіденційності даних (фактично врахована поправка від Ю. Тимошенко, №10). Необхідно скоригувати даний термін так, щоб він відповідав визначенню захисту.		
16	«пристрої обробки інформації – технічні пристрої (засоби) обробки інформації, в яких технічно неможлива реалізація програмних процедур розмежування доступу користувачів та інших функціональних послуг безпеки»;			«пристрої обробки інформації – технічні пристрої (засоби) обробки інформації, в яких технічно неможливо реалізувати програмні процедури розмежування доступу користувачів та інші функціональні послуги безпеки»;
17		**-18- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)** Доповнити підпункт 1) пункту 1 Розділу І абзацом одинадцятим в такій редакції: «пристрої обробки інформації жорсткої архітектури – технічні пристрої (засоби) обробки інформації, в яких технічно неможлива реалізація програмних процедур розмежування доступу користувачів та інших функціональних послуг безпеки;».	Відхилено	
18	«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			«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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»;			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»;
19	«технічний канал витоку інформації – взаємопов'язана сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки, спрямовані на забезпечення витоку інформації»;	**-19- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163)** «технічний канал витоку інформації – взаємопов'язана сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки, спрямовані на забезпечення витоку інформації» У частині 1 статті 1, з урахуванням алфавітного порядку, викласти абзац в наступній редакції: «технічний канал витоку інформації – взаємопов'язана сукупність джерела небезпечного сигналу або з'єднання, середовища його поширення та програмно-апаратних засобів (в т. ч. технічної розвідки), що використовуються для забезпечення витоку чи втручання в цілісність та конфіденційність інформації». Обгрунтування: Пропонована редакція звужує поняття технічного каналу витоку	Відхилено	«технічний канал витоку інформації – взаємопов'язана сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки, спрямована на забезпечення витоку інформації»;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		інформації лише до спеціального фізичного каналу (наприклад, радіочастотного, або буквально пристрій на дроті). Однак окрім фізичного каналу може бути і програмний (т. зв. бекдори, експлойти та ін.) канал витоку, який створюється "поверх" існуючого. З огляду на це визначення необхідно скоригувати, включивши не лише сигнал, а й з'єднання, а замість звуження засобів лише до спецзасобів технічної розвідки, розширити визначення інструментарію для забезпечення витоків також таким чином, щоб воно включало засоби для втручання в цілісність та конфіденційність даних. Це відповідає визначенню захисту інформації, яке дається в цій же частині.		
20	2) Статтю 8 викласти в новій редакції:	**-20- Н.д. Пузійчук А. В. (р.к. №182)** В абзаці першому підпункту 2 пункту 1 розділу I слово «новій» замінити словом «такій».	Відхилено	2) статтю 8 викласти в такій редакції:
		-21- Н.д. Федієнко О. П. (р.к. №89) 2) Статтю 8 викласти в новій редакції:	Відхилено	
21	«Стаття 8. Умови обробки інформації в системі	**-22- Н.д. Федієнко О. П. (р.к. №89)** «Стаття 8. Умови обробки інформації в системі	Відхилено	«Стаття 8. Умови обробки інформації в системі
22	Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.	**-23- Н.д. Федієнко О. П. (р.к. №89)** ***Умови обробки інформації в системі, об'єкті критичної інформаційної інфраструктури, визначаються власником або розпорядником системи з урахуванням вимог захисту інформації, визначених законодавством.***	Відхилено	Умови обробки інформації в системі, об'єкті критичної інформаційної інфраструктури визначаються власником або розпорядником відповідної системи з урахуванням вимог щодо захисту інформації, визначених законодавством.
23	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	**-24- Н.д. Федієнко О. П. (р.к. №89)** 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	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	організації, органи місцевого самоврядування, повинні оброблятися 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.	органи, державні підприємства, установи та організації, органи місцевого самоврядування, повинні оброблятися із застосуванням комплексної системи захисту інформації, або шляхом авторизації **системи безпеки інформації**, або шляхом отримання сертифікату відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності.		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.
		-25- Н.д. Федієнко О. П. (р.к. №89) ***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.***	Відхилено	
		-26- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Абзац 2 статті 8 викласти в наступній редакції: 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	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		місцевого самоврядування, мають оброблятися із застосуванням комплексної системи захисту інформації або шляхом авторизації з безпеки, або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності. Інформаційна безпека даних в таких системах обов'язково повинна поширюватись на резервні копії державних інформаційних ресурсів. Обґрунтування: Чинне формулювання приписує захист комплексною системою захисту лише безпосередньо процесів обробки даних. Однак, з огляду на масштабний злам реєстрів Мін'юсту, під час якого також були знищені резервні копії, вбачається необхідним ввести законодавчий припис поширити інформаційну безпеку даних на резервування даних.		
24	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:	**-27- Н.д. Федієнко О. П. (р.к. №89)** ***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, здійснюється в порядку, встановленому Кабінетом Міністрів України.***	Відхилено	
25	національним органом України з акредитації;	**-28- Н.д. Федієнко О. П. (р.к. №89)** ***Складовою такого порядку авторизації з безпеки має бути встановлення повідомного (декларативного) принципу про прийняття рішення власником або розпорядником системи, об'єкта критичної інформаційної інфраструктури (крім тих, в яких обробляється інформація, що становить***	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		державну таємницю) про авторизацію 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 всього життєвого циклу відповідної системи, об'єкта критичної інформаційної інфраструктури.		
26	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.	**-29- Н.д. Федієнко О. П. (р.к. №89)** ***Підтвердження відповідності стандарту інформаційної безпеки 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 національний орган України з акредитації та 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.***	Відхилено	
27	Процедури авторизації систем безпеки інформації та отримання сертифікату відповідності стандарту інформаційної безпеки не застосовуються для обробки інформації категорії державна таємниця.	**-30- Н.д. Федієнко О. П. (р.к. №89)** ***Процедура отримання сертифіката відповідності стандарту інформаційної безпеки не застосовується до систем, в яких обробляється інформація, що становить державну таємницю.***	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
				(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.
28	Підтвердження відповідності комплексної системи захисту інформації забезпечується власником/розпорядником системи з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому Кабінетом Міністрів України.	**-31- Н.д. Федієнко О. П. (р.к. №89)** Підтвердження відповідності комплексної системи захисту інформації забезпечується власником/розпорядником системи **у порядку, встановленому Кабінетом Міністрів України.**	Відхилено	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.
		-32- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176) Абзац дев’ятий підпункту 2) пункту 1 Розділу І викласти в такій редакції: «Підтвердження відповідності комплексної системи захисту інформації забезпечується власником/розпорядником системи на основі технічних регламентів щодо безпеки даних, складених за Європейською схемою сертифікації кібербезпеки, з урахуванням галузевих вимог та норм інформаційної безпеки у порядку,	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		встановленому Кабінетом Міністрів України.».		
		-33- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Абзац 5 статті 8 викласти в наступній редакції: Підтвердження відповідності комплексної системи захисту інформації забезпечується власником/розпорядником системи на основі технічних регламентів щодо безпеки даних, складених за Європейською схемою сертифікації кібербезпеки, з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому Кабінетом Міністрів України. Обгрунтування (повторення поправки №20, відхиленої до другого читання): Пропонована норма орієнтує підтвердження відповідності системи захисту інформації лише на урахування національних вимог та норм інформаційної безпеки, які з огляду на численні випадки порушення кібербезпеки і витоки даних, слід вважати заслабкими. Тому вбачається доцільним посилити умови підтвердження відповідності жорстким приписом використовувати технічні регламенти за Європейською схемою сертифікації кібербезпеки. Це, по-перше, узгоджує процедуру підтвердження відповідності кібербезпеки із чинним законодавством про оцінку відповідності (зокрема, Законом України "Про технічні регламенти та оцінку відповідності"), а також узгоджує даний закон із європейським законодавством щодо кібербезпеки, зокрема, Актом про Кібербезпеку, який вводить загальну схему сертифікації кібербезпеки	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		(European cybersecurity certification framework).		
29	Авторизація системи безпеки інформації здійснюється в порядку, встановленому Кабінетом Міністрів України.	**-34- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	
		Авторизаціяї системи безпеки відповідної інформаційної, електронної комунікаційної та інформаційно-комунікаційної систем здійснюється в порядку, встановленому Кабінетом Міністрів України		
		-35- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)	Відхилено	
		Абзац десятий підпункту 2 пункту 1 розділу І проекту Закону викласти в такій редакції: «Авторизація системи з безпеки здійснюється в порядку, встановленому Кабінетом Міністрів України».	Народні депутати України - члени Комітету	
		-36- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		Авторизаціяї системи безпеки відповідної інформаційної, електронної комунікаційної та інформаційно-комунікаційної систем здійснюється в порядку, встановленому Кабінетом Міністрів України		
		-37- Н.д. Федієнко О. П. (р.к. №89)	Відхилено	
		Авторизація з безпеки або отримання сертифіката відповідності стандарту інформаційної безпеки щодо систем, об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, здійснюється за одночасного дотримання таких умов:		
30	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.	**-38- Н.д. Федієнко О. П. (р.к. №89)** ***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;***	Відхилено	Процедура отримання сертифіката відповідності стандарту інформаційної безпеки не застосовується до систем, в яких обробляється інформація, що становить державну таємницю.
31	Авторизація систем безпеки або отримання сертифікату підтвердження відповідності стандарту інформаційної безпеки щодо систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорії службова інформація, об'єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, здійснюється за	**-39- Н.д. Федієнко О. П. (р.к. №89)** ***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;***	Відхилено	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,

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	одночасного дотримання таких додаткових умов:			здійснюється за одночасного дотримання таких умов:
32	використання для захисту інформації в системі 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, виданий органом з оцінки відповідності, який акредитовано або національним органом України з акредитації, або національним органом з акредитації іншої держави, якщо і національний орган з акредитації України 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;	**-40- Н.д. Федієнко О. П. (р.к. №89)** ***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";***	Відхилено	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;
33	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;	**-41- Н.д. Федієнко О. П. (р.к. №89)** ***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;***	Відхилено	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;
		-42- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168),	Відхилено	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,

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Абзац 11 статті 8 викласти в такій редакції: власник, кінцевий бенефіціар або розпорядник жодного з елементів системи безпеки 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"; Обґрунтування: Пропоноване формулювання неявно передбачає, що об'єкт критичної інфраструктури може мати власника або розпорядника, який знаходиться за межами України - тобто, резидента іншої держави. На нашу думку, ані об'єкти критичної інфраструктури, на яких обробляються державні ресурси або службова інформація, ані елементи таких об'єктів, не можуть знаходитись у власності чи розпорядженні іноземних юридичних чи фізичних осіб. Таким чином, необхідно змінити дане визначення таким чином, щоб воно включало лише систему безпеки (найкращі антивірусні пакети, наприклад, на даний момент є хмарними сервісами, елементи яких знаходяться в інших країнах), а також буде включати не лише власника чи розпорядника, а й кінцевого бенефіціара такої системи (наприклад, той же антивірус Касперського, який визнаний шпигунським програмним забезпеченням, керується холдинговою компанією у Великій Британії (тобто, вона є його розпорядником), але кінцевим бенефіціаром її є російська компанія Kaspersky Lab).		яка входить до митного або воєнного союзу з такими державами або щодо якої застосовано санкції відповідно до Закону України "Про санкції";

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
34	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;	**-43- Н.д. Федієнко О. П. (р.к. №89)** ***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.*** **-44- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163)** Абзац 12 статті 8 викласти в такій редакції: власник системи безпеки об'єкта критичної інформаційної інфраструктури або його представник, який надає послуги інформаційної безпеки для об'єкта критичної інфраструктури з використанням системи, елементи якої розміщуються поза межами України, є юридичною особою, зареєстрованою в Україні, або має свого офіційного представника в Україні; Обгрунтування: Пропоноване формулювання неявно передбачає, що об'єкт критичної інфраструктури може мати власника або розпорядника, який знаходиться за межами України - тобто, резидента іншої держави. На нашу думку, ані об'єкти критичної інфраструктури, на яких обробляються державні ресурси або службова інформація, ані елементи таких об'єктів, не можуть знаходитись у власності чи розпорядженні іноземних юридичних чи фізичних осіб. Таким чином, необхідно змінити дану норму таким чином, щоб вона поширювались лише на послуги інформаційної безпеки та системи безпеки	Відхилено Відхилено	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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		об'єктів критичної інфраструктури, і прибрати з даного визначення розпорядників - оскільки якщо окремий елемент системи безпеки можна замовити через субпідряд (якщо йдеться про спеціальний додаток чи модуль, написаний на певній універсальній платформі), то система безпеки в цілому та послуги інформаційної безпеки для об'єктів інформаційної інфраструктури має закупатись виключно за прямими контрактами для мінімізації корупційної складової.		
35	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.	**-45- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163)** 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. Абзац 13 статті 8 викласти в такій редакції: 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, а також збереження державної власності на оброблювану інформацію (або її копій - тимчасових або резервних) внаслідок використання елементів системи безпеки, що знаходяться за межами України. Обгрунтування: Використання систем безпеки, чиї елементи знаходяться за межами України, несуть в собі потенційний ризик зміни власності на дані. В українському законодавстві, наприклад, персональні дані не	Відхилено	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.

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		є секретними, а їх володільцем (власником) по факту є власник системи, в якій вони обробляються. Скажімо, антивірусні пакети передбачають завантаження даних на хмарний сервіс, тобто, таким чином дані перетинають кордон - і в силу цього факту дані (або їх копія) можуть стати власністю того, хто володіє системою, в якій вони обробляються. Точно так само, власником резервних копій може стати власник системи, в якій вони зберігаються. З огляду на те, що закон про персональні дані, який утверджує право власності українських громадян на персональні дані, ще не ухвалений (і термін ухвалення невідомий), вбачається доцільним законодавчо обумовити юридичне збереження хоча б державної власності на інформацію з державних інформаційних ресурсів.		
36	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 та за умови використання засобів криптографічного захисту суб'єктів господарювання, які провадять ліцензовану діяльність відповідно до законодавства України. Порядок атестації такого комплексу технічного захисту інформації визначається спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.	**-46- Н.д. Пузійчук А. В. (р.к. №182)** Абзац сімнадцятий підпункту 2 пункту 1 розділу I після слів «захисту інформації від» доповнити словами «несанкціонованих дій та».	Відхилено	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.
		-47- Н.д. Федієнко О. П. (р.к. №89) ***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.***	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
37	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.	**-48- Н.д. Федієнко О. П. (р.к. №89)** ***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.***	Відхилено	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.
38	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.	**-49- Н.д. Василевська-Смаглюк О. М. (р.к. №302)** В абзаці дев’ятнадцятому підпункту 2 пункту 1 законопроекту слово "депозитарію" виключити.	Відхилено	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.
		-50- Н.д. Федієнко О. П. (р.к. №89) 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.	Відхилено	
		-51- Н.д. Федієнко О. П. (р.к. №89) ***Національний банк України визначає умови обробки інформації в системах у сфері надання банківських, інших фінансових та платіжних послуг, інформації з обмеженим доступом, що є***	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		складовою системи депозитарного обліку 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.		
39	Власники систем для забезпечення належного функціонування систем та захисту інформації, що обробляється в них:	**-52- Н.д. Федієнко О. П. (р.к. №89)** ***Власники або розпорядники систем, об'єктів критичної інфраструктури для забезпечення їх належного функціонування та захисту інформації, що обробляється в них:***	Відхилено	Власники або розпорядники систем, об'єктів критичної інформаційної інфраструктури для забезпечення їх належного функціонування та захисту інформації, що обробляється в них:
40	створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх захисту, цілісності та конфіденційності;	**-53- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)** Абзац двадцять перший підпункту 2) пункту 1 Розділу I викласти в такій редакції: «створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх захисту, цілісності та конфіденційності. Повне резервування інформаційних ресурсів, необхідних для забезпечення критичних державних функцій або соціально значущих послуг, має здійснюватись не рідше за 1 раз на тиждень, а протягом періоду дії правового	Відхилено	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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		режиму воєнного стану в Україні та шести місяців після його припинення чи скасування - із обов'язковим збереженням резервних копій на окремих фізичних носіях в зашифрованій формі;».		
		-54- Н.д. Федієнко О. П. (р.к. №89) ***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;***	Відхилено	
		-55- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) 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; Абзац 18 статті 8 викласти в такій редакції: створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх захисту, цілісності та конфіденційності. Повне резервування інформаційних ресурсів, необхідних для забезпечення критичних державних функцій або соціально значущих послуг, має здійснюватись не рідше за 1 раз на тиждень, а протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування - із обов'язковим збереженням резервних копій на окремих фізичних носіях в зашифрованій формі;	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Обгрунтування (повторення поправки №26, яка була відхилена в другому читанні): Кейс масштабного знищення реєстрів Мін'юсту, який включав знищення всіх резервних копій показав, що вітчизняне законодавство щодо резервування та дублікації критичних даних є вкрай слабким. Процедура валідації реєстрів, яку проводив Мінюст з 24 грудня, означає, що дані фактично втрачені не були, але їх відновлення відбувалось або із часткових резервних копій, або т. зв. інкрементальних (тобто, коли резервується не реєстр, а лише зміни в ньому). Остаточно відновлені реєстри були лише 20 січня ц. р., що додатково доказує, що відновлення відбувалось з часткових резервних копій. З огляду на це, вбачається доцільним внести законодавчий припис на мінімальний період повного резервування інформаційних ресурсів, які дозволять відновлення критичних даних із втратою даних не менше тижня транзакцій. Також, для військового часу слід передбачити законодавчий припис про обов'язкове резервування на фізичних носіях - бо чинне формулювання наступного абзаца дозволяє тлумачення про його необов'язковість.		
41	забезпечують створення резервних копій державних інформаційних ресурсів та систем 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), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування;	**-56- Н.д. Федієнко О. П. (р.к. №89)** ***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;***	Відхилено	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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-57- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) забезпечують створення резервних копій державних інформаційних ресурсів та систем 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), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування; Абзац 19 статті 8 викласти в такій редакції: Забезпечують створення резервних копій (в т. ч. обов'язкове періодичне повне резервування) державних інформаційних ресурсів та систем 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), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування; Обгрунтування: Під час війни (як повномасштабної, так і повзучої) будь-який державний інформаційний ресурс знаходиться під постійною хакерською атакою. З огляду на це необхідно передбачити законодавчий припис обов'язкового періодичного повного резервування саме для періода воєнного стану.	Відхилено	
42		**-58- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після 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.*** **-59- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163)** 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, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування. Абзац 20 статті 8 викласти в такій редакції: 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, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування. Резервні копії, які переміщуються за межі України, мають обов'язково дублюватись на території України на фізичних носіях або на ресурсах, що не мають постійного підключення до комунікаційних мереж. Обгрунтування: З огляду на те, що резервні копії, переміщені за кордон, можуть	Відхилено	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.

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		також бути атаковані, необхідно законодавчо обумовити основний спосіб убезпечення даних в умовах постійних хакерських атак - мати резервні копії поза мережею (наприклад, в локальній мережі, яка не має прямого з'єднання з Інтернетом). Тоді у випадку масштабного зламу можна оперативно підімкнути ці резерви або напряму (система зеркалювання), або просто відновити з них дані.		
43	Розміщення систем та зберігання резервних копій державних інформаційних ресурсів та систем на територіях України, на яких органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та територіях держав, які входять до митних та воєнних союзів з такими державами, забороняється».	**-60- Н.д. Федієнко О. П. (р.к. №89)** ***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».***	Відхилено	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»;
44	3) у статті 9:			3) у статті 9:
45	у частині першій після слова «власника» доповнити словами «або розпорядника»;			частину першу після слова «власника» доповнити словами «або розпорядника»;
46	у частині другій слова «службу захисту інформації» замінити словами «підрозділ із кіберзахисту»;	**-61- Н.д. Сірко Ю. Л. (р.к. №210)** виключити	Відхилено	у частині другій слова «службу захисту інформації» замінити словами «підрозділ із кіберзахисту»;
		-62- Н.д. Сірко Ю. Л. (р.к. №210) виключити	Відхилено	
47	4) у статті 10:			4) у статті 10:
48	частину першу викласти в такій редакції:			частину першу викласти в такій редакції:
49	«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,	**-63- Н.д. Федієнко О. П. (р.к. №89)** **Мінімальні** вимоги захисту **як базовий профіль безпеки в системах,** власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування та в яких	Відхилено	«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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), встановлюються Кабінетом Міністрів України»;	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), встановлюються Кабінетом Міністрів України.		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»;
50		**-64- Н.д. Ар'єв В. І. (р.к. №202)**	Відхилено	
		Президент України, прем’єр-міністр України, члени уряду України, народні депутати України, працівники патронатних служб, депутати місцевих рад, державні службовці і керівники та працівники державних установ та підприємств, які працюють з пристроями з обробки інформації з доступом у інформаційні, електронно-комунікаційні та інформаційно-комунікаційні системи не рідше одного разу на три місяці проходять інструктаж з основ кібербезпеки, порядок якого встановлюється Кабінетом міністрів. Профільні технічні працівники державних установ та підприємств, які працюють з пристроями з обробки інформації з доступом у інформаційні, електронно-комунікаційні та інформаційно-комунікаційні системи не рідше одного разу на три місяці проходять навчання з кібербезпеки, порядок якого встановлюється Кабінетом Міністрів.		
51	у частині третій:			у частині третій:
52	абзац шостий викласти в такій редакції:			абзац шостий викласти в такій редакції:
53	«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 та	**-65- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук**	Відхилено	«здійснює заходи щодо виявлення загроз державним інформаційним ресурсам від несанкціонованих дій та витоку інформації технічними каналами в інформаційних, електронних комунікаційних, інформаційно-комунікаційних та

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	надає рекомендації щодо запобігання таким загрозам»;	**Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)** Абзац шостий підпункту 4) пункту 1 Розділу I викласти в такій редакції: «здійснює заходи щодо виявлення загроз державним інформаційним ресурсам від несанкціонованого доступу, втручань в діяльність та від витоку інформації технічними каналами в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та надає рекомендації щодо запобігання таким загрозам;».		технологічних системах, надає рекомендації щодо запобігання таким загрозам»;
		-66- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) 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; Абзац 6 частини 3 статті 10 викласти в такій редакції: здійснює заходи щодо виявлення загроз державним інформаційним ресурсам від несанкціонованого доступу, втручань в діяльність та від витоку інформації технічними каналами в інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних системах та надає рекомендації щодо запобігання таким загрозам; Обгрунтування (повторення поправки №30, яка була відхилена до другого читання):	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		В пропонованих змінах попередня розпливчаста норма замінюється на конкретику, зокрема, виокремлюється загроза від витоку. Однак витік даних не є основною загрозою. Основними загрозами є несанкціонований доступ (а витік є наслідком отримання такого доступа) та втручання в діяльність державного інформаційного ресурсу. Таким чином, пропоноване формулювання орієнтуватиме заходи лише на боротьбу із наслідками, а не причинами кіберінцидентів. З огляду на це вбачається доцільним уточнити формулювання і додати до нього несанкціонований доступ та втручання, які є основними загрозами для державних інформаційних ресурсів.		
54	після абзацу шостого доповнити трьома новими абзацами такого змісту:	**-67- Н.д. Ар'єв В. І. (р.к. №202)** після абзацу шостого доповнити чотирма новими абзацами такого змісту:	Відхилено	після абзацу шостого доповнити трьома новими абзацами такого змісту:
55	«забезпечує реалізацію та здійснює методичне керівництво підтвердження відповідності комплексної системи захисту інформації, авторизацією з безпеки, порядок проведення яких затверджується Кабінетом Міністрів України;			«забезпечує реалізацію та здійснює методичне керівництво щодо підтвердження відповідності комплексної системи захисту інформації, авторизації з безпеки, порядок проведення яких затверджується Кабінетом Міністрів України;
56	затверджує порядок ведення переліку авторизованих систем;			затверджує порядок ведення переліку авторизованих систем з безпеки;
57	здійснює включення систем з безпеки до переліку авторизованих систем та виключення з такого переліку».			здійснює включення авторизованих систем з безпеки до переліку авторизованих систем з безпеки та виключення з такого переліку».
58		**-68- Н.д. Ар'єв В. І. (р.к. №202)** розробляє методичні рекомендації для інструктажу з основ кібербезпеки та навчань з кібербезпеки та оновлює методичні рекомендації не рідше ніж один раз на три місяці з врахуванням аналізу нових тенденцій кібератак та інцидентів.	Відхилено	
59	У зв’язку з цим абзац дев’ятий вважати абзацом десятим;			У зв’язку з цим абзац сьомий вважати абзацом десятим;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
60	частину четверту викласти в такій редакції:			частини четверту і п'яту замінити чотирма новими частинами такого змісту:
61	«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 цільові профілі безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, власником (розпорядником) яких вони є»;	**-69- Н.д. Федієнко О. П. (р.к. №89)** Органи державної влади, державні органи, органи місцевого самоврядування, з урахуванням набору мінімальних вимог 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 та інформаційно-комунікаційних систем, власником (розпорядником) яких вони є. частину 4 ст. 10 викласти в такій редакції **Органи державної влади, державні органи, що в межах своїх повноважень формують або реалізують державну політику у відповідній сфері або галузі, розробляють та, за погодженням Державної служби спеціального зв'язку та захисту інформації України, затверджують галузеві профілі безпеки для відповідної галузі або сфери з урахуванням мінімальних вимог заходів захисту (базового профілю), а також відповідних політик, стандартів та особливостей у відповідній галузі або сфері.** додати чатину 5 ст. 10 в такій редакції **Порядок затвердження цільових та галузевих профілів безпеки затверджується Кабінетом Міністрів України.**	Відхилено	«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
		-70- Н.д. Федієнко О. П. (р.к. №89) **додатково** …. **Національний банк України встановлює вимоги щодо забезпечення захисту інформації (вимоги щодо захисту якої встановлені законами у сфері надання**	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		банківських, інших фінансових, крім професійної діяльності на ринках капіталу та діяльності в системі накопичувального пенсійного забезпечення, та платіжних послуг) у системах Національного банку України, включаючи системи депозитарного обліку 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		нагляд за діяльністю яких здійснює Національний банк України, валютного регулювання та валютного нагляду, а також в системі депозитарного обліку Національного банку України». У зв'язку з цим частину шосту вважати частиною восьмою;
		-71- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)	Відхилено	
		Абзац тринадцятий підпункту 4) пункту 1 Розділу I викласти в такій редакції: «Органи державної влади, державні органи, органи місцевого самоврядування, в межах своїх повноважень та компетенцій, з урахуванням набору відповідних вимог заходів захисту встановлених для відповідних систем, розробляють та затверджують цільові профілі та рівні безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, власником (розпорядником) яких вони є.».		
62		**-72- Н.д. Василевська-Смаглюк О. М. (р.к. №302)**	Відхилено	
		Підпункт 4 пункту 1 доповнити двома новими абзацами такого змісту:		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		“частину п’яту викласти у такій редакції: “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, включаючи системи депозитарного обліку 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”.		
		-73- Н.д. Сірко Ю. Л. (р.к. №210) Міністерство оборони України з врахуванням особливостей виконання завдань Збройними Силами України, визначених законом, а також вимог нормативних документів НАТО в порядку, встановленому Кабінетом Міністрів України, для власних систем визначає: умови обробки та особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; особливості порядку створення комплексних систем захисту інформації та галузевих профілів безпеки; особливості забезпечення кібербезпеки, кіберзахисту та організації моніторингу стану кіберзахисту; особливості взаємодії з урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA та інформування CERT-UA про інциденти кібербезпеки; особливості використання програмного забезпечення та	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		засобів захисту інформації; особливості вибору засобів технічного та криптографічного захисту інформації при створенні комплексної системи захисту інформації або систем управління інформаційної безпеки.		
63	5) у статті 13 «Прикінцеві положення»:			5) у статті 13 «Прикінцеві положення»:
64	назву викласти у такій редакції:			назву викласти в такій редакції:
65	«Стаття 13. Прикінцеві та перехідні положення»;			«Стаття 13. Прикінцеві та перехідні положення»;
66	доповнити підпунктом 1^1 такого змісту:			доповнити пунктом 1^1 такого змісту:
67	«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)».			«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)».
68	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):	**-74- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Частину 2 вважати частиною 3	Відхилено	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):
		-75- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Бобровська С. А. (р.к. №217), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Чернєв Є. В. (р.к. №26)	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Пункт 2 Розділу I проекту Закону викласти в такій редакції: «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	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 багаторазового застосування правил та настанов щодо наявних чи потенційних завдань спрямованого на досягнення оптимального ступеня впорядкованості у сферах криптографічного та технічного захисту		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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»; «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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 органах місцевого самоврядування;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, держаним органам, органам місцевого самоврядування, операторам		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 надання 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 та національної системи обміну інформацією 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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».		
		-76- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Касай Г. О. (р.к. №280), Н.д. Ковальов О. І. (р.к. №262), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Хоменко О. В. (р.к. №68), Н.д. Чернєв Є. В. (р.к. №26) Пункт 2 розділу І проекту Закону викласти в такій редакції: «2. У Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» (Відомості Верховної	Враховано Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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»;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 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»;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		(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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		(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 органах місцевого самоврядування; 101) забезпечення нормативно-правового регулювання відносин у сферах стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, держаним органам, органам місцевого самоврядування, операторам критичної інфраструктури, власникам або розпорядникам об’єктів критичної інформаційної інфраструктури;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 надання 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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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».		
69	1) у частині першій статті 1:			1) у частині першій статті 1:
70	абзаци шостий і сьомий викласти в такій редакції:			абзаци шостий і сьомий викласти в такій редакції:
71	«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;			«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;
72	експертні дослідження – дослідження та аналіз конкретних властивостей засобів криптографічного захисту інформації, криптографічних алгоритмів з метою			експертні дослідження – дослідження та аналіз конкретних властивостей засобів криптографічного захисту інформації, криптографічних алгоритмів з метою

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	перевірки їх відповідності вимогам нормативно-правових актів, оцінки ступеня захищеності інформації або їх науково-технічного рівня»;			перевірки їх на відповідність вимогам нормативно-правових актів, оцінки ступеня захищеності інформації або науково-технічного рівня таких засобів, алгоритмів»;
73	абзаци дев’ятий і десятий виключити;			абзаци дев’ятий і десятий виключити;
74	абзац сімнадцятий викласти в такій редакції:			абзац сімнадцятий викласти в такій редакції:
75	«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»;			«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»;
76	доповнити з урахуванням алфавітного порядку термінами такого змісту:			доповнити з урахуванням алфавітного порядку термінами такого змісту:
77	«верифікація – комплекс заходів щодо перевірки відповідності програмних і технічних засобів вимогам, встановленим нормативними документами»;			«верифікація – комплекс заходів щодо перевірки відповідності програмних і технічних засобів вимогам, встановленим нормативними документами»;
78	«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»;	**-77- Н.д. Сірко Ю. Л. (р.к. №210)** -засіб технічного захисту інформації – технічний або програмний засіб, у якому передбачено функції технічного захисту інформації, або контролю ефективності технічного захисту інформації;	Відхилено	«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»;
79		**-78- Н.д. Сірко Ю. Л. (р.к. №210)** засіб технічного захисту інформації – технічний або програмний засіб, у якому передбачено функції технічного захисту інформації, або контролю ефективності технічного захисту інформації; **-79- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	«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»;	орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам – наукова (науководослідна, науково-технологічна, науково-технічна, науково-практична) 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»; Примітка: зміни відповідно до Закону України «Про наукову і науково-технічну діяльність»		«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»;
		-80- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам – наукова (науководослідна, науково-технологічна, науково-технічна, науковопрактична) 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»; Примітка: зміни відповідно до Закону України «Про наукову і науково-технічну діяльність»		
80	«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	**-81- Н.д. Мокан В. І. (р.к. №99)**	Відхилено	«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
		Визначення терміну "оцінювання стану кіберзахисту" виключити із законопроєкту. ***Обґрунтування.*** Як вказує ГНЕУ, пропозиція встановлювати «відповідність … аналітичним оглядам та іншим документам», без чіткого розуміння їх зобов'язального чи навіть рекомендаційного характеру,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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»;	слугуватиме розширенню дискреції Державної служби спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ) у процесах оцінювання. Норма містить ризик надзвичайно широких дискреційних повноважень для ДССЗЗІ.		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»;
		-82- Н.д. Мамка Г. М. (р.к. №147), Н.д. Макаренко М. В. (р.к. №153), Н.д. Борт В. П. (р.к. №152), Н.д. Ларін С. М. (р.к. №132), Н.д. Чорний В. І. (р.к. №151), Н.д. Іоффе Ю. Я. (р.к. №136), Н.д. Німченко В. І. (р.к. №130)	Відхилено	
		У статті 1 у терміні «оцінювання стану кіберзахисту» слова «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» виключити.		
		-83- Н.д. Бурміч А. П. (р.к. №144)	Відхилено	
		Абзац дванадцятий пункту 1 частини другої розділу І законопроекту після слів «або відповідності національним стандартам у сфері захисту інформації або кіберзахисту або» доповнити словами «затвердженим до використання згідно із пунктом 771 частини першої статті 14 цього Закону», а після слів «розробленим та прийнятим іноземними та міжнародними організаціями» доповнити словами «(за умови їх оприлюднення Державною службою спеціального зв'язку та захисту інформації України із офіційним перекладом державною мовою);»		
		-84- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О.	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		(р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176) Підпункт 1) пункту 2 Розділу I доповнити абзацом тринадцятим в такій редакції: «оцінювання стану кіберзахисту – процес перевірки обраних та/або запрова-джених методів, заходів, засобів захисту інформації або кіберзахисту з метою встановлення поточного та/або цільового стану захищеності або їх відповід-ності вимогам законодавства щодо повноти запроваджених заходів захисту інформації або кіберзахисту, або відповідності національним стандартам у сфері захисту інформації або кіберзахисту або стандартам, настановам, реко-мендаціям та іншим документам, розроблених та ухвалених іноземними та міжнародними організаціями в галузі кібербезпеки;».		
		-85- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 12 пункту 1 частини 2 розділу I законопроекту викласти у наступній редакції: «оцінювання ступеню кіберзахисту - процес перевірки обраних та/або запроваджених методів, заходів, засобів захисту інформації або кіберзахисту з метою встановлення поточного та/або цільового ступеню 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»;	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-86- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Частину 1 статті 1 доповнити з урахуванням алфавітного порядку абзацем такого змісту: 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 та іншим документам, розроблених та ухвалених іноземними та міжнародними організаціями в галузі кібербезпеки Обгрунтування (повторення поправки №44, відхиленої в другому читанні): В даному терміні пропонується оцінювання стану відповідності прив'язати не лише до нормативних документів, а й до аналітичних оглядів, які, як правило, не є обов'язковими як такі, відтак їх зобов'язувальний характер та ступінь зобов'язань на їх основі буде визначатись ДССЗЗІ на власний розсуд. Це необ-грунтоване розширення дискреційних повноважень, оскільки аналітичні звіти в профільних організаціях не повисають в повітрі, а обробляються, системати-зуються і результують в рекомендації, настанови та стандарти, які уже мають зобов'язувальну дію. Відтак, аналітичні звіти з даного терміну варто виключи-ти, а також обмежити поняття "іншого документа" лише галуззю	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		кібербезпеки. Тому що без такого уточнення підставою для зобов'язання в галузі кібербезпеки може стати взагалі будь-який документ, що також стане необгрунтованим збільшенням дискреційних повноважень ДССЗЗІ.		
81	«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»;	**-87- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 13 пункту 1 частини 2 розділу I законопроекту викласти у наступній редакції: «репозитарій інформації про кіберінциденти - електронна база даних, в якій накопичуються, зберігаються і систематизуються відомості про кіберінциденти у порядку, встановленому Державною службою спеціального зв'язку та захисту інформації України»;	Відхилено	«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»;
82	«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»;			«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»;
83	«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»;			«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
				досягнення оптимального ступеня впорядкованості у зазначених сферах»;
84	«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»;			«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»;
85	«таксономія інцидентів кібербезпеки – схема понять та класифікації інцидентів кібербезпеки, призначена для застосування при обміні, повідомленні, зберіганні інформації та підготовці звітів про кіберінциденти»;	**-88- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 17 пункту 1 частини 2 розділу I законопроекту викласти у наступній редакції: «таксономія кіберінцидентів - схема понять та класифікації кіберінцидентів, призначена для застосування при обміні, повідомленні, зберіганні інформації та підготовці звітів про кіберінциденти»;	Відхилено	«таксономія кіберінцидентів – схема понять та класифікації кіберінцидентів, призначена для застосування під час обміну, повідомлення, зберігання інформації та підготовки звітів про кіберінциденти»;
86	2) частину першу статті 3 після абзацу дев’ятого доповнити новим абзацом такого змісту:			2) частину першу статті 3 після абзацу дев’ятого доповнити новим абзацом такого змісту:
87	«здійснення стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам».			«здійснення стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам».
88	У зв’язку з цим абзац десятий вважати абзацом одинадцятим.			У зв’язку з цим абзац десятий вважати абзацом одинадцятим;
89	3) у частині першій статті 14:			3) у частині першій статті 14:
90	у пункті 9 слова «засобів, комплексів та систем спеціального зв’язку» виключити;			у пункті 9 слова «засобів, комплексів та систем спеціального зв’язку» виключити;
91	пункт 13, 30 та 39 викласти в такій редакції:			пункти 13, 30 і 39 викласти в такій редакції:
92	«13) забезпечення в порядку, встановленому Кабінетом Міністрів України, функціонування державної системи	**-89- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д.**	Відхилено	«13) забезпечення функціонування державної системи урядового зв’язку, її безпеки, розвитку та готовності до роботи в

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	урядового зв'язку, її безпеки, розвитку та готовності до роботи в особливий період і в разі виникнення надзвичайної ситуації»;	**Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)**		особливий період і в разі виникнення надзвичайної ситуації»;
		Абзац четвертий підпункту 3 пункту 2 розділу I проекту Закону викласти в такій редакції: «13) забезпечення функціонування державної системи урядового зв'язку, її безпеки, розвитку та готовності до роботи в особливий період і у разі виникнення надзвичайної ситуації»	Народні депутати України - члени Комітету	
93	«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»;			«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»;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
94	«39) забезпечення функціонування CERT-UA»;			«39) забезпечення функціонування CERT-UA»;
95	пункт 48 після слів «ключових документів» доповнити словами «та державних шифрів»;			пункт 48 після слів «ключових документів» доповнити словами «та державних шифрів»;
96	у пункті 50:			пункти 50, 67 і 72 викласти в такій редакції:
97	абзаци другий та третій викласти в такій редакції:			«50) встановлення:
98	«технічних вимог до електронних комунікаційних мереж та об’єктів спеціального зв’язку;			технічних вимог до електронних комунікаційних мереж та об’єктів спеціального зв’язку;
99	порядку і забезпечення проведення експертизи інфраструктури електронних комунікацій проектів будівництва, реконструкції та модернізації електронних комунікаційних мереж, споруд»;			порядку і забезпечення проведення експертизи інфраструктури електронних комунікацій проектів будівництва, реконструкції та модернізації електронних комунікаційних мереж, споруд спеціального зв'язку»;
100	пункти 67 і 72 викласти в такій редакції:			
101	«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»;			«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»;
102	«72) здійснення відповідно до законодавства підготовки, перепідготовки та підвищення кваліфікації осіб у сферах кіберзахисту, криптографічного та технічного захисту інформації, електронних комунікацій та радіочастотного спектра»;			«72) здійснення відповідно до законодавства підготовки, перепідготовки та підвищення кваліфікації осіб у сферах криптографічного та технічного захисту інформації, кіберзахисту, електронних комунікацій та радіочастотного спектра»;
103	доповнити пунктом 77^1 такого змісту:			доповнити пунктом 77^1 такого змісту:
104	«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 The International Organization for Standartization	**-90- Н.д. Мамка Г. М. (р.к. №147), Н.д. Макаренко М. В. (р.к. №153), Н.д. Борт В. П. (р.к. №152), Н.д. Ларін С. М. (р.к. №132), Н.д. Чорний В. І. (р.к. №151), Н.д. Іоффе Ю. Я. (р.к. №136), Н.д. Німченко В. І. (р.к. №130)** 77-1) затвердження до використання переліків стандартів, настанов, рекомендацій, аналітичних оглядів та інших документів,	Відхилено	«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	(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, а також оприлюднення документів із переліку із перекладом державною мовою»;	розроблених та прийнятих іноземними та міжнародними організаціями з питань, що належать до повноважень Державної служби спеціального зв'язку та захисту інформації України; **-91- Н.д. Федієнко О. П. (р.к. №89)** 771) 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 цими організаціями процедур оцінки відповідності, включаючи, сертифікацію, рекомендованих для застосування у сферах організації спеціального зв'язку, **криптографічного та технічного** захисту інформації, кіберзахисту;	Відхилено	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»;
105	пункт 90 викласти в такій редакції:			пункт 90 викласти в такій редакції:
106	«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	**-92- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169),**	Відхилено	«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	службова інформація та державна таємниця, об'єктів критичної інфраструктури»;	**Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)**		інформація, що становить державну таємницю, стану кіберзахисту об'єктів критичної інформаційної інфраструктури та об’єктів критичної інфраструктури»;
		Абзац вісімнадцятий підпункту 3) пункту 2 Розділу I викласти в такій редакції: «90) забезпечення впровадження системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури, методичне забезпечення оцінювання стану кіберзахисту, стану захищеності інформації, проведення аудиту 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, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації);».		
		-93- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 18 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: Абзац 17 пункту 1 частини 2 розділу I законопроекту викласти у наступній редакції: «90) методичне регулювання оцінювання ступеню кіберзахисту, ступеню захищеності інформації, проведення оцінювання ступеню 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»;		
		-94- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Підпункт 90 частини 1 статті 14 викласти в такій редакції: 90) забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, методичне забезпечення оцінювання стану кіберзахисту, стану захищеності інформації, проведення аудиту 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, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації); Обгрунтування (повторення поправки №51, відхиленої до другого читання): Для того, щоб забезпечити максимально можливий рівень захисту, який необхідний в критичній інфраструктурі, потрібна комплексна оцінка (в т. ч. із моделюванням загроз та перевіркою програмних засобів за стандартами, наприклад, DevSecOps), яка можлива лише в форматі аудита і лише спеціально підготовленими фахівцями в цій галузі. З огляду на це необхідно зберегти чинні норми про аудит інформаційної безпеки та атестацію фахівців в цій галузі.		
107	пункт 91 виключити;	**-95- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута**	Відхилено	пункт 91 виключити;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)		
		Абзац дев’ятнадцятий підпункту 3) пункту 2 Розділу I викласти в такій редакції: «91) координація, організація аудиту захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури;».		
		-96- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Підпункт 91 частини 1 статті 14 викласти в такій редакції: 91) координація, організація аудиту захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури; Обгрунтування: Для того, щоб забезпечити максимально можливий рівень захисту, який необхідний в критичній інфраструктурі, потрібна комплексна оцінка, яка можлива лише в форматі аудита і лише спеціально підготовленими фахівцями в цій галузі. З огляду на це необхідно зберегти чинну норму про аудит інформаційної безпеки.	Відхилено	
108	доповнити пунктами 96-114 такого змісту:	**-97- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)**	Відхилено	доповнити пунктами 96-115 такого змісту:

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		У абзаці двадцятому підпункту 3 пункту 2 розділу I проекту Закону цифри «96-114» замінити цифрами «96-115».	Народні депутати України - члени Комітету	
109	«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.	**-98- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	«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.
		Абзац двадцять перший підпункту 3 пункту 2 розділу I виключити.		
		-99- Н.д. Бурміч А. П. (р.к. №144)	Відхилено	
		У абзаці двадцять першому пункту 3 частини другої розділу I законопроекту виключити слова «(їхніми субпідрядниками)», а після слів «, а також об'єктів критичної інформаційної інфраструктури» доповнити словами «; при цьому до таких вимог обов’язково включається вимога про заборону залучення постачальниками субпідрядників».		
		-100- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)	Відхилено	
		Абзаци двадцять перший, двадцять другий, двадцять третій підпункту 3) пункту 2 Розділу I викласти в такій редакції: «96) встановлення вимог щодо впровадження постачальниками 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		державна таємниця, а також об'єктів критичної інформаційної інфраструктури. Такі вимоги щодо впровадження заходів безпеки інформації застосовуються до постачальників 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 відповідності впроваджених заходів безпеки інформації встановленим вимогам відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг;».		
110	Такі вимоги щодо впровадження заходів безпеки інформації застосовуються до постачальників (їх субпідрядників) лише у разі, якщо товари, роботи, послуги, які вони	**-101- Н.д. Пузійчук А. В. (р.к. №182)** Абзац двадцять другий підпункту 3 пункту 2 розділу I виключити.	Відхилено	Такі вимоги щодо запровадження заходів безпеки застосовуються до постачальників товарів, робіт, послуг лише в разі, якщо товари, роботи, послуги, які вони
		-102- Н.д. Бурміч А. П. (р.к. №144)	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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.	У абзаці двадцять другому пункту 3 частини другої розділу I законопроекту виключити слова «(їх субпідрядників)».		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.
		-103- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		Такі вимоги щодо впровадження заходів безпеки інформації застосовуються .виключно для органів державної влади, державних органів, державних підприємств, установ та організацій, органів місцевого самоврядування 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		
		-104- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		Такі вимоги щодо впровадження заходів безпеки інформації застосовуються .виключно для органів державної влади, державних органів, державних підприємств, установ та організацій, органів місцевого самоврядування 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		
111	З метою встановлення таких вимог Державна служба спеціального зв’язку та захисту інформації України визначає критерії	**-105- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	З метою встановлення таких вимог Державна служба спеціального зв’язку та захисту інформації України визначає
		Абзац двадцять третій підпункту 3 пункту 2 розділу I виключити.		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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;	**-106- Н.д. Бурміч А. П. (р.к. №144)** У абзаці двадцять третьому пункту 3 частини другої розділу I законопроекту виключити слова «(їх субпідрядниками)», а після слів «відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг;» доповнити словами «обов'язково встановлює заборону залучення постачальниками субпідрядників;».	Відхилено	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;
112	97) 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;			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;
113	98) 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	**-107- Н.д. Федієнко О. П. (р.к. №89)** 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/розпорядниками інформаційних, електронних комунікаційних та	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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;	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;		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;
		-108- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 25 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «98) 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 ступеню 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;»	Відхилено	
114		**-109- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д.**	Відхилено	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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)		
		Підпункт 3 пункту 2 розділу I проекту Закону після абзацу двадцять п’ятого доповнити новим абзацом такого змісту: після абзацу двадцять п’ятого підпункту 3 пункту 2 розділу I проекту Закону доповнити новим абзацом такого змісту: «99) розробляє та забезпечує 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». Відповідно пункти 99-114 вважати пунктами 100-115;	Народні депутати України - члени Комітету	
115	99) 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 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;	**-110- Н.д. Пузійчук А. В. (р.к. №182)** Абзац двадцять шостий підпункту 3 пункту 2 розділу I виключити.	Відхилено	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 органах місцевого самоврядування;
116	100) забезпечення нормативно-правового регулювання відносин у сферах стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;	**-111- Н.д. Сірко Ю. Л. (р.к. №210)** виключити **-112- Н.д. Сірко Ю. Л. (р.к. №210)** виключити	Відхилено Відхилено	101) забезпечення нормативно-правового регулювання відносин у сферах стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;
117	101) забезпечення розроблення, прийняття, внесення змін, скасування,			102) забезпечення розроблення, прийняття, внесення змін, скасування,

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам в порядку, встановленому Кабінетом Міністрів України;			відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам у порядку, встановленому Кабінетом Міністрів України;
118	102) 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;	**-113- Н.д. Сірко Ю. Л. (р.к. №210)** виключити **-114- Н.д. Сірко Ю. Л. (р.к. №210)** виключити	Відхилено Відхилено	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;
119	103) забезпечення реалізації та методичне керівництво авторизацією систем з безпеки, порядок проведення якої затверджується Кабінетом Міністрів України;			104) забезпечення реалізації та методичне керівництво авторизацією з безпеки, порядок проведення якої затверджується Кабінетом Міністрів України;
120	104) затвердження порядку ведення переліку авторизованих систем, включення таких систем до переліку та виключення з нього, надання доступу до переліку та інформації з нього;	**-115- Н.д. Сірко Ю. Л. (р.к. №210)** виключити **-116- Н.д. Сірко Ю. Л. (р.к. №210)** виключити	Відхилено Відхилено	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;
121	105) 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 органах, органах місцевого самоврядування, державних установах, організаціях, органах місцевого самоврядування та які рекомендуються до застосування на об'єктах критичної інфраструктури;	**-117- Н.д. Сірко Ю. Л. (р.к. №210)** виключити **-118- Н.д. Сірко Ю. Л. (р.к. №210)** виключити	Відхилено Відхилено	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;
122		**-119- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	106) створення та забезпечення функціонування кваліфікаційного центру за групами кваліфікацій у сферах безпеки інформації та кіберзахисту;	106) створення та забезпечення функціонування кваліфікаційного центру за групами кваліфікацій у сферах безпеки інформації та кіберзахисту є обов'язковим виключно в органах державної влади, державних органах, органах місцевого самоврядування, державних установах, організаціях, органах місцевого самоврядування;		107) створення та забезпечення функціонування кваліфікаційного центру за групами кваліфікацій у сферах безпеки інформації та кіберзахисту;
		-120- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		створення та забезпечення функціонування кваліфікаційного центру за групами кваліфікацій у сферах безпеки інформації та кіберзахисту є обов'язковим виключно в органах державної влади, державних органах, органах місцевого самоврядування, державних установах, організаціях, органах місцевого самоврядування;		
123	107) забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;	**-121- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)**	Відхилено	108) забезпечення функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;
		Абзац тридцять четвертий підпункту 3) пункту 2 Розділу I (підпункт 107 частини 1 статті 14) виключити.		
		-122- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 34 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції:		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«107) забезпечення функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;»		
124	108) координація діяльності об’єктів критичної інфраструктури з питань кіберзахисту у разі введення надзвичайного стану або воєнного стану;	**-123- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	109) координація діяльності об’єктів критичної інфраструктури з питань кіберзахисту у разі введення надзвичайного стану або воєнного стану;
		108) координація діяльності об’єктів критичної інфраструктури з питань кіберзахисту у разі введення надзвичайного стану або воєнного стану разом із державними органами влади;		
		-124- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		координація діяльності об’єктів критичної інфраструктури з питань кіберзахисту у разі введення надзвичайного стану або воєнного стану разом із державними органами влади;		
125	109) забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози;	**-125- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	110) забезпечення функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;
		Абзац 36 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «109) забезпечення функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;»		
126	110) забезпечення функціонування регіональних центрів кіберзахисту;			111) забезпечення функціонування регіональних центрів кіберзахисту;
127	111) визначення для виконання завдання щодо функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози:	**-126- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	112) визначення для виконання завдання щодо функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози:
		111) визначення для суб'єктів господарювання державного та комунального секторів економіки виконання завдання щодо функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози:		
		-127- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О.	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		(р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)		
		Абзаци тридцять восьмий, тридцять дев’ятий, сороковий, сорок перший, сорок другий, сорок третій, сорок четвертий підпункту 3) пункту 2 Розділу I (підпункт 111 частини 1 статті 14) виключити.		
		-128- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 38 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «111) визначення для виконання завдання щодо функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози:»		
		-129- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
128		визначення для суб'єктів господарювання державного та комунального секторів економіки виконання завдання щодо функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози: **-130- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	
		рекомендації для суб'єктів приватного сектору виконання завдання щодо функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози:		
		-131- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
129	основних завдань, що можуть бути делеговані національною командою	рекомендації для суб'єктів приватного сектору виконання завдання щодо функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози:		основних завдань, що можуть бути делеговані національною командою

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	реагування галузевим та регіональним командам реагування, та порядку взаємодії таких команд з національною командою реагування;			реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA галузевим та регіональним командам реагування на кіберінциденти, кібератаки, кіберзагрози, та порядку взаємодії команд реагування з CERT-UA;
130	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, органам місцевого самоврядування та юридичним особам щодо об'єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких вони є;	**-132- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	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;
		вимог до організаційно-технічної спроможності, до сервісу з управління інцидентами кібербезпеки національної команди реагування, галузевих, регіональних команд реагування, а також **інших 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, органам місцевого самоврядування та юридичним особам щодо об'єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких вони є;		
		-133- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 40 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «вимог до організаційно-технічної спроможності, до сервісу з управління кіберінцидентами 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 кіберінцидентами органам державної влади, органам місцевого самоврядування та юридичним особам щодо об'єктів критичної інформаційної інфраструктури, власниками/розпорядниками яких вони є;»		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
131	порядку ведення репозитарію інформації про інциденти кібербезпеки, таксономій інцидентів кібербезпеки та їх версій;	**-134- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 41 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «порядку ведення репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій;»	Відхилено	порядку ведення репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій;
132	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;	**-135- Н.д. Федієнко О. П. (р.к. №89)** порядку здійснення моніторингу за діяльністю національної команди реагування, галузевих та регіональних команд реагування, а також **інших 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; **-136- Н.д. Сірко Ю. Л. (р.к. №210)** 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	Відхилено Відхилено	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 надання 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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		
		-137- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 42 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «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 кіберінцидентами 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;»	Відхилено	
		-138- Н.д. Сірко Ю. Л. (р.к. №210) 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	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		
133		**-139- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	
		порядок визначеннння для державного сектору та рекомендації для суб'єктів приватного сектору		
		-140- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		порядок визначеннння для державного сектору та рекомендації для суб'єктів приватного сектору		
134	порядку здійснення заходів реагування у кризовій ситуації в кіберпросторі;	**-141- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	порядку здійснення заходів реагування у кризовій ситуації в кіберпросторі;
		визначеннння для держ сектору і рекомендації для приватного		
		-142- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		визначеннння для держ сектору і рекомендації для приватного 4 Внесення програмного забезпечення та комунікаційного (мережевого) обладнання до переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання може бути оскаржене власником\розпорядником до постійно діючої апеляційної комісії, склад якої затверджується в порядку визначеним Кабінетом Міністрів України.		
135	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	**-143- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	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
		підстав надання на основі отриманої від CERTUA інформації вимог про реагування власникам/розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	інфраструктури, а також порядку, строків реалізації визначених відповідною вимогою про реагування заходів реагування та подання звіту про їх виконання;	категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури, **в яких оброблятиметься інформація, власниками/розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування,** а також порядку, строків реалізації визначених відповідною вимогою про реагування заходів реагування та подання звіту про їх виконання;		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;
136	112) встановлення для виконання завдання щодо функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози:	**-144- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 44 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «112) встановлення для виконання завдання щодо функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози:»	Відхилено	113) встановлення для виконання завдання щодо функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози:
137	порядку обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози, форм повідомлення, національної таксономії інцидентів кібербезпеки;	**-145- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 45 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, форм повідомлення, національної таксономії кіберінцидентів;»	Відхилено	порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, форм повідомлення, національної таксономії кіберінцидентів;
138	критеріїв для визначення значності впливу інциденту кібербезпеки, кібератаки, у тому числі для цілей визначення обов'язку здійснення повідомлення оператором критичної інфраструктури;	**-146- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 46 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «критеріїв для визначення значності впливу кіберінциденту, кібератаки, у тому числі для цілей визначення обов'язку здійснення повідомлення оператором критичної інфраструктури;»	Відхилено	критеріїв визначення значного кіберінциденту, у тому числі для цілей виконання зобов'язань, визначених законодавством про здійснення повідомлень про кіберінциденти;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
139	113) впровадження організаційно-технічних заходів щодо створення національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози;	**-147- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 47 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «113) впровадження організаційно-технічних заходів щодо створення національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;»	Відхилено	114) запровадження організаційно-технічних заходів щодо створення національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;
140	114) забезпечення функціонування платформи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози та встановлення порядку приєднання до такої платформи»;	**-148- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 48 пункту 3 частини 2 розділу I законопроекту викласти у наступній редакції: «114)забезпечення функціонування платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та встановлення порядку приєднання до такої платформи»;»	Відхилено	115) забезпечення функціонування платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та встановлення порядку приєднання до такої платформи»;
141	4) у частині першій статті 15:			4) у частині першій статті 15:
142	доповнити пунктами 1^1 і 1^2 такого змісту:			доповнити пунктами 1^1 і 1^2 такого змісту:
143	«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;	**-149- Н.д. Сірко Ю. Л. (р.к. №210)** «11) надавати виключно в органах державної влади, державних органах, органах місцевого самоврядування, державних установах, організаціях, органах місцевого самоврядування 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,	Відхилено	«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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		визначеному законодавством за діяльністю команд реагування;		
		-150- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 3 пункту 4 частини 2 розділу I законопроекту викласти у наступній редакції: ««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 невиконання вимог законодавства за результатами моніторингу в порядку, визначеному законодавством за діяльністю команд реагування;»	Відхилено	
		-151- Н.д. Сірко Ю. Л. (р.к. №210) надавати виключно в органах державної влади, державних органах, органах місцевого самоврядування, державних установах, організаціях, органах місцевого самоврядування 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;	Відхилено	
144	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	**-152- Н.д. Сірко Ю. Л. (р.к. №210)** 12) у визначених цим Законом випадках вживати заходів оперативного реагування на кіберзагрози та інциденти кібербезпеки, кібератаки шляхом надання обов’язкових до	Відхилено	1^2) у визначених законодавством випадках вживати заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози шляхом надання обов’язкових до виконання вимог про реагування

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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.	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 виключно в органах державної влади, державних органах, органах місцевого самоврядування, державних установах, організаціях, органах місцевого самоврядування;		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.
		-153- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 4 пункту 4 частини 2 розділу I законопроекту викласти у наступній редакції: «1[2]) у визначених законодавством випадках вживати заходів оперативного реагування на кіберзагрози та кіберінциденти, 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.»	Відхилено	
		-154- Н.д. Сірко Ю. Л. (р.к. №210) у визначених цим Законом 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 інформаційнокомунікаційних систем, в яких	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		обробляються державні інформаційні ресурси або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об'єктів критичної інформаційної інфраструктури виключно в органах державної влади, державних органах, органах місцевого самоврядування, державних установах, організаціях, органах місцевого самоврядування;		
145	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;»;	**-155- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 5 пункту 4 частини 2 розділу I законопроекту викласти у наступній редакції: «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 кіберінцидентом, кібератакою або кіберзагрозою;»;	Відхилено	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»;
146	в абзаці третьому пункту 8 слова «засобів, комплексів та систем спеціального зв'язку» виключити;			в абзаці третьому пункту 8 слова «засобів, комплексів та систем спеціального зв'язку» виключити;
147	пункт 22 після слів «ключових документів» доповнити словами «та державних шифрів».			пункт 22 після слів «ключових документів» доповнити словами «та державних шифрів».
148	3. Частину другу статті 2 Закону України «Про стандартизацію» (Відомості Верховної Ради України, 2014 р., № 31, ст. 1058 із наступними змінами) після слів «військові стандарти» доповнити словами «стандарти криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам».	**-156- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Частину 3 вважати частиною 4 **-157- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Бобровська С. А. (р.к. №217), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г.**	Відхилено Відхилено	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».

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Чернєв Є. В. (р.к. №26)		
		Пункт 3 Розділу І проекту Закону викласти в такій редакції: «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».	Народні депутати України - члени Комітету	
		-158- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Касай Г. О. (р.к. №280), Н.д. Ковальов О. І. (р.к. №262), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Хоменко О. В. (р.к. №68), Н.д. Чернєв Є. В. (р.к. №26)	Враховано	
		Пункт 3 Розділу І проекту Закону викласти в такій редакції: «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».	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
149	4. У Законі України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради України, 2017 р., № 45, ст. 403 із наступними змінами):	**-159- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Частину 4 вважати частиною 5	Відхилено	4. У Законі України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради України, 2017 р., № 45, ст. 403 із наступними змінами):
		-160- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Бобровська С. А. (р.к. №217), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Чернєв Є. В. (р.к. №26), Н.д. Івченко В. Є. (р.к. №185) Пункт 4 Розділу І проекту Закону викласти в такій редакції: «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	Відхилено Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		процесу надання основних 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, контрозвідувальними, 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, призначення відповідальної особи, яка виконує функції та завдання керівника з кіберзахисту в юридичній особі, що є власником або розпорядником об’єктів критичної інформаційної інфраструктури I і II категорій критичності, у порядку, затвердженому Кабінетом Міністрів України, погоджується Державною службою 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.		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 інфрастраструктури 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 в банківській системі України 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 розвитку 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 конкурентноспроможності 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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 та кіберзагрози щодо об'єктів кіберзахисту. Державний центр кіберзахисту проводить систематичні навчання із 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 здійснюють відповідно до порядку пошуку та/або		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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),		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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, 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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.		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 в банківській системі України 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-		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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.		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 можут 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 повідомляти 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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 встановленою національною таксономією кіберінцидентів у порядку, встановленому 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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».		
150		**-161- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Касай Г. О. (р.к. №280), Н.д. Ковальов О. І. (р.к. №262), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Хоменко О. В. (р.к. №68), Н.д. Чернєв Є. В. (р.к. №26)** Пункт 4 розділу І проекту Закону викласти в такій редакції: «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	Враховано Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, із суб'єктами забезпечення кібербезпеки, з правоохоронними, контрозвідувальними, 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 51. 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**		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 інфрастраструктури 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:		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 розвитку 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 конкурентноспроможності 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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-		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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.		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 функціонуванняСитуаційного 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		постійно діюча Об'єднана група реагування на кіберінциденти, кібератаки, кіберзагрози, до 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 91. 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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,		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 встановленою національною таксономією кіберінцидентів у порядку, встановленому 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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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».		
151	1) у частині першій статті 1:			1) у частині першій статті 1:
152		**-162- Н.д. Федієнко О. П. (р.к. №89)** Ст.1 доповнити пунктом **5-1) кібердиверсія – кібератака, спрямована на виведення з ладу або тимчасове пошкодження інформаційно-комунікаційних систем державних органів України або об'єктів критичної інформаційної інфраструктури;**	Відхилено	
153	пункт 7 викласти в такій редакції:			пункти 7 і 19 викласти в такій редакції:
154	«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;»;			«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»;
155		**-163- Н.д. Федієнко О. П. (р.к. №89)** пунк 14) викласти в наступній редакції **14) кібершпигунство – кібератака, що пов'язана з викраденням у політичних,**	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		економічних, військових чи інших цілях іноземних держав та їх структур інформації, вимога щодо захисту якої встановлена законом;		
156	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»;			
157		**-164- Н.д. Василевська-Смаглюк О. М. (р.к. №302)**	Відхилено	«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»;
		Підпункт 1 пункту 4 доповнити новими абзацами п'ятим та шостим такого змісту: “пункт 19 викласти у такій редакції: “19) об’єкт критичної інформаційної інфраструктури – інформаційна, електронно-комунікаційна, інформаційно-комунікаційна або технологічна система оператора критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування об’єкта критичної інфраструктури цього оператора та/або стійкість надання оператором критичної інфраструктури життєво важливої функції та/або послуги”. У зв'язку з цим абзаци п'ятий-сьомий вважати абзацами сьомим-дев'ятим відповідно.		
		-165- Н.д. Федієнко О. П. (р.к. №89)	Відхилено	
		19) **об’єкт критичної інформаційної інфраструктура – інформаційна, електронно комунікаційна, інформаційно-комунікаційна або технологічна система оператора критичної інфраструктури, кібератака на яку безпосередньо вплине на стале** функціонування об’єкта критичної інфраструктури цього оператора **та/або стійкість надання оператором життєво важливої функції та/або послуги;**		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-166- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)	Відхилено	
		Підпункт 1 пункту 4 розділу I проекту Закону після абзацу четвертого доповнити двома новими абзацами такого змісту: «пункт 19 викласти у такій редакції: «19) об’єкт критичної інформаційної інфраструктура – інформаційна, електронно комунікаційна, інформаційно-комунікаційна або технологічна система, яка необхідна для стійкого та безперервного функціонування об’єкта критичної інфраструктури, істотно впливає на безперервність та стійкість надання основних послуг та відсутній альтернативний об’єкт (спосіб) їх надання»;	Народні депутати України - члени Комітету	
158	доповнити пунктами 24 і 25 такого змісту:			доповнити пунктами 24 і 25 такого змісту:
159	«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;	**-167- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 5 пункту 1 частини 4 розділу I законопроекту викласти у наступній редакції: «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,	Відхилено	«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		об'єктів критичної інформаційної інфраструктури у зв'язку з кіберінцидентом, кібератакою або кіберзагрозою, переривання яких може призвести до значних негативних наслідків для національної безпеки;»		яких може призвести до значних негативних наслідків для національної безпеки;
160	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»;	**-168- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 6 пункту 1 частини 4 розділу I законопроекту викласти у наступній редакції: «25) реагування на кіберінциденти - структурована сукупність дій, спрямованих на підготовку до кіберінциденту, виявлення та аналіз інциденту, мінімізацію шкоди від інциденту та запобігання повторенню інциденту у майбутньому»	Відхилено	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»;
161	2) пункт 2 частини першої статті 2 виключити;			2) пункт 2 частини першої статті 2 виключити;
162		**-169- Н.д. Сірко Ю. Л. (р.к. №210)** Доповнити частиною третьою статті 2 наступного змісту: 3. Норми цього Закону, що визначають порядок функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози, не поширюються на інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційно-комунікаційних систем Міністерства оборони України, Збройних Сил України, Державної спеціальної служби транспорту, Служби безпеки України та розвідувальних органів України.	Відхилено	
163	3) у статті 4:			3) у статті 4:
164	у пунктах 1 і 3 частини другої слова «комунікаційні системи» замінити словами «інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи»;			у пунктах 1 і 3 частини другої слова «комунікаційні системи» замінити словами «інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи»;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
165	в абзаці першому частини третьої слова «перелік таких об’єктів» виключити;			в абзаці першому частини третьої слова «перелік таких об’єктів» виключити;
166	доповнити частиною четвертою такого змісту:	**-170- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	доповнити частиною четвертою такого змісту:
		Абзац четвертий підпункту 3 пункту 4 розділу І виключити.		
167	«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.	**-171- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	«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.
		Абзац п’ятий підпункту 3 пункту 4 розділу І виключити.		
168	Порядок формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання затверджуються Кабінетом Міністрів України.	**-172- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	Порядок формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання затверджується Кабінетом Міністрів України.
		Абзац шостий підпункту 3 пункту 4 розділу І виключити.		
169		**-173- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	
		Внесення програмного забезпечення та комунікаційного (мережевого) обладнання до переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання може бути оскаржене власником\розпорядником до постійно діючої апеляційної комісії, склад якої затверджується в порядку визначеним Кабінетом Міністрів України.		
170	Повноваження щодо забезпечення формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного	**-174- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	Повноваження щодо забезпечення формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного
		Абзац сьомий підпункту 3 пункту 4 розділу І виключити.		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	(мережевого) обладнання покладаються на Державну службу спеціального зв'язку та захисту інформації України»;			(мережевого) обладнання покладаються на Державну службу спеціального зв'язку та захисту інформації України»;
171	4) у статті 5:			4) у статті 5:
172	частину третю викласти в такій редакції:	**-175- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	частини другу і третю викласти в такій редакції:
		частину другу 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, **суб'єктів національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози; формує пропозиції для РНБОУ про оголошення кризової ситуації у кібербезпеці; координує реалізацію Стратегії кібербезпеки України, надає Раді національної безпеки і оборони України пропозиції щодо її формування та уточнення; визначає пріоритети, розробляє концептуальні засади та вносить пропозиції Президентові України 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.**		«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.
		-176- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)		
		Абзац другий підпункту 4 пункту 4 розділу I проекту Закону викласти в такій редакції: «частини другу і третю викласти в такій редакції:».	Народні депутати України - члени Комітету	
		-177- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)	Відхилено	
		Підпункт 4 пункту 4 розділу I проекту Закону після абзацу другого доповнити новим абзацом такого змісту: «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, суб'єктів національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози; формує пропозиції для РНБОУ про оголошення кризової ситуації у кібербезпеці; координує реалізацію Стратегії кібербезпеки України, надає Раді національної безпеки і оборони України пропозиції щодо її формування та уточнення, в тому числі, з урахуванням положень NIS 2 Директиви; визначає пріоритети, розробляє концептуальні засади та вносить пропозиції	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Президентові України 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»;		
173	«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»;	**-178- Н.д. Василевська-Смаглюк О. М. (р.к. №302)** В абзаці третьому підпункту 4 пункту 4 слова "крім об'єктів критичної інфраструктури у банківській системі України” замінити словами “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”. **-179- Н.д. Федієнко О. П. (р.к. №89)** «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**~~ **затверджує порядок** 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	Відхилено Відхилено	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, контрозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності»;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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»;		
		-180- Н.д. Федієнко О. П. (р.к. №89) 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 систем та** об’єктів ~~критичної інфраструктури у банківській системі 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), зокрема шляхом прийняття постанов та розпоряджень; встановлює порядок взаємодії суб'єктів національної системи реагування, їх взаємодії із суб'єктами	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		забезпечення кібербезпеки, з правоохоронними органами та суб'єктами оперативно-розшукової діяльності.		
		-181- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		«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 ступеню 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»;		
174	пункт 7 частини четвертої викласти в такій редакції:			пункт 7 частини четвертої викласти в такій редакції:
175	«7) оператори критичної інфраструктури та власники/розпорядники критичної інформаційної інфраструктури»;	**-182- Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Івченко В. Є. (р.к. №185)** У четвертому абзаці підпункту 4, пункту 4, розділу І законопроекту перед словами	Відхилено	«7) оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури»;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«критичної інформаційної інфраструктури» доповнити словом «об’єктів»; *Обґрунтування*: Пропущено слово «об’єктів» - законопроєкт за текстом використовує саме таке словосполучення як «власники/розпорядники об'єктів критичної інформаційної інфраструктури» (наприклад див. зміни до ст.6 цього ж закону нижче). Тому пропонується доповнити словом «об’єктів» перед словами «критичної інформаційної інфраструктури».		
176	5) доповнити статтею 5^1 такого змісту:			5) доповнити статтею 5^1 такого змісту:
177	«Стаття 5^1. Підрозділи з кіберзахисту, керівники із кіберзахисту			«Стаття 5^1. Підрозділи з кіберзахисту, керівники з кіберзахисту
178	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.	**-183- Н.д. Сірко Ю. Л. (р.к. №210)** 1. В органах державної влади, державних органах, державних підприємствах, установах та організаціях, органах місцевого самоврядування, 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.	Відхилено	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.
		-184- Н.д. Сірко Ю. Л. (р.к. №210) 1. В органах державної влади, державних органах, державних підприємствах, установах та організаціях, органах місцевого самоврядування, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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.		
179	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).	**-185- Н.д. Федієнко О. П. (р.к. №89)** Власники/розпорядники об'єктів критичної інформаційної інфраструктури, **в яких оброблятиметься інформація, власниками/розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування**, 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).	Відхилено	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.
180	Призначення керівника із кіберзахисту на посаду в органах державної влади, а також відповідальної особи, яка виконує функції та завдання керівника із кіберзахисту в юридичних особах, що є власниками/розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності, в порядку, затвердженому Кабінетом Міністрів України, погоджується Державною службою спеціального зв'язку та захисту інформації України після перевірки, проведеної Службою безпеки України в межах її повноважень.	**-186- Н.д. Пузійчук А. В. (р.к. №182)** Абзац п'ятий підпункту 5 пункту 4 розділу I виключити.	Відхилено	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.
		-187- Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Івченко В. Є. (р.к. №185) 1. У п'ятому абзаці підпункту 5, пункту 4, розділу I законопроекту перед словами «в порядку, затвердженому Кабінетом Міністрів України,» доповнити словами та символами «державної форми власності,»;	Відхилено	
		-188- Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Івченко В. Є. (р.к. №185) П'ятий абзац підпункту 5, пункту 4, розділу I законопроекту доповнити наступним реченням «Про призначення керівника із кіберзахисту на посаду в юридичних особах, що власниками/розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності приватної форми	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		власності, повідомляється Державній службі спеціального зв'язку та захисту інформації України до початку роботи працівника на посаді керівника із кіберзахисту.»; *Обґрунтування*: Зважаючи на дефіцит профільних експертів у галузі кібербезпеки, а також на кількість спроб кібератак на державні та приватні компанії, додаткова перевірка кандидата на посаду керівника кібербезпеки з боку державних органів в приватних компаніях може призвести: • відмов фахівців та/або діючих співробітників проходити перевірки та як наслідок підприємства об'єктів критичної інформаційної інфраструктури I і II категорій критичності залишаться без керівника функції, що в перспективі може призвести до негативних наслідків, • формального призначення керівника «з бездоганною репутацією» на посаду керівника з кібербезпеки з метою виконання регуляторних вимог для підприємств об'єктів критичної інформаційної інфраструктури I і II категорій критичності, але фактичного виконання обов'язків такого керівника іншими особами. Враховуючи зазначене пропонується: 1) встановити обов'язкову попередню перевірку для власників/розпорядників ОКІІ державної форми власності, 2) для приватних власників/розпорядників ОКІІ необхідним буде повідомлення Держспецзв'язку про призначення керівника до початку його роботи на посаді (фактично зберігається можливість здійснити перевірку такої особи у порядку виконання Закону України «Про контррозвідувальну діяльність», у тому числі негласно).		
		-189- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		У випадку призначення керівника із кіберзахисту на відповідну посаду в органах державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування він повинен мати сертифікат від Державної служби зайнятості відповідно до цього Закону		
		-190- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		У випадку призначення керівника із кіберзахисту на відповідну посаду в органах державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування він повинен мати сертифікат від Державної служби зайнятості відповідно до цього Закону		
		-191- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		Призначення керівника із кіберзахисту на посаду в органах державної влади (крім Міністерства оборони України, Збройних Сил України, Державної спеціальної служби транспорту, Служби безпеки України та розвідувальних органів України), а також відповідальної особи, яка виконує функції та завдання керівника із кіберзахисту в юридичних особах, що власниками/розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності, в порядку, затвердженому Кабінетом Міністрів України, погоджується Державною службою спеціального зв'язку та захисту інформації України після отримання позитивного висновку за результатами перевірки, проведеної Службою безпеки України в межах її повноважень.		
		-192- Н.д. Кучеренко О. Ю. (р.к. №179)	Відхилено	
		У п'ятому абзаці підпункту 5 пункту 4 розділу I законопроекту перед словами «в порядку, затвердженому Кабінетом Міністрів		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		України,» доповнити словами та символами «державної форми власності,»		
		-193- Н.д. Кучеренко О. Ю. (р.к. №179) П’ятий абзац підпункту 5 пункту 4 розділу І законопроекту доповнити наступним реченням «Про призначення керівника із кіберзахисту на посаду в юридичних особах, які є власниками або розпорядниками об’єктів критичної інформаційної інфраструктури I і II категорій критичності приватної форми власності, повідомляється Державній службі спеціального зв’язку та захисту інформації України не пізніше ніж за 5 робочих днів до початку роботи працівника на посаді керівника із кіберзахисту.»; *Обґрунтування*: Зважаючи на дефіцит профільних експертів у галузі кібербезпеки, а також на кількість спроб кібератак на державні та приватні компанії, додаткова перевірка кандидата на посаду керівника кібербезпеки з боку державних органів в приватних компаніях може призвести: • відмов фахівців та/або діючих співробітників проходити перевірки та як наслідок підприємства об’єктів критичної інформаційної інфраструктури I і II категорій критичності залишаться без керівника функції, що в перспективі може призвести до негативних наслідків, • формального призначення керівника «з бездоганною репутацією» на посаду керівника з кібербезпеки з метою виконання регуляторних вимог для підприємств об’єктів критичної інформаційної інфраструктури I і II категорій критичності, але фактичного виконання обов’язків такого керівника іншими особами. Враховуючи зазначене пропонується: 1) встановити обов’язкову попередню перевірку для власників/розпорядників ОКІІ державної форми власності,	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		2) для приватних власників/розпорядників ОКІІ необхідним буде повідомлення Держспецзв'язку про призначення керівника за 5 робочих днів до початку його роботи на посаді (фактично зберігається можливість здійснити перевірку такої особи у порядку виконання Закону України «Про контррозвідувальну діяльність», у тому числі негласно).		
		-194- Н.д. Буймістер Л. А. (р.к. №424)	Відхилено	
		У п'ятому абзаці підпункту 5, пункту 4, розділу І законопроєкту перед словами «в порядку, затвердженому Кабінетом Міністрів України,» доповнити словами та символами «державної форми власності,»;		
		-195- Н.д. Приходько Б. В. (р.к. №411)	Відхилено	
		Абзац 5 підпункту 5 пункту 4 Розділу І проекту закону виключити.		
181		**-196- Н.д. Кучеренко О. Ю. (р.к. №179)**	Відхилено	
		Після абзацу п'ятого підпункту 5 пункту 4 розділу І законопроекту доповнити абзацем такого змісту: «Відмова Державної служби спеціального зв'язку та захисту інформації України від погодження призначення керівника із кіберзахисту на посаду має бути вмотивована та викладена у письмовому вигляді з посиланням на конкретні вимоги, затверджені відповідно до частини третьої цієї статті, яким не відповідає кандидат на посаду керівника із кіберзахисту. Така відмова має бути підписана Головою Державної служби спеціального зв'язку та захисту інформації України і може бути оскаржена у судовому порядку.» *Обґрунтування:* Відмова від погодження призначення керівника із кіберзахисту має бути вмотивованою та посилатись на конкретні вимоги, які висуваються до такого керівника і яким кандидат на цю посаду не відповідає. В іншому випадку		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Держспецзв'язку матиме нічим не обмежену можливість безпідставно відмовляти у погодженні кандидатів, у тому числі з корупційних мотивів. Також з метою контролю та виключення останнього ризику, мотивована відмова від погодження має підписуватись першим керівником (головою) Держспецзв'язку.		
		-197- Н.д. Буймістер Л. А. (р.к. №424) 1) Після абзацу п'ятого підпункту 5, пункту 4, розділу І законопроєкту доповнити новими абзацами такого змісту: «Служба безпеки України, в межах її повноважень, здійснює перевірку претендента на посаду керівника із кіберзахисту виключно щодо наступних питань: - наявність у претендента на посаду допуску до державної таємниці, якщо такий допуск необхідний для зайняття посади керівника із кіберзахисту в органах державної влади, - наявності у претендента на посаду афілійованих осіб з числа осіб щодо яких застосовано санкції відповідно до Закону України «Про санкції», - наявності у претендента на посаду не знятої або не погашеної судимості за корупційні кримінальні правопорушення або кримінальні правопорушення, пов'язані з корупцією, злочини проти основ національної безпеки України, кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, кримінальні правопорушення передбачені статтями 328 – 330, 357 - 360 Кримінального кодексу України. Результати перевірки Служби безпеки України додаються до письмового погодження або письмової відмови Державної	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		служби спеціального зв'язку та захисту інформації України від погодження призначення керівника із кіберзахисту на посаду. Відмова від погодження має бути вмотивована та ґрунтуватись на конкретних фактах невідповідності претендента на посаду затвердженим загальним вимогам які висуваються до керівників із кіберзахисту. Відмова від погодження може бути оскаржена у судовому порядку.» *Обґрунтування*: Застосування вимоги про попереднє погодження керівників із кіберзахисту у тому числі для приватних компаній фактично буде зовнішнім управлінням кадровою політикою підприємства. Відповідно має бути залишена така умова тільки для державного сектора. Крім того необхідним є встановлення чіткого переліку питань, які має перевіряти СБУ та, відповідно, які будуть слугувати підставою для не погодження претендента на посаду. Так доречним буде проводити перевірку з питань допуску до держаної таємниці, наявності афілійованих підсанкційних осіб, наявність судимості щодо злочинів/кримінальних правопорушень які безпосередньо можуть стосуватись характеру виконуваної роботи керівника з кіберзахисту. У випадку ж невідповідності претендента існуючим вимогам – Держспецзв'язку має надати вмотивовану письмову відмову у якій має бути конкретно зазначено причини відмови/невідповідності.		
182	У разі ненадання Державною службою спеціального зв'язку та захисту інформації України протягом одного календарного місяця з дня отримання нею відповідного звернення мотивованої відповіді щодо непогодження призначення керівника із кіберзахисту із зазначенням підстави,	**-198- Н.д. Пузійчук А. В. (р.к. №182)** Абзац шостий підпункту 5 пункту 4 розділу І виключити.	Відхилено	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
		-199- Н.д. Сірко Ю. Л. (р.к. №210) виключити	Відхилено	
		-200- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	визначеної відповідним порядком, таке погодження вважається наданим.	виключити **-201- Н.д. Приходько Б. В. (р.к. №411)**	Відхилено	відповідним порядком, таке погодження вважається наданим.
		Абзац 6 підпункту 5 пункту 4 Розділу I проекту закону виключити. **-202- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	
183	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.	В абзаці сьомому підпункту 5 пункту 4 розділу I слова «здійснюють керівництво, координацію та контроль з питань» замінити словами «забезпечують організацію та здійснення заходів». **-203- Н.д. Сірко Ю. Л. (р.к. №210)** 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, державних органів, державних підприємств, установ та організацій, органів місцевого самоврядування 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.	Відхилено	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.
		-204- Н.д. Сірко Ю. Л. (р.к. №210) 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, державних органів, державних підприємств, установ та організацій, органів місцевого	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		самоврядування органу місцевого самоврядування, що є власником або розпорядником інформаційних, електронних комунікаційних та інформаційнокомунікаційних 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		
184	3. Методичні рекомендації щодо типових вимог до підрозділів з кіберзахисту, загальних вимог 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, надаються Державною службою спеціального зв'язку та захисту інформації України»;	**-205- Н.д. Пузійчук А. В. (р.к. №182)** В абзаці восьмому підпункту 5 пункту 4 розділу I слова «надаються Державною службою спеціального зв'язку та захисту інформації України» замінити словами «затверджуються Кабінетом Міністрів України». **-206- Н.д. Кучеренко О. Ю. (р.к. №179)** В абзаці восьмому підпункту 5 пункту 4 розділу I слова «надаються Державною службою спеціального зв'язку та захисту інформації України» замінити словами «затверджуються Кабінетом Міністрів України». *Обгрунтування:* Використання слова «надаються» породжує правову невизначеність – незрозуміло кому надаються, як надаються, у які строки надаються, у яких випадках тощо. Методичні рекомендації та вимоги мають бути чіткими та однозначними, такими, що можуть бути застосовані неодноразово відносно різних суб’єктів та об’єктів. З огляду на це вони мають носити нормативний характер та, відповідно, «затверджуватись». А враховуючи, що Держспецзв’язку матиме повноваження давати оцінку щодо відповідності та/або невідповідності окремих суб’єктів (їх дій) таким методичним рекомендаціям та вимогам – необхідним є затвердження таких нормативних документів	Відхилено Відхилено	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»;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		вищим, ніж Держспецзв'язку, органом влади. Це також дозволить додержати принципу стримувань та противаг, особливо в контексті можливості Держспецзв'язку не погоджувати призначення керівників з кіберзахисту у випадку їх невідповідності «загальним вимогам до керівників із кіберзахисту».		
		-207- Н.д. Буймістер Л. А. (р.к. №424)	Відхилено	
		1) В абзаці восьмому підпункту 5 пункту 4 розділу I слова «надаються Державною службою спеціального зв'язку та захисту інформації України» замінити словами «затверджуються Кабінетом Міністрів України». *Обґрунтування*: Методичні рекомендації та вимоги повинні бути чіткими, однозначними та придатними для багаторазового застосування до різних суб'єктів та об'єктів – тому вони мають мати нормативний характер та, відповідно, затверджуватись, а не у невизначений спосіб «надаватись» незрозуміло якому колу суб'єктів та як відповідь на що (на запит індивідуально або необмеженому колу на періодичній основі). Також враховуючи, що законопроєкт дозволить Держспецзв'язку застосовувати заходи впливу до тих, хто не додержується таких рекомендацій – доцільно забезпечити додержання принципу стримувань та противаг і, відповідно, затверджувати рекомендації вищим органом в системі органів виконавчої влади.		
185	6) статтю 6 викласти в такій редакції:	**-208- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута**	Відхилено	6) статтю 6 викласти в такій редакції:

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176) Підпункт 6) пункту 4 Розділу I викласти в такій редакції: «статтю 6 викласти в такій редакції: «Стаття 6. Кіберзахист критичної інфраструктури 1. Віднесення об'єктів до об'єктів критичної інфраструктури та формування Реєстру об'єктів критичної інфраструктури здійснюються відповідно до Закону України "Про критичну інфраструктуру". 2. Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Національним координаційним центром кібербезпеки, а щодо 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 - Національним банком України. 3. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України. Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється Національним координаційним центром кібербезпеки на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій. 4. Посадові особи операторів критичної інфраструктури, власників/розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечити дотримання вимог з кіберзахисту, в установленному порядку 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. 5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України "Про захист персональних даних".».		
186	«Стаття 6. Кіберзахист критичної інфраструктури	**-209- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163)** Статтю 6 викласти в такій редакції: 1. Віднесення об'єктів до об'єктів критичної інфраструктури та формування Реєстру об'єктів критичної інфраструктури здійснюються відповідно до Закону України "Про критичну інфраструктуру". 2. Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Національним координаційним центром кібербезпеки, а щодо банків, інших осіб, що	Відхилено	«Стаття 6. Кіберзахист критичної інфраструктури

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 - Національним банком України. 3. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України. Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури здійснюється Національним координаційним центром кібербезпеки на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов’язковим залученням представників основних суб’єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій. 4. Посадові особи операторів критичної інфраструктури, власників/розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечити дотримання вимог з кіберзахисту, в установленному порядку 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. 5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України "Про захист персональних даних".		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
187	1. Посадові особи операторів критичної інфраструктури, власників/розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечити дотримання вимог з кіберзахисту, в установленому порядку 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.	**-210- Н.д. Сірко Ю. Л. (р.к. №210)** 1. Посадові особи операторів критичної інфраструктури, власників/розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечити дотримання вимог з кіберзахисту, в установленому порядку повідомляти про інциденти кібербезпеки, кібератаки, виключно для суб'єктів господарювання державного та комунального секторів економіки, виконувати інші зобов'язання щодо захисту інформації та кіберзахисту відповідно до законодавства, а також несуть відповідальність за невиконання таких вимог згідно із законом.	Відхилено	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.
		-211- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 3 пункту 6 частини 4 розділу I законопроекту викласти у наступній редакції: «1. Посадові особи операторів критичної інфраструктури, власників/розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечити дотримання вимог з кіберзахисту, в установленому порядку повідомляти про кіберінциденти, кібератаки, виконувати інші зобов'язання щодо захисту інформації та кіберзахисту відповідно до законодавства, а також несуть відповідальність за невиконання таких вимог згідно із законом.»	Відхилено	
		-212- Н.д. Сірко Ю. Л. (р.к. №210) 1. Посадові особи операторів критичної інфраструктури, власників/розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечити дотримання вимог з кіберзахисту, в установленому порядку повідомляти про інциденти кібербезпеки, кібератаки, виключно для суб'єктів господарювання	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		державного та комунального секторів економіки, виконувати інші зобов'язання щодо захисту інформації та кіберзахисту відповідно до законодавства, а також несуть відповідальність за невиконання таких вимог згідно із законом.		
188	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 інфрастраструктури або об’єктів критичної інформаційної інфраструктури III і IV категорій критичності), визначених Державною службою спеціального зв'язку та захисту інформації України»;	**-213- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 4 пункту 6 частини 4 розділу I законопроекту викласти у наступній редакції: «2. Оцінювання ступеню 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 ступеню кіберзахисту, загальних вимог до суб'єктів оцінювання ступеню кіберзахисту (крім оцінювання ступеню кіберзахисту щодо об’єктів критичної інфрастраструктури або об’єктів критичної інформаційної інфраструктури III і IV категорій критичності), визначених Державною службою спеціального зв'язку та захисту інформації України»;	Відхилено	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 інфрастраструктури або об’єктів критичної інформаційної інфраструктури III і IV категорій критичності), визначених Державною службою спеціального зв'язку та захисту інформації України»;
189	7) у статті 8:			7) у статті 8:
190	у частині другій:			у частині другій:
191	абзац перший, пункти 1-3 викласти в такій редакції	**-214- Н.д. Василевська-Смаглюк О. М. (р.к. №302)** В абзаці третьому підпункту 7 пункту 4 замінити цифри "1-3" цифрами "1-3, 6".	Відхилено	абзац перший, пункти 1-3 та 6 викласти в такій редакції:
192	«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	**-215- Н.д. Пузійчук А. В. (р.к. №182)** В абзаці четвертому підпункту 7 пункту 4 розділу I слова та знак «Міністерство закордонних справ України,» виключити.	Відхилено	«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	України, Національний банк України, Міністерство закордонних справ України, які відповідно до Конституції і законів України виконують у встановленому порядку такі основні завдання:			органи України, Національний банк України, Міністерство закордонних справ України, які відповідно до Конституції і законів України виконують у встановленому порядку такі основні завдання:
193	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 у кіберпросторі, кіберзахисту критичної інфраструктури; здійснює державний контроль у цих сферах; 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	**-216- Н.д. Сірко Ю. Л. (р.к. №210)** слова "Державна служба спеціального зв'язку та захисту інформації України" замінити словами"Центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв’язку, захисту інформації" у відповідних відмінках по тексту Закону. **-217- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 5 пункту 7 частини 4 розділу I законопроекту викласти у наступній редакції: «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 у кіберпросторі, кіберзахисту критичної інфраструктури; здійснює державний контроль у цих 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	Відхилено Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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;	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 (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 ступеню кіберзахисту, встановлює вимоги до суб'єктів оцінювання ступеню 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;»		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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-218- Н.д. Сірко Ю. Л. (р.к. №210) слова "Державна служба спеціального зв'язку та захисту інформації України" замінити словами"Центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації" у відповідних відмінках по тексту Закону.	Відхилено	
194	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;			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;
195	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	**-219- Н.д. Федієнко О. П. (р.к. №89)** 3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки України, миру і безпеки людства, **а також терористичної спрямованості, які 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	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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»;	інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури;		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»;
		-220- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)	Відхилено	
		Абзац сьомий підпункту 7 пункту 4 розділу І проекту Закону викласти в такій редакції: «Служба безпеки України у відповідності до законів України здійснює: запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки України, миру і безпеки людства, а також терористичної спрямованості, які 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	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки»;		
196		**-221- Н.д. Василевська-Смаглюк О. М. (р.к. №302)** Підпункт 7 пункту 4 доповнити абзацом восьмим такого змісту: “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 (уключаючи команду реагування на кіберінциденти, пов’язані з комп’ютерною безпекою 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	Відхилено	«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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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”.		та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг»;
		-222- Н.д. Федієнко О. П. (р.к. №89)	Відхилено	
		пункт 6) викласти в такій редакції 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 **(уключаючи команду реагування на кіберінциденти, пов’язані з комп’ютерною безпекою 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; **установлює вимоги до проведення аудиту інформаційної безпеки в банках, інших**		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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.		
197	доповнити пунктом 7 такого змісту:	**-223- Н.д. Пузійчук А. В. (р.к. №182)** Абзац восьмий підпункту 7 пункту 4 розділу I виключити.	Відхилено	доповнити пунктом 7 такого змісту:
198	«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	**-224- Н.д. Пузійчук А. В. (р.к. №182)** Абзац дев’ятий підпункту 7 пункту 4 розділу I виключити. **-225- Н.д. Сірко Ю. Л. (р.к. №210)** слова "узгоджених із ключовими міжнародними партнерами заходів, замінити словами" розвитку та зміцненню міжнародного співробітництва,"- слова "у міжнародних організаціях" замінити словами "з міжнародними підприємствами, установами, організаціями, фондами тощо" **-226- Н.д. Сірко Ю. Л. (р.к. №210)** слова "узгоджених із ключовими міжнародними партнерами заходів, замінити словами" розвитку та зміцненню міжнародного співробітництва," слова "у міжнародних організаціях" замінити словами "з міжнародними підприємствами, установами, організаціями, фондами тощо"	Відхилено Відхилено Відхилено	«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 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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	деструктивну кіберактивність, виконує інші завдання відповідно до закону»;			заходів у відповідь на деструктивну кіберактивність; виконує інші завдання відповідно до закону»;
199	у частині третій:			у частині третій:
200	пункти 1-2 викласти в такій редакції:			пункти 1 і 2 викласти в такій редакції:
201	«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;			«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;
202	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»;			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»;
203	пункт 3 виключити;	**-227- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)** Абзац п’ятнадцятий підпункту 7) пункту 4 Розділу І викласти в такій редакції: «3) встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію,	Відхилено	пункт 3 виключити;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури;».		
		-228- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Підпункт 3 частини 3 статті 8 викласти в такій редакції: 3) встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури; Обгрунтування (повторення поправки №149, відхиленої до другого читання): Враховуючи те, що вітчизняна інформаційна система знаходиться під постійною загрозою хакерського втручання, доцільно зберегти одним із завдань функціонування національної системи кібербезпеки встановлення вимог до інформаційної безпеки критичної інформаційної інфраструктури як галузевого та міжгалузевого комплекса, які закладаються прямо на етапі створення та введення в експлуатацію відповідних об'єктів. Особливо це буде важливим під час відбудови зруйнованого, тому що відбудоване має бути не таким самим, не гіршим за попереднє, а набагато кращим.	Відхилено	
204	пункти 4-8 викласти в такій редакції:			пункти 4-8 викласти в такій редакції:
205	«4) впровадження заходів стимулювання розвитку та конкурентноспроможності	**-229- Н.д. Сірко Ю. Л. (р.к. №210)** «4) впровадження заходів стимулювання розвитку та конкурентноспроможності	Відхилено	«4) запровадження заходів стимулювання розвитку та

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	індустрії послуг та продуктів в сфері кібербезпеки в Україні;	індустрії послуг та продуктів в сфері кібербезпеки в Україні відповідно до законодавства України;		конкурентноспроможності індустрії послуг та продуктів у сфері кібербезпеки в Україні;
		-230- Н.д. Сірко Ю. Л. (р.к. №210) «4) впровадження заходів стимулювання розвитку та конкурентноспроможності індустрії послуг та продуктів в сфері кібербезпеки в Україні відповідно до законодавства України;	Відхилено	
206	5) залучення експертного потенціалу приватного сектору, наукових установ, професійних та громадських об’єднань до розробки проектів щодо стратегічного планування, державної політики, розробки нормативно-правових актів, нормативних документів, стандартів та методичних рекомендацій у сфері кібербезпеки;			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;
207	6) 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;	**-231- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	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;
		6) 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 суб'єктів господарювання державного та комунального секторів економіки;		
		-232- Н.д. Сірко Ю. Л. (р.к. №210) 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	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		ресурси категорій службова інформація та державна таємниця, а також на об’єктах критичної інфраструктури суб'єктів господарювання державного та комунального секторів економіки;		
208	7) функціонування системи оцінювання стану кіберзахисту публічного сектору та критичної інфраструктури;	**-233- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	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;
		функціонування системи оцінювання стану кіберзахисту державного сектору та державної критичної інфраструктури;		
		-234- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)	Відхилено	
		Абзац двадцятий підпункту 7) пункту 4 Розділу I викласти в такій редакції: «7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту в галузях публічного сектору та критичної інфраструктури;».		
		-235- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 19 пункту 7 частини 4 розділу I законопроекту викласти у наступній редакції: «7) функціонування системи оцінювання ступеню кіберзахисту публічного сектору та критичної інфраструктури;»		
		-236- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д.	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)		
		Абзац дев'ятнадцятий підпункту 7 пункту 4 розділу І проекту Закону викласти в такій редакції: «7) функціонування системи оцінювання стану кіберзахисту в органах державної влади, державних органах, органах місцевого самоврядування, державних підприємствах, господарських товариствах, 50 відсотків і більше акцій (часток) якого належать державі, державних наукових установах та закладах вищої освіти, а також щодо об'єктів критичної інфраструктури»;	Народні депутати України - члени Комітету	
		-237- Н.д. Сірко Ю. Л. (р.к. №210) функціонування системи оцінювання стану кіберзахисту державного сектору та державної критичної інфраструктури	Відхилено	
		-238- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Цимбалюк М. М. (р.к. №176), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Дубіль В. О. (р.к. №171), Н.д. Соколов М. В. (р.к. №452), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Немиря Г. М. (р.к. №169), Н.д. Тарута С. О. (р.к. №163) Підпункт 7 частини 3 статті 8 викласти в такій редакції: 7) функціонування системи аудиту інформаційної безпеки та 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,	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		щодо об'єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури; Обгрунтування: Для того, щоб забезпечити максимально можливий рівень захисту, який необхідний в критичній інфраструктурі, потрібна комплексна оцінка, яка можлива лише в форматі аудита і лише спеціально підготовленими фахівцями у відповідній галузі. З огляду на це, доцільно зберегти норму про функціонування системи аудиту інформаційної безпеки.		
209	8) розвитку мережі команд реагування на інциденти кібербезпеки, кіберзагрози на національному, галузевому та регіональному рівнях, в тому числі, із залученням приватних команд реагування»;	**-239- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 20 пункту 7 частини 4 розділу I законопроекту викласти у наступній редакції: «8) розвитку мережі команд реагування на кіберінциденти, кіберзагрози на національному, галузевому та регіональному рівнях, в тому числі, із залученням приватних команд реагування»;	Відхилено	8) розвитку мережі команд реагування на кіберінциденти, кіберзагрози на національному, галузевому та регіональному рівнях, у тому числі із залученням приватних команд реагування»;
210	пункт 10 виключити;			пункт 10 виключити;
211	пункти 12, 15 та 17 викласти в такій редакції:			пункти 12, 15 і 17 викласти в такій редакції:
212	«12) функціонування національних систем реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та обміну інформацією про інциденти кібербезпеки»;	**-240- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 23 пункту 7 частини 4 розділу I законопроекту викласти у наступній редакції: «12) функціонування національних систем реагування на кіберінциденти, кібератаки, кіберзагрози та обміну інформацією про кіберінциденти»;	Відхилено	«12) функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози»;
213	«15) впровадження організаційно-технічної моделі кіберзахисту національної системи кібербезпеки»;			«15) впровадження організаційно-технічної моделі кіберзахисту національної системи кібербезпеки»;
214		**-241- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	«17) застосування інструментів та механізмів державно-приватної взаємодії для виконання завдань в сфері кібербезпеки, включаючи, але не обмежуючись, функціонування систем обміну інформацією щодо кіберзагроз, кібератак та кіберінцидентів, заходів кіберзахисту та захисту інформації, створення колективної системи або індивідуальних програм моніторингу, аналізу, координації дій, в тому числі, при реагуванні на кіберінциденти, усуненні наслідків та здійсненні заходів з відновлення, організації та здійсненні заходів з підготовки кадрів, підвищення знань та навичок, проведення навчань, створенні та реалізації освітніх і просвітницьких програм, в здійсненні досліджень та нових розробок, забезпеченні функціонування центрів кібербезпеки та їх сервісів, підготовці програмних документів та нормативно-правових актів у сфері кібербезпеки, а також для вирішення інших завдань в сфері кібербезпеки, що можуть бути вирішені через державно-приватну взаємодію»;	«17) застосування інструментів та механізмів державно-приватної взаємодії для виконання завдань в сфері кібербезпеки, включаючи, але не обмежуючись, функціонування систем обміну інформацією щодо кіберзагроз, кібератак та кіберінцидентів, заходів кіберзахисту та захисту інформації, створення колективної системи або індивідуальних програм моніторингу, аналізу, координації дій, в тому числі, при реагуванні на кіберінциденти, усуненні наслідків та здійсненні заходів з відновлення, організації та здійсненні заходів з підготовки кадрів, підвищення знань та навичок, проведення навчань, створенні та реалізації освітніх і просвітницьких програм, в здійсненні досліджень та нових розробок, забезпеченні функціонування центрів кібербезпеки та їх сервісів, підготовці програмних документів та нормативно-правових актів у сфері кібербезпеки, а також для вирішення інших завдань в сфері кібербезпеки, що можуть бути вирішені через державно-приватну взаємодію виключно для суб'єктів господарювання державного та комунального секторів економіки;		«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»;
		-242- Н.д. Сірко Ю. Л. (р.к. №210) застосування інструментів та механізмів державно-приватної взаємодії для виконання завдань в сфері кібербезпеки, включаючи, але не обмежуючись, функціонування систем обміну інформацією щодо кіберзагроз, кібератак та кіберінцидентів, заходів кіберзахисту та захисту інформації, створення колективної системи або індивідуальних програм моніторингу, аналізу, координації дій, в тому числі, при реагуванні на кіберінциденти, усуненні наслідків та здійсненні заходів з відновлення, організації та здійсненні заходів з підготовки кадрів, підвищення знань та навичок, проведення	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		навчань, створенні та реалізації освітніх і просвітницьких програм, в здійсненні досліджень та нових розробок, забезпеченні функціонування центрів кібербезпеки та їх сервісів, підготовці програмних документів та нормативноправових актів у сфері кібербезпеки, а також для вирішення інших завдань в сфері кібербезпеки, що можуть бути вирішені через державно-приватну взаємодію виключно для суб'єктів господарювання державного та комунального секторів економіки;		
215	Доповнити пунктом 26 такого змісту:	**-243- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)** У абзаці двадцять шостому підпункту 7 пункту 4 розділу I проекту Закону цифру «26» замінити цифрами «26-27».	Відхилено Народні депутати України - члени Комітету	доповнити пунктами 26 і 27 такого змісту:
216	«26) планування витрат та здійснення відповідного фінансування органами державної влади, державними органами, органами місцевого самоврядування, операторами критичної інфраструктури, власниками/розпорядниками об’єктів критичної інформаційної інфраструктури заходів кіберзахисту, передбачених законодавством»;	**-244- Н.д. Пузійчук А. В. (р.к. №182)** Абзац двадцять сьомий підпункту 7 пункту 4 розділу I викласти в такій редакції: «26) фінансування заходів кіберзахисту відповідно до законодавства».	Відхилено	«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;
217		**-245- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В.**	Відхилено	27) проведення інструктажів та систематичних тренінгів щодо кібергігієни для членів уряду України, народних депутатів України, працівників патронатних служб, депутатів місцевих рад, державних

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)		служб овців, 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»;
		Підпункт 7 пункту 4 розділу І проекту Закону після абзацу двадцять сьомому доповнити новим абзацом такого змісту: «27) проведення особистих інструктажів та систематичних тренінгів щодо кібергігієни 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, порядок та систематичність яких встановлюється Кабінетом міністрів України».	Народні депутати України - члени Комітету	
218	частину п’яту викласти в такій редакції:			частину п’яту викласти в такій редакції:
219	«5. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення, функціонування та розвиток:	**-246- Н.д. Федієнко О. П. (р.к. №89)** 5. Впровадження організаційно-технічної моделі **кіберзахисту** як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який … …	Відхилено	«5. Впровадження організаційно-технічної моделі кіберзахисту як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення, функціонування та розвиток:
220	системи захищеного доступу державних органів до мережі Інтернет;			1) системи захищеного доступу державних органів до мережі Інтернет;
221	Національного центру резервування державних інформаційних ресурсів;			2) Національного центру резервування державних інформаційних ресурсів;
222	Центру антивірусного захисту інформації;			3) Центру антивірусного захисту інформації;
223	системи виявлення вразливостей і реагування на інциденти кібербезпеки, кібератаки та кіберзагрози щодо об’єктів кіберзахисту, а також організовує та	**-247- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	4) системи виявлення вразливостей, а також здійснення для органів державної влади, державних органів, органів місцевого самоврядування, власників або

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	проводить систематичні навчання із 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 критичної інформаційної інфраструктури»;	Абзац 33 пункту 7 частини 4 розділу I законопроекту викласти у наступній редакції: «системи виявлення вразливостей і реагування на кіберінциденти, кібератаки та кіберзагрози щодо об'єктів кіберзахисту, а також організовує та проводить систематичні навчання із 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 ступеню кіберзахисту критичної інформаційної інфраструктури»		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»;
224		**-248- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)** Підпункт 7 пункту 4 розділу I проекту Закону після абзацу тридцять третього доповнити новим абзацом такого змісту:	Відхилено Народні депутати України - члени Комітету	пункт 4 частини шостої виключити;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«пункт 4 частини шостої виключити»;		
225	доповнити частиною сьомою такого змісту:			доповнити частиною сьомою такого змісту:
226	«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.	**-249- Н.д. Сірко Ю. Л. (р.к. №210)** «7. Розроблення та застосування 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.	Відхилено	«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.
		-250- Н.д. Сірко Ю. Л. (р.к. №210) «7. Розроблення та застосування 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	Відхилено	
227	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	**-251- Н.д. Мамка Г. М. (р.к. №147), Н.д. Макаренко М. В. (р.к. №153), Н.д. Борт В. П. (р.к. №152), Н.д. Ларін С. М. (р.к. №132), Н.д. Чорний В. І. (р.к. №151), Н.д. Іоффе Ю. Я. (р.к. №136), Н.д. Німченко В. І. (р.к. №130)** Абзац другий нової частини 7 статті 8 законопроекту виключити.	Відхилено	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
		-252- Н.д. Федієнко О. П. (р.к. №89) Однією із складових такого порядку пошуку та/або виявлення потенційних	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	пошуку та виявлення вразливостей за винагороду (Bug Bounty), а також порядок узгодженого розкриття вразливостей»;	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**, а також порядок узгодженого розкриття вразливостей.		проведення програм пошуку і виявлення вразливостей за винагороду та порядок узгодженого розкриття вразливостей»;
		-253- Н.д. Бурміч А. П. (р.к. №144)	Відхилено	
		У абзаці тридцять шостому пункту 7 частини четвертої розділу I законопроекту слова «має бути порядок розроблення та проведення програм пошуку та виявлення вразливостей за винагороду (Bug Bounty)» замінити словами «може бути порядок розроблення та проведення програм пошуку та виявлення вразливостей за винагороду».		
		-254- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		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, органах державної влади, державних органів, державних підприємств, установ та організаціях, органах місцевого самоврядування має бути порядок розроблення та проведення програм пошуку та виявлення вразливостей за винагороду (Bug Bounty), а також порядок узгодженого розкриття вразливостей»;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-255- Н.д. Сірко Ю. Л. (р.к. №210) Однією із складових такого порядку пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних та інформаційнокомунікаційних 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, органах державної влади, державних органів, державних підприємств, установ та організаціях, органах місцевого самоврядування має бути порядок розроблення та проведення програм пошуку та виявлення вразливостей за винагороду (Bug Bounty), а також порядок узгодженого розкриття вразливостей»;	Відхилено	
228	8) статтю 9 викласти в такій редакції:			8) статтю 9 викласти в такій редакції:
229	«Стаття 9. Національна система реагування на інциденти кібербезпеки, кібератаки, кіберзагрози	**-256- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 2 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «Стаття 9. Національна система реагування на кіберінциденти, кібератаки, кіберзагрози»	Відхилено	«Стаття 9. Національна система реагування на кіберінциденти, кібератаки, кіберзагрози
230	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.	**-257- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 3 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «1. В Україні створюється та забезпечується функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в	Відхилено	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.

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури.»		
231	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.	**-258- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 4 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «2. Уповноваженим органом, що здійснює забезпечення функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози є Державна служба спеціального зв'язку та захисту інформації України.»	Відхилено	2. Уповноваженим органом, що забезпечує функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, є Державна служба спеціального зв'язку та захисту інформації України.
232	3. До складу національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози входять:	**-259- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 5 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «3. До складу національної системи реагування на кіберінциденти, кібератаки, кіберзагрози входять:»	Відхилено	3. До складу національної системи реагування на кіберінциденти, кібератаки, кіберзагрози входять:
233	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:	**-260- Н.д. Пузійчук А. В. (р.к. №182)** В абзаці шостому підпункту 8 пункту 4 розділу I слова та знаки «(національний CSIRT)» виключити. **-261- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 6 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «1) CERT-UA, що є національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (національний CSIRT), діяльність якої забезпечується Державною службою спеціального зв'язку та	Відхилено Відхилено	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:

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		захисту інформації України та завданнями якої є:»		
234	моніторинг, накопичення та проведення аналізу даних про інциденти кібербезпеки, кібератаки, кіберзагрози на національному, секторальному, регіональному рівнях;	**-262- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	моніторинг, накопичення та проведення аналізу даних про кіберінциденти, кібератаки, кіберзагрози на національному, галузевому, регіональному рівнях, динамічний аналіз ризиків та ситуаційної обізнаності;
		В абзаці сьомому підпункту 8 пункту 4 розділу I слово «секторальному» замінити словом «галузевому».		
		-263- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 7 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «моніторинг, накопичення та проведення аналізу даних про кіберінциденти, кібератаки, кіберзагрози на національному, секторальному, регіональному рівнях;»		
235	отримання та опрацювання у встановленому порядку обов'язкових та інших повідомлень, здійснених у межах національної системи обміну інформацією відповідно до цього Закону;			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);
236	здійснення заходів із запобігання та інформування щодо інцидентів кібербезпеки, кібератак, кіберзагроз та вразливостей;	**-264- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	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;
		Абзац 8 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «здійснення заходів із запобігання та інформування щодо кіберінцидентів, кібератак, кіберзагроз та вразливостей;»		
237	надання у встановленому порядку сервісу з реагування та рекомендацій з реагування власникам/розпорядникам інформаційних,	**-265- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	надання у встановленому порядку сервісу у зв’язку з реагуванням, рекомендацій з реагування на
		надання у встановленому порядку безоплатного сервісу з реагування та		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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);	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);		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);
		-266- Н.д. Сірко Ю. Л. (р.к. №210) надання у встановленому порядку безоплатного сервісу з реагування та рекомендацій з реагування власникам/розпорядникам інформаційних, електронних комунікаційних та інформаційнокомунікаційних 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);	Відхилено	
238				виконання функції координатора з метою узгодженого розкриття вразливостей;
239	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;	**-267- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 11 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «інформування у встановленому порядку Державної служби спеціального зв'язку та захисту інформації України про кіберінциденти, 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	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		державна таємниця, а також на об'єктах критичної інформаційної інфраструктури із зазначенням обов'язкових та/або рекомендованих заходів реагування для видання вимоги про реагування;»		рекомендованих заходів реагування для видання вимоги про реагування;
240	здійснення аналізу ризиків у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою та надання рекомендацій щодо їх усунення;	**-268- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	проведення аналізу ризиків у зв'язку з кіберінцидентом, кібератакою, кіберзагрозою та надання відповідних рекомендацій;
		Абзац 12 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «здійснення аналізу ризиків у зв'язку з кіберінциденом, кібератакою, кіберзагрозою та надання рекомендацій щодо їх усунення;»		
241	забезпечення у встановленому порядку функціонування репозитарію інформації про інциденти кібербезпеки, таксономій інцидентів кібербезпеки та їх версій;	**-269- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	забезпечення у встановленому порядку функціонування репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій;
		Абзац 13 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «забезпечення у встановленому порядку функціонування репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій;»		
242	взаємодія у встановленому порядку з іншими суб'єктами національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;	**-270- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	взаємодія у встановленому порядку з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;
		Абзац 14 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «взаємодія у встановленому порядку з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;»		
		-271- Н.д. Сірко Ю. Л. (р.к. №210) взаємодія у встановленому законодавством порядку з суб'єктами приватного сектору, у тому числі з іноземними суб'єктами господарювання, з питань реагування;	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
243	взаємодія у встановленому порядку з суб'єктами національної системи обміну інформацією про інциденти кібербезпеки, кібератаки;	**-272- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 15 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «взаємодія у встановленому порядку з суб'єктами національної системи обміну інформацією про кіберінциденти, кібератаки;»	Відхилено	взаємодія у встановленому порядку із суб'єктами національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;
244	взаємодія у встановленому порядку з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності в межах, необхідних для виконання ними повноважень, визначених законом;			взаємодія у встановленому порядку з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності в межах, необхідних для виконання ними повноважень, визначених законом;
245	виконання функцій національного контактного центру відповідно до Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS Directive);	**-273- Н.д. Пузійчук А. В. (р.к. №182)** Абзац сімнадцятий підпункту 8 пункту 4 розділу I після абревіатури «NIS» доповнити цифрою «2».	Відхилено	виконання функцій національного контактного центру відповідно до Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2 Directive);
246	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;	**-274- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 18 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «взаємодія з іноземними та міжнародними організаціями з питань реагування, зокрема в рамках участі у Форумі команд реагування на кіберінциденти FIRST із сплатою щорічних членських внесків;»	Відхилено	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;
247	взаємодія у встановленому порядку з суб'єктами приватного сектору, у тому числі з іноземними суб'єктами господарювання, з питань реагування;	**-275- Н.д. Сірко Ю. Л. (р.к. №210)** взаємодія у встановленому законодавством порядку з суб'єктами приватного сектору, у тому числі з іноземними суб'єктами господарювання, з питань реагування;	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
				органами, суб'єктами оперативно-розшукової діяльності затверджується Кабінетом Міністрів України;
248	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.	**-276- Н.д. Пузійчук А. В. (р.к. №182)** В абзаці двадцятому підпункту 8 пункту 4 розділу I слова та знаки «(далі - галузеві та регіональні CSIRT)» виключити.	Відхилено	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.
		-277- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 20 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «2) галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (далі - галузеві та регіональні CSIRT), що 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 іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України.»	Відхилено	
249	Альтернативою створення органами державної влади або органами місцевого самоврядування власних галузевих або регіональних CSIRT є залучення послуг приватних команд реагування, що можуть виконувати повністю або частково завдання галузевого або регіонального CSIRT відповідно до цього закону за умови дотримання ними вимог, встановлених для	**-278- Н.д. Пузійчук А. В. (р.к. №182)** Абзац двадцять перший підпункту 8 пункту 4 розділу I викласти в такій редакції: «Альтернативою створення органами державної влади або органами місцевого самоврядування власних галузевих або регіональних команд реагування є залучення послуг приватних команд реагування, що можуть виконувати повністю або частково завдання галузевої або регіональної команди	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	таких галузевих та регіональних CSIRT відповідно до законодавства.	реагування відповідно до цього закону за умови дотримання ними вимог, встановлених для таких галузевих та регіональних команд реагування відповідно до законодавства.».		законодавством вимог до таких галузевих, регіональних CSIRT.
250	Галузевим та регіональним CSIRT у порядку, визначеному Державною службою спеціального зв'язку та захисту інформації України, делегуються від національного CSIRT відповідні завдання щодо:	**-279- Н.д. Пузійчук А. В. (р.к. №182)** Абзац двадцять другий підпункту 8 пункту 4 розділу I викласти в такій редакції: «Галузевим та регіональним командам реагування у порядку, визначеному Державною службою спеціального зв'язку та захисту інформації України, делегуються від CERT-UA відповідні завдання щодо:».	Відхилено	Галузевим, регіональним CSIRT у порядку, визначеному Державною службою спеціального зв'язку та захисту інформації України, делегуються від національного CSIRT завдання щодо:
251	моніторингу та проведення аналізу даних про інциденти кібербезпеки, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні;	**-280- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 23 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «моніторингу та проведення аналізу даних про кіберінциденти, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні;»	Відхилено	моніторингу та проведення аналізу даних про інциденти кібербезпеки, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні, динамічного аналізу ризиків та ситуаційної обізнаності;
252	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;			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);
253	здійснення заходів із попередження та інформування щодо інцидентів кібербезпеки, кібератак, кіберзагроз та вразливостей;	**-281- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 25 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції:	Відхилено	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;

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«здійснення заходів із попередження та інформування щодо кіберінцидентів, кібератак, кіберзагроз та вразливостей;»		
254	надання у встановленому порядку сервісу з реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;	**-282- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	надання у встановленому порядку сервісу у зв’язку з реагуванням, рекомендацій з реагування на кіберінциденти, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні.
		Абзац 26 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «надання у встановленому порядку сервісу з реагування на кіберінциденти, кібератаки, кіберзагрози;»		
255	здійснення аналізу ризиків у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою та надання рекомендацій щодо їх усунення.	**-283- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	
		Абзац 27 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «здійснення аналізу ризиків у зв'язку з кіберінцидентом, кібератакою, кіберзагрозою та надання рекомендацій щодо їх усунення.»		
256	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.	**-284- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	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.
		В абзаці двадцять восьмому підпункту 8 пункту 4 розділу I абревіатуру «CSIRT» замінити словами «команди реагування».		
257	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	**-285- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	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
		абзаці двадцять дев’ятому підпункту 8 пункту 4 розділу I слова «галузевого або регіонального CSIRT» замінити словами «галузевої або регіональної команди реагування».		
		-286- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д.	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	системи обміну інформацією або національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози.	**Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 29 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «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 кіберінциденти, кібератаки, кіберзагрози.»		про кіберінциденти, кібератаки, кіберзагрози або національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.
258	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.	**-287- Н.д. Пузійчук А. В. (р.к. №182)** В абзаці тридцятому підпункту 8 пункту 4 розділу I слова та знаки «(CSIRT-NBU) є галузевим CSIRT та» виключити. **-288- Н.д. Василевська-Смаглюк О. М. (р.к. №302)** В абзаці тридцятому підпункту 8 пункту 4 слова “Центр кіберзахисту Національного банку України (CSIRT-NBU)” замінити словами “Команда реагування на кіберінциденти в банківській системі України (CSIRT-NBU), що входить до складу Центру кіберзахисту Національного банку України". **-289- Н.д. Федієнко О. П. (р.к. №89)** **Команда реагування на кіберінциденти в банківській системі України (CSIRT-NBU), що входить до складу** Центру кіберзахисту Національного банку України, 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.	Відхилено Відхилено Відхилено	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.

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-290- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 30 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «Центр кіберзахисту Національного банку України (CSIRT-NBU) є галузевим CSIRT та діє у складі національної системи обміну інформацією та національної системи реагування на кіберінциденти, кібератаки, кіберзагрози з урахуванням постанов Національного банку України в частині, що не суперечить цьому Закону.»	Відхилено	
259	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;	**-291- Н.д. Пузійчук А. В. (р.к. №182)** В абзаці тридцять першому підпункту 8 пункту 4 розділу I слова та знаки (MIL.CERT-UA) є галузевим CSIRT та» виключити.	Відхилено	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;
		-292- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 31 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «Центр кіберзахисту Міністерства оборони України (MIL.CERT-UA) є галузевим CSIRT та діє у складі національної системи обміну інформацією та національної системи реагування на кіберінциденти, кібератаки, кіберзагрози з урахуванням організаційно-розпорядчих актів Міністерства оборони України в частині, що не суперечить цьому Закону;»	Відхилено	
		-293- Н.д. Сірко Ю. Л. (р.к. №210) виключити	Відхилено	
260	3) Національна поліція України, Служба безпеки України взаємодіють у рамках національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози з іншими суб'єктами	**-294- Н.д. Пузійчук А. В. (р.к. №182)** Абзац тридцять другий підпункту 8 пункту 4 розділу I викласти в такій редакції: «3) Національна поліція України, Служба безпеки України взаємодіють у рамках	Відхилено	3) Національна поліція України, Служба безпеки України - взаємодіють у рамках національної системи реагування на кіберінциденти, кібератаки, кіберзагрози з іншими суб'єктами національної системи

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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.	національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози з іншими суб'єктами національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози в порядку та відповідно до повноважень, визначених законом.».		реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України, з урахуванням вимог цього Закону та в межах повноважень, визначених законом.
		-295- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 32 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «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 своїх повноважень, визначених законами України.»		
261	Служба безпеки України визначає особливості здійснення реагування на кіберінциденти, кібератаки, кіберзагрози у сфері державної безпеки;	**-296- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	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;
		Служба безпеки України **забезпечує функціонування системи центрів забезпечення кібербезпеки, до складу якої входять Ситуаційний центр забезпечення кібербезпеки Служби безпеки України та регіональні центри забезпечення кібербезпеки регіональних органів Служби безпеки України та завданнями якої є реагування на кризові ситуації у сфері кібербезпеки, організація, координація та безпосереднє здійснення заходів щодо протидії кібершпигунству, кібертероризму, кібердиверсіям та іншим кіберзагрозам у сфері державної безпеки.**		
		-297- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д.	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 33 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «Служба безпеки України визначає особливості здійснення реагування на кіберінциденти, кібератаки, кіберзагрози у сфері державної безпеки;»		
		-298- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)	Відхилено	
		Абзац тридцять третій підпункту 8 пункту 4 розділу I проекту Закону викласти в такій редакції: «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, іншим кіберзагрозам у сфері державної безпеки».	народні депутати України - члени Комітету	
262	4) 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	**-299- Н.д. Пузійчук А. В. (р.к. №182)**	Відхилено	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
		В абзаці тридцять четвертому підпункту 8 пункту 4 розділу I абревіатуру «CSIRT» замінити словами «команд реагування».		
		-300- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		4) приватні команди реагування можуть залучатись для надання послуг з управління		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	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.	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 Кабінетом Міністрів України.		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.
		-301- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190) Абзац 34 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «4) 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 кіберінциденти, кібератаки, кіберзагрози, у тому числі щодо обміну інформацією про кіберінциденти, кібератаки, з урахуванням вимог до організаційно-технічної спроможності та в порядку, встановленому Державною службою спеціального зв'язку та захисту інформації України.»	Відхилено	
		-302- Н.д. Сірко Ю. Л. (р.к. №210) приватні команди реагування можуть залучатись для надання послуг з управління інцидентами кібербезпеки, кібератаками,	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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 Кабінетом Міністрів України.		
263	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.	**-303- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 35 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «Суб'єкти національної системи реагування на кіберінциденти, 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.»	Відхилено	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.
264	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	**-304- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 36 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «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 кіберінциденти, кібератаки,	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	або інформація з обмеженим доступом категорій службова інформація та державна таємниця, об’єктів критичної інформаційної інфраструктури.	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.»		обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інформаційної інфраструктури, операторам критичної інфраструктури.
265	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.	**-305- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 37 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «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 кіберінцидентом, кібератакою або кіберзагрозою.»	Відхилено	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.
266	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.			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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
				спеціального зв’язку та захисту інформації України.
267	Підстави надання вимог про реагування, строк і порядок подання звіту про вжиті заходи реагування встановлюються Державною службою спеціального зв'язку та захисту інформації України;	**-306- Н.д. Сірко Ю. Л. (р.к. №210)**	Відхилено	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;
		Підстави надання вимог про реагування, строк і порядок подання звіту про вжиті заходи реагування встановлюються у порядку визначеному Кабінетом Міністрів України;		
		-307- Н.д. Сірко Ю. Л. (р.к. №210)	Відхилено	
		Підстави надання вимог про реагування, строк і порядок подання звіту про вжиті заходи реагування встановлюються у порядку визначеному Кабінетом Міністрів України;		
268	5) 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:	**-308- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	5) Національний координаційний центр кібербезпеки - здійснює загальну координацію функціонування суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.
		5) Національний координаційний центр кібербезпеки здійснює загальну координацію функціонування суб'єктів національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози.		
		-309- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 40 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «5) Національний координаційний центр кібербезпеки, що здійснює загальну координацію функціонування суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, для виконання своїх завдань має такі повноваження:»		
		-310- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к.	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		№243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)		
		Абзаци сороковий - сорок третій підпункту 8 пункту 4 розділу I проекту Закону викласти в такій редакції: «5) Національний координаційний центр кібербезпеки здійснює загальну координацію функціонування суб'єктів національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози. Суб'єкти національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, крім приватних компаній, що не здійснюють функції галузевих або регіональних CSIRT, забезпечують в порядку, визначеному для функціонування національної системи обміну інформацією про інциденти кібербезпеки, невідкладне інформування Національного координаційного центру кібербезпеки про всі значні інциденти кібербезпеки, кібератаки. Для забезпечення скоординованого, оперативного та ефективного реагування на кризову ситуацію у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою у складі Національного координаційного центру кібербезпеки функціонує постійно діюча Об'єднана група реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, до якої входять представники Національного координаційного центру кібербезпеки, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, та (за обґрунтованої необхідності) представників інших основних суб'єктів національної системи кібербезпеки. Керівництво Об'єднаної групи реагування, затвердження її персонального складу та	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		порядку роботи з урахуванням компетенції та повноважень її учасників, визначених законом здійснюється відповідним заступником керівника Національного координаційного центру кібербезпеки».		
269	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;	**-311- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	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.
		Суб'єкти Національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози забезпечують невідкладне інформування Національного координаційного центру кібербезпеки про всі значні інциденти кібербезпеки, кібератаки.		
		-312- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 41 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «проведення аналізу ступеню 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;»		
270	визначення наявності ознак кризової ситуації у зв'язку з інцидентом кібербезпеки, кібератакою, кіберзагрозою та подання інформації щодо наявності ознак кризової ситуації у кіберпросторі до Рада національної безпеки і оборони України;	**-313- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	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,
		Для забезпечення скоординованого, оперативного та ефективного реагування на інциденти кібербезпеки, кібератаки, кіберзагрози у складі Національного координаційного центру кібербезпеки функціонує постійнодіюча Об'єднана група реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, до якої входять представники Національного координаційного центру кібербезпеки, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		України, та (за обґрунтованої необхідності) представників інших основних суб'єктів національної системи кібербезпеки.		Національної поліції України та представники інших основних суб'єктів національної системи кібербезпеки (за обґрунтованої необхідності).
		-314- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 42 пункту 8 частини 4 розділу I законопроекту викласти у наступній редакції: «визначення наявності ознак кризової ситуації у зв'язку з кіберінцидентом, кібератакою, кіберзагрозою та подання інформації щодо наявності ознак кризової ситуації у кіберпросторі до Рада національної безпеки і оборони України;»		
271	здійснення координації між суб'єктами національної системи обміну інформацією та національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози;	**-315- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	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»;
		Керівництво Об'єднаної групи реагування, затвердження її персонального складу та порядку роботи здійснюється відповідним заступником керівника Національного координаційного центру кібербезпеки.		
		-316- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		«здійснення координації між суб'єктами національної системи обміну інформацією та національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;»		
272	впровадження механізмів взаємодії основних суб'єктів національної системи кібербезпеки»;	**-317- Н.д. Федієнко О. П. (р.к. №89)**	Відхилено	
		видалити		
273	9) доповнити статтею 9[1] такого змісту:			9) доповнити статтею 9[1] такого змісту:
274	«Стаття 9[1]. Національна система обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози	**-318- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)**	Відхилено	«Стаття 9[1]. Національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози
		Абзац 2 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції:		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«Стаття 91. Національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози»		
275	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.	**-319- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 3 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «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.»	Відхилено	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.
276	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).	**-320- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 4 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «2. Уповноваженим органом, що здійснює забезпечення функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози є Державна служба спеціального зв'язку та захисту інформації України (далі - Уповноважений орган).»	Відхилено	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).
277	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	**-321- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 5 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «Уповноважений орган визначає порядок, форми здійснення повідомлень про	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	обміну інформацією, забезпечує функціонування платформи обміну інформацією та порядку приєднання до такої платформи.	кіберінциденти, кібератаки, кіберзагрози з урахуванням обмежень, що унеможливлюють розкриття розвідувальної інформації, національну таксономію кіберінцидентів, впроваджує організаційно-технічні заходи щодо створення системи обміну інформацією, забезпечує функціонування платформи обміну інформацією та порядку приєднання до такої платформи.»		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.
278	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.	**-322- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 6 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «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 кіберінциденти, кібератаки.»	Відхилено	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.
279	Власники/розпорядники об’єктів критичної інформаційної інфраструктури зобов'язані повідомляти про всі значні інциденти кібербезпеки, кібератаки.	**-323- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 7 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «Власники/розпорядники об’єктів критичної інформаційної інфраструктури зобов'язані повідомляти про всі значні кіберінциденти, кібератаки.»	Відхилено	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.
280				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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
				обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, повідомляти відповідний CSIRT про такі кіберінциденти.
281	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.	**-324- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 8 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «Встановлення законами України зобов'язання для суб'єктів, що обробляють інші категорії інформації з обмеженим доступом, надавати обов'язкові повідомлення про кіберінциденти, кібератаки, є підставою для приєднання у встановленому порядку до національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози згідно з цим Законом.»	Відхилено	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.
282	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 в порядку, визначеному Уповноваженим органом.	**-325- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 9 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «Суб'єкти, для яких не встановлені зобов'язання надавати обов'язкові повідомлення про кіберінциденти, кібератаки мають право приєднатися до національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та здійснювати добровільний обмін інформацією про кіберінциденти, кібератаки відповідно до встановленої національної таксономії кіберінцидентів в порядку, визначеному Уповноваженим органом.»	Відхилено	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.
283	4. Усі обов'язкові повідомлення подаються суб'єктами, визначеними цією статтею, у строки та порядку, визначені Уповноваженим органом.			4. Усі обов'язкові повідомлення про кіберінциденти, кібератаки, кіберзагрози подаються суб'єктами, визначеними цією статтею, у строки та порядку, встановлені Уповноваженим органом.
284	5. Уповноважений орган визначає критерії значності впливу інцидентів кібербезпеки,	**-326- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д.**	Відхилено	5. Уповноважений орган визначає критерії значного кіберінциденту для цілей

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	кібератаки, що призводить до обов'язку надавати обов'язкові повідомлення для власників/розпорядників критичної інформаційної інфраструктури згідно з цим Законом.	**Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 11 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «5. Уповноважений орган визначає критерії значності впливу кіберінцидентів, кібератаки, що призводить до обов'язку надавати обов'язкові повідомлення для власників/розпорядників критичної інформаційної інфраструктури згідно з цим Законом.»		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.
285	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.	**-327- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)** Абзац 12 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «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 кіберінциденти, кібератаки.»	Відхилено	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.
286	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.	**-328- Н.д. Ар'єв В. І. (р.к. №202)** 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 та про наслідки інцидента кібератаки на об'єктах критичної	Відхилено	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		інформаційної інфраструктури є відкритою інформацією, окрім інформації про характер, деталі і технічні подробиці інциденту кібербезпеки, кібератаки.		деталі кіберінциденту, кібератаки, що віднесена до інформації з обмеженим доступом.
		-329- Н.д. Пузійчук А. В. (р.к. №182)	Відхилено	
		Абзац тринадцятий підпункту 9 пункту 4 розділу І виключити.		
		-330- Н.д. Мокан В. І. (р.к. №99)	Відхилено	
		Абзаци перший частини сьомої статті 9-1 Закону в редакції проєкту виключити. ***Обґрунтування.*** Приховування і обмеження доступу суспільства до інформації про сам факт кібератаки, її потенційні ризики та наслідки не вирішать проблему кібератак, а лише сприятимуть зростанню недовіри суспільства до державних органів.		
		-331- Н.д. Штепа С. С. (р.к. №283)	Відхилено	
		Абзац тринадцятий підпункту 9 пункту 4 розділу І законопроєкту виключити.		
		-332- Н.д. Тимошенко Ю. В. (р.к. №162), Н.д. Дубіль В. О. (р.к. №171), Н.д. Івченко В. Є. (р.к. №185), Н.д. Кабаченко В. В. (р.к. №184), Н.д. Кириленко І. Г. (р.к. №167), Н.д. Кожем'якін А. А. (р.к. №168), Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Лукашук Б. О. (р.к. №454), Н.д. Наливайченко В. О. (р.к. №164), Н.д. Немиря Г. М. (р.к. №169), Н.д. Соколов М. В. (р.к. №452), Н.д. Тарута С. О. (р.к. №163), Н.д. Цимбалюк М. М. (р.к. №176)	Відхилено	
		Абзац тринадцятий підпункту 9) пункту 4 Розділу І викласти в такій редакції: «7. Інформація про інцидент кібербезпеки, кібератаку щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем (за винятком інцидентів, наслідки яких становлять значний суспільний інтереси та/або можуть спричинити шкоду громадянам через неналежне інформування), в яких		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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.».		
		-333- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 13 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «7. Інформація про кіберінцидент, 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.»		
		-334- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)	Відхилено	
		У абзаці тринадцятому підпункту 9 пункту 4 розділу I проекту Закону слова «є інформацією з обмеженим доступом» замінити словами «та про наслідки інцидента кібератаки на об'єктах критичної інформаційної інфраструктури є відкритою інформацією, окрім інформації про характер,	Народні депутати України - члени Комітету.	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		технічні характеристики та інші деталі інциденту кібербезпеки, кібератаки, що віднесено до інформації з обмеженим доступом».		
287	Підстави, порядок та мету розкриття інформації про інцидент кібербезпеки, кібератаку в рамках функціонування національної системи обміну інформації про інциденти кібербезпеки, затверджується Кабінетом Міністрів України.	**-335- Н.д. Ар'єв В. І. (р.к. №202)**	Відхилено	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.
		Підстави, порядок та мету розкриття інформації про характер, деталі і технічні подробиці інциденту кібербезпеки, кібератаки в рамках функціонування національної системи обміну інформації про інциденти кібербезпеки, затверджується Кабінетом Міністрів України.		
		-336- Н.д. Пузійчук А. В. (р.к. №182)	Відхилено	
		Абзац чотирнадцятий підпункту 9 пункту 4 розділу I виключити.		
		-337- Н.д. Мокан В. І. (р.к. №99)	Відхилено	
		Абзаци другий частини сьомої статті 9-1 Закону в редакції проєкту виключити. ***Обґрунтування.*** Приховування і обмеження доступу суспільства до інформації про сам факт кібератаки, її потенційні ризики та наслідки не вирішать проблему кібератак, а лише сприятимуть зростанню недовіри суспільства до державних органів.		
		-338- Н.д. Герасимов А. В. (р.к. №196), Н.д. Гончаренко О. О. (р.к. №338), Н.д. Павленко Р. М. (р.к. №203), Н.д. Федина С. Р. (р.к. №190)	Відхилено	
		Абзац 14 пункту 9 частини 4 розділу I законопроекту викласти у наступній редакції: «Підстави, порядок та мету розкриття інформації про кіберінцидент, кібератаку в рамках функціонування національної системи обміну інформації про кіберінциденти, затверджується Кабінетом Міністрів України.»		
		-339- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д.	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Парубій А. В. (р.к. №187), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Фріз І. В. (р.к. №198), Н.д. Хоменко О. В. (р.к. №68)		
		Абзац чотирнадцятий підпункту 9 пункту 4 розділу І проекту Закону викласти в такій редакції: «Критерії віднесення інформації про характер, технічні та інші деталі інциденту кібербезпеки, кібератаки, підстави, порядок та мету розкриття такої інформації, в тому числі, службової інформації з метою обміну в рамках функціонування національної системи обміну інформації про інциденти кібербезпеки, а також порядок публічного інформування або звітування про реагування та відновлення за результатами інциденту кібербезпеки, кібератаки, затверджується Кабінетом Міністрів України».	Народні депутати України - члени Комітету.	
288	Інформація, одержана національним, галузевим, регіональним CSIRT або приватною командою реагування, що виконує їх завдання відповідно до цього Закону, використовується ними виключно в цілях та у порядку, визначеному законодавством щодо функціонування національної системи обміну інформацією та забезпечують відповідний захист та умови обробки одержаної інформації.»;	**-340- Н.д. Пузійчук А. В. (р.к. №182)** Абзац п’ятнадцятий підпункту 9 пункту 4 розділу І виключити.	Відхилено	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»;
289	10) статтю 15 доповнити частиною четвертою такого змісту:	**-341- Н.д. Кучеренко О. Ю. (р.к. №179), Н.д. Івченко В. Є. (р.к. №185)** Підпункт 10, пункту 4, розділу І законопроекту виключити. *Обгрунтування*: У висновку Комітету Верховної Ради України з питань	Відхилено	10) статтю 15 доповнити частиною четвертою такого змісту:

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		національної безпеки, оборони та розвідки у своєму висновку від 12.12.2024 (до повторного першого читання) зазначили, що з тексту законопроєкту виключено нову статтю 15^1 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» щодо закріплення за ДССЗЗІ права державного контролю за станом технічного захисту інформації та кіберзахисту. Разом з цим у тексті законопроєкту зберіглись доповнення до ст.15 Закону України «Про основні засади забезпечення кібербезпеки України» які відсилають до вищезгаданих виключених положень статті 15^1 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України». Враховуючи вищенаведене, а також що: 1) стаття 15 Закону України «Про основні засади забезпечення кібербезпеки України» врегульовує питання саме «законності заходів із забезпечення кібербезпеки України», а не саме додержання вимог законодавства у сфері кіберзахисту, 2) стаття 15 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», у редакції законопроєкту, іншим чином врегульовує це питання через здійснення «моніторінгу», надання «обов'язкових до виконання вимог» тощо, пропонується виключити зміни до статті 15 Закону України «Про основні засади забезпечення кібербезпеки України».		
		-342- Н.д. Кучеренко О. Ю. (р.к. №179) Підпункт 10 пункту 4 розділу I законопроекту виключити. *Обгрунтування:* У висновку Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки у своєму висновку від 12.12.2024 (до повторного першого читання) зазначили, що з	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		тексту законопроєкту виключено нову статтю 151 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» щодо закріплення за ДССЗЗІ права державного контролю за станом технічного захисту інформації та кіберзахисту. Разом з цим у тексті законопроєкту зберіглись доповнення до ст.15 Закону України «Про основні засади забезпечення кібербезпеки України» які відсилають до вищезгаданих виключених положень статті 151 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України». Враховуючи вищенаведене, а також що: 1) стаття 15 Закону України «Про основні засади забезпечення кібербезпеки України» врегульовує питання саме «законності заходів із забезпечення кібербезпеки України», а не саме додержання вимог законодавства у сфері кіберзахисту, 2) стаття 15 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», у редакції законопроєкту, іншим чином врегульовує це питання через здійснення «моніторінгу», надання «обов'язкових до виконання вимог» тощо, 3) навіть редакція законопроекту, яку було подано до другого читання, містила комітетську поправку, якою закріплювалось, що повноваження Держспецзв'язку передбачені статтею 15 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» «не є заходом державного контролю за технічним захистом інформації та кіберзахистом», пропонується виключити зміни до статті 15 Закону України «Про основні засади забезпечення кібербезпеки України».		
290	«4. Державна служба спеціального зв'язку та захисту інформації України здійснює	**-343- Н.д. Сірко Ю. Л. (р.к. №210)** виключити	Відхилено	«4. Державна служба спеціального зв'язку та захисту інформації України

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	державний контроль за додержанням вимог законодавства у сфері кіберзахисту відповідно до закону.	**-344- Н.д. Сірко Ю. Л. (р.к. №210)** виключити	Відхилено	здійснює державний контроль за додержанням вимог законодавства у сфері кіберзахисту відповідно до законодавства.
291	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».	**-345- Н.д. Сірко Ю. Л. (р.к. №210)** 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» та Законом України " Про основні засади державного нагляду (контролю) у сфері господарської діяльності".	Відхилено	Порядок здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту встановлюється Кабінетом Міністрів України».
		-346- Н.д. Сірко Ю. Л. (р.к. №210) 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» та Законом України " Про основні засади державного нагляду (контролю) у сфері господарської діяльності".	Відхилено	
		-347- Н.д. Федієнко О. П. (р.к. №89) Частину першу статті 11 Закону України «Про публічні електронні реєстри» (Відомості Верховної Ради України, 2023 р., № 11, ст. 27 із наступними змінами) після пункту 6 доповнити новим 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, визначеному Кабінетом Міністрів України;»**	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
292		**-348- Н.д. Василевська-Смаглюк О. М. (р.к. №302)** Розділ І законопроекту доповнити пунктом 5 такого змісту: “5. У статті 7 Закону України “Про Національний банк України” (Відомості Верховної Ради України (ВВР), 1999, № 29, ст.238 із наступними змінами): 1) пункт 32 викласти у новій редакції: “32) 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, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням, утворює центр кіберзахисту Національного банку (уключаючи команду реагування на кіберінциденти в банківській системі України (CSIRT-NBU), забезпечує функціонування системи кіберзахисту для банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, 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”; 2) доповнити підпунктом 32^1 такого змісту:	Відхилено	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		“32[1]) визначає умови обробки інформації та встановлює вимоги щодо забезпечення захисту інформації в інформаційних, електронно-комунікаційних та інформаційно-комунікаційних системах у сфері надання банківських, інших фінансових та платіжних послуг, інформації з обмеженим доступом, що є складовою системи депозитарного обліку Національного банку України, використання засобів захисту інформації в інформаційних, електронно-комунікаційних та інформаційно-комунікаційних 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”.		
		-349- Н.д. Мамка Г. М. (р.к. №147)	Відхилено	
		Доповнити Розділ І новим пунктом 5 такого змісту: "5. У пункті 4 частини першої статті 8 Закону України "Про державну таємницю" (Відомості Верховної Ради України, 1999 р., № 49, ст. 428): абзац п'ятий викласти у такій редакції: "про систему спеціального зв’язку та національну систему урядових електронних комунікацій"; доповнити новими абзацами 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, стан, планування та здійснення заходів із захисту та забезпечення безпеки і стійкості об’єктів критичної інфраструктури;		

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		про створення матеріально-технічного резерву для реагування на кризові ситуації та ліквідації їх наслідків на об’єктах критичної інфраструктури.""		
		-350- Н.д. Корнієнко О. С. (р.к. №7)	Відхилено	
		Розділ І доповнити новим пунктом такого змісту: “5. Частину першу статті 11 Закону України “Про публічні електронні реєстри” (Відомості Верховної Ради України, 2023 р., № 11, ст. 27 із наступними змінами) після пункту 6 доповнити новим 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, визначеному Кабінетом Міністрів України;”		
293		**-351- Н.д. Мамка Г. М. (р.к. №147)**	Відхилено	
		Доповнити Розділ І новим пунктом 6 такого змісту: "6. Пункт 11 Розділу VI "Прикінцеві та перехідні положення" Закону України "Про критичну інфраструктуру" (Відомості Верховної Ради України, 2023 р., № 5, ст.13 із наступними змінами) виключити."		
294		**-352- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Касай Г. О. (р.к. №280), Н.д. Ковальов О. І. (р.к. №262), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д.**	Враховано	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

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Федієнко О. П. (р.к. №89), Н.д. Хоменко О. В. (р.к. №68), Н.д. Чернєв Є. В. (р.к. №26) 3) Розділ I проекту Закону доповнити новим пунктом такого змісту: «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, визначеному Кабінетом Міністрів України».	Народні депутати України - члени Комітету	функціонування, можливість використання програмного забезпечення Платформи для створення, ведення та адміністрування реєстрів у порядку, встановленому Кабінетом Міністрів України».
295	II. Прикінцеві положення.	**-353- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Бобровська С. А. (р.к. №217), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Івченко В. Є. (р.к. №185), Н.д. Касай Г. О. (р.к. №280), Н.д. Копитін І. В. (р.к. №330), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Чернєв Є. В. (р.к. №26)**	Відхилено	II. Прикінцеві положення
		Розділ II «Прикінцеві положення» проекту Закону викласти в такій редакції: «II. Прикінцеві положення. 1. Цей Закон набирає чинності з дня, наступного за днем його опублікування, крім підпункту 5 пункту 4 розділу I 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:	Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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».		
296		**-354- Н.д. Завітневич О. М. (р.к. №38), Н.д. Березін М. Ю. (р.к. №352), Н.д. Веніславський Ф. В. (р.к. №85), Н.д. Герасименко І. Л. (р.к. №268), Н.д. Здебський Ю. В. (р.к. №373), Н.д. Касай Г. О. (р.к. №280), Н.д. Ковальов О. І. (р.к. №262), Н.д. Копитін І. В. (р.к. №330), Н.д. Костенко Р. В. (р.к. №221), Н.д. Мисягін Ю. М. (р.к. №243), Н.д. Припутень Д. С. (р.к. №97), Н.д. Рахманін С. І. (р.к. №216), Н.д. Федієнко О. П. (р.к. №89), Н.д. Хоменко О. В. (р.к. №68), Н.д. Чернєв Є. В. (р.к. №26)** Розділ ІІ «Прикінцеві положення» проекту Закону викласти в такій редакції: «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	Враховано Народні депутати України - члени Комітету	

№	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		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».		
297	1. Цей Закон набирає чинності через три місяці з дня його опублікування, крім підпункту 5 пункту 4 розділу I цього Закону, який набирає чинності через шість місяців з дати набрання чинності цим Законом та пункту 2 цього розділу, який набирає чинності з дня опублікування цього Закону.	**-355- Н.д. Пузійчук А. В. (р.к. №182)** Пункт 1 розділу II викласти в такій редакції: «1. Цей Закон набирає чинності з дня, наступного за днем його опублікування, крім підпункту 5 пункту 4 розділу I цього Закону, який набирає чинності через шість місяців з дня його опублікування.».	Відхилено	1. Цей Закон набирає чинності з дня, наступного за днем його опублікування, крім підпункту 5 пункту 4 розділу I цього Закону, який набирає чинності через шість місяців з дня його опублікування.
298	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.	**-356- Н.д. Пузійчук А. В. (р.к. №182)** Пункт 2 розділу II викласти в такій редакції: «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.».	Відхилено	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.
299	3. Кабінету Міністрів України у 2025 році поінформувати Верховну Раду України про стан виконання цього Закону.			3. Кабінету Міністрів України у 2025 році поінформувати Верховну Раду України про стан виконання цього Закону.
300	**Голова Верховної Ради України**			**Голова Верховної Ради України**