ВЕРХОВНА РАДА УКРАЇНИ

КОМІТЕТ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ ІНФОРМАТИЗАЦІЇ ТА ЗВ'ЯЗКУ

ПРОТОКОЛ ЗАСІДАННЯ №67

"10" липня 2017 р.

вул. Садова 3а,
кім 1034 (зал засідань),
м. Київ
17:00

Головує: Голова Комітету Данченко О.І.

Присутні: Перший заступник Голови Комітету – Лук`янчук Р.В., Секретар Комітету – Матузко О.О., Члени Комітету – Семенуха Р.С., Бабенко В.Б.

Працівники секретаріату Комітету: керівник секретаріату Старинець О.Г., головний консультант секретаріату Поташев С.В., головний консультант секретаріату Бурсак І.А.

Запрошені: Севрюков В.В. – народний депутат України, Кулешов М.В. – представник СБУ, Мялковський Д.С. – директор Департаменту Держспецзв'язку.

Додаток: (Порівняльна таблиця до проекту Закону України «Про основні засади забезпечення кібербезпеки України», реєстр. № 2126а), (повторне друге читання).

ПОРЯДОК ДЕННИЙ:

1. Проект Закону про основні засади забезпечення кібербезпеки України (реєстр. № 2126а від 19.06.2015, (доопрацьований) 14.04.2016), внесений н.д. Лук'янчуком Р.В. та іншими, (повторне друге читання).
2. Проект Закону про внесення змін до деяких законів України щодо тимчасових дозволів на мовлення в зоні проведення антитерористичної операції та прикордонних районах України, внесений н.д. Сюмар В.П. та іншими, реєстр. № 6565 від 08.06.2017.
3. Різне

Слухали:

Інформацію Голови Комітету Данченка Олександра Івановича про проект порядку денного засідання Комітету з питань інформатизації та зв'язку на 10 липня 2017 року.

Ухвалили:

Затвердити порядок денний засідання Комітету з питань інформатизації та зв'язку на 10 липня 2017 року.

«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято

1.

Слухали:

Інформацію Першого заступника Голови Комітету Лук'янчука Руслана Валерійовича про проект Закону про основні засади забезпечення кібербезпеки України (реєстр. № 2126а від 19.06.2015, (доопрацьований) 14.04.2016), внесений н.д. Лук'янчуком Р.В., та іншими, (повторне друге читання).

В обговоренні взяли участь: Лук'янчук Р.В., Данченко О.І., Старинець О.Г., Семенуха Р.С., Матузко О.О., Кулешов М.В.

Під час обговорення порівняльної таблиці до проекту Закону **про основні засади забезпечення кібербезпеки України** народні депутати України – члени Комітету висловили пропозицію розглянути поправки, що надійшли до повторного другого читання, а саме:

3. Поправку третю народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

30. Поправку тридцяту народного депутата Лук'янчука Р.В. – врахувати:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

50. Поправку п'ятдесяту народного депутата Лук'янчука Р.В. – врахувати:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

54. Поправку п'ятдесят четверту народного депутата Лук'янчука Р.В. – врахувати:
«За» - 4 (Данченко О.І., Лук'янчук Р.В., Матузко О.О., Бабенко В.Б.)
«Проти» - 0
«Утримались» - 1 (Семенуха Р.С.)
Рішення прийнято.

55. Поправку п'ятдесят п'яту народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

Повернутися до розгляду поправки п'ятдесят восьмої народного депутата Козиря Б.Ю.
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

58. Поправку п'ятдесят восьму народного депутата Козиря Б.Ю.
– врахувати:
«За» - 4 (Данченко О.І., Лук'янчук Р.В., Матузко О.О., Бабенко В.Б.)
«Проти» - 0
«Утримались» - 1 (Семенуха Р.С.)
Рішення прийнято.

72. Поправку сімдесят другу народного депутата Боднаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

82. Поправку вісімдесят другу народного депутата Данченка О.І. – врахувати:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

85. Поправку вісімдесят п'яту народного депутата Данченка О.І. – врахувати:

«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

86. Поправку вісімдесят шосту народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

87. Поправку вісімдесят сьому народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

97. Поправку дев'яносто сьому народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

109. Поправку сто дев'яту народного депутата Лук'янчука Р.В. – врахувати:
«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

110. Поправку сто десяту народного депутата Данченка О.І. – врахувати:
«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

126. Поправку сто двадцять шосту народного депутата Лук'янчука Р.В. – відхилити:
«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

128. Поправку сто двадцять восьму народного депутата Лук'янчука Р.В. – відхилити:
«За» - 5
«Проти» - 0

«Утримались» - 0
Рішення прийнято.

131. Поправку сто тридцять першу народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

139. Поправку сто тридцять дев'яту народного депутата Лук'янчука Р.В. – врахувати:
«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

140. Поправку сто сорокову народного депутата Данченка О.І. – врахувати:
«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

153. Поправку сто п'ятдесят третю народного депутата Данченка О.І. – врахувати:
«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

154. Поправку сто п'ятдесят четверту народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

155. Поправку сто п'ятдесят п'яту народного депутата Бондаря В.В. – відхилити:
«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

170. Поправку сто сімдесяту народного депутата Лук'янчука Р.В. – відхилити:
«За» - 5

«Проти» - 0
«Утримались» - 0
Рішення прийнято.

171. Поправку сто сімдесят першу народного депутата Лук'янчука Р.В. – відхилити:

«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

172. Поправку сто сімдесят другу народного депутата Лук'янчука Р.В. – відхилити:

«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

185. Поправку сто вісімдесят п'яту народного депутата Лук'янчука Р.В. – відхилити:

«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

189. Поправку сто вісімдесят дев'яту народного депутата Лук'янчука Р.В. – врахувати:

«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

190. Поправку сто дев'яносту народного депутата Лук'янчука Р.В. – врахувати:

«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

191. Поправку сто дев'яносто першу народного депутата Данченка О.І. – врахувати частково:

«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

192. Поправку сто дев'яносто другу народного депутата Бондаря В.В. – відхилити:

«За» - 5 (одноголосно)
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

193. Поправку сто дев'яносто третю народного депутата Данченка О.І. – врахувати:

«За» - 5
«Проти» - 0
«Утримались» - 0
Рішення прийнято.

Ухвалили:

1. Рекомендувати Верховній Раді України прийняти проект Закону про основні засади забезпечення кібербезпеки України (реєстр. № 2126а від 19.06.2015, (доопрацьований) 14.04.2016), в редакції Комітету з питань інформатизації та зв'язку в повторному другому читанні та в цілому як Закон.

2. Звернутись до Головного юридичного управління Апарату Верховної Ради України щодо техніко-юридичного опрацювання редакції законопроекту, підготовленої до повторного другого читання.

3. Визначити доповідачем на сесії Верховної Ради України із зазначеного законопроекту Першого заступника Голови Комітету з питань інформатизації та зв'язку Лук'янчука Руслана Валерійовича.

«За» - 4 (Данченко О.І., Матузко О.О., Семенуха Р.С., Бабенко В.Б.)
«Проти» - 0
«Утримались» - 1 (Лук'янчук Р.В.)
Рішення прийнято.

2.

Слухали:

Інформацію Голови Комітету Данченка Олександра Івановича про проект Закону про внесення змін до деяких законів України щодо тимчасових дозволів на мовлення в зоні проведення антитерористичної операції та прикордонних районах України, внесений н.д. Сюмар В.П. та іншими, реєстр. № 6565 від 08.06.2017.

В обговоренні взяли участь: Данченко О.І. Севрюков В.В., Лук'янчук Р.В., Семенуха Р.С., Матузко О.О.

Ухвалили:

1. Рекомендувати Верховній Раді України за результатами розгляду в першому читанні направити суб'єктам права законодавчої ініціативи на доопрацювання проект Закону про внесення змін до деяких законів України щодо тимчасових дозволів на мовлення в зоні проведення антитерористичної операції та прикордонних районах України, реєстраційний номер 6565 від 08.06.2017, внесений народними депутами Сюмар В.П. та іншими.

2. Відповідно до частини четвертої статті 111 Регламенту Верховної Ради України, наполягати на співдоповіді від Комітету під час розгляду проекту Закону про внесення змін до деяких законів України щодо тимчасових дозволів на мовлення в зоні проведення антитерористичної операції та прикордонних районах України, (реєстраційний номер 6565 від 08.06.2017), на Пленарному засіданні Верховної Ради України.

3. Співдоповідачем визначити Голову Комітету Данченка О.І.

4. Звернутися до Голови Верховної Ради України щодо надання слова для співдоповіді Голові Комітету Данченку О.І. із зазначеного питання.

5. Надіслати Висновок Комітету до Голови Верховної Ради України та до Комітету Верховної Ради України з питань свободи слова та інформаційної політики.

«За» -5 (одноголосно)
«Проти» - 0
«Утримались» -0
Рішення прийнято

3.

Слухали:

Інформацію Голови Комітету Данченка Олександра Івановича про запит до Кабінету Міністрів України щодо висновку до проекту Закону про внесення змін до деяких законодавчих актів України щодо ідентифікації особи для оформлення, видачі, обміну, визнання недійсними та знищення документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, а також звільнення від сплати адміністративного збору за оформлення таких документів осіб, постраждалих в наслідок окупації або збройного конфлікту, поданий н.д. Веселовою Н.В., реєстр. № 6630-1 від 06.07.2017р.

В обговоренні взяли участь: Данченко О.І. Старинець О.Г.

Ухвалили:

Надіслати запит до Кабінету Міністрів України стосовно надання висновку, пропозицій та зауважень до зазначеного законопроекту.

«За» -5 (одноголосно)
«Проти» - 0
«Утримались» -0
Рішення прийнято

Голова Комітету **О.І.Данченко**

Секретар Комітету **О.О.Матузко**

Порівняльна таблиця до проекту Закону України
Про основні засади кібербезпеки України

Реєстраційний № 2126а

Автор(и): Народні депутати України Лук'янчук Р.В., Кожем'якін А.А., Бухарєв В.В., Паламарчук М.П., Король В.М., Семенуха Р.С., Поляков М.А., Бабенко В.Б., Сочка О.О., Данченко О.І.

(Повторне Друге читання)

Автори остаточної редакції: Народні депутати України - члени Комітету з питань інформатизації та зв'язку

Дата розгляду в комітеті: 22.02.2017

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
0.	Закон України			Закон України
1.	Про основні засади забезпечення кібербезпеки України			Про основні засади забезпечення кібербезпеки України
2.	Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки України, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їх діяльності із забезпечення кібербезпеки України.	***-1- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Вилучити з Преамбули законопроекту слова «і обов'язки».	Враховано	Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.
		-2- Н.д.Козир Б.Ю. (Реєстр.картка №127) З преамбули законопроекту вилучити після слова «повноваження» слово «і обов'язки», далі за текстом.	Враховано	
3.	Стаття 1.Визначення термінів			Стаття 1. Визначення термінів
4.	У цьому Законі наведені нижче терміни вживаються в такому значенні:			У цьому Законі наведені нижче терміни вживаються в такому значенні:
		-3- Н.д.Бондар В.В. (Реєстр.картка №191) Частину першу статті 1 Законопроекту доповнити абзацом такого змісту: «авторизований електронний майданчик – авторизована інформаційно-телекомунікаційна система, яка є частиною електронної системи та	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		забезпечує реєстрацію осіб, автоматичне розміщення, отримання і передання інформації та документів, користування сервісами з автоматичним обміном інформацією, доступ до якого здійснюється за допомогою мережі Інтернет;»		
		-4- Н.д.Мирний І.М. (Реєстр.картка №402) Доповнити статтю 1 новими абзацами такого змісту: «індикатори кіберзагроз — показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;»	Враховано	1) індикатори кіберзагроз — показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;
		-5- Н.д.Мирний І.М. (Реєстр.картка №402) Доповнити статтю 1 новими абзацами такого змісту: інформація про інцидент кібербезпеки — відомості про обставини кіберінциденту, що вказують на те, які об'єкти кіберзахисту і за яких умов, зазнали кібератаки, які з них були успішно виявлені, попереджені або нейтралізовані, і за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз».	Враховано	2) інформація про інцидент кібербезпеки — відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;
5.	інцидент кібербезпеки (кіберінцидент) — подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі людського фактору) та/або таких, що є можливими (потенційними) ознаками кібератаки, які пов'язані з безпекою та кіберзахистом систем електронних комунікацій, систем управління технологічними процесами, і створюють значну ймовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи та/або несанкціонованого управління її ресурсами),	***-6- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У статті 1 у терміні "інцидент кібербезпеки (кіберінцидент)" слова "та/або таких, що є можливими (потенційними) ознаками кібератаки, які пов'язані з безпекою та кіберзахистом систем електронних комунікацій, систем управління технологічними процесами, і створюють значну ймовірність порушення штатного режиму функціонування таких систем" замінити словами "та/або таких, що мають ознаки	Враховано	3) інцидент кібербезпеки (далі - кіберінцидент) — подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи та/або несанкціонованого управління її ресурсами), ставлять

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;	можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, і створюють ймовірність порушення штатного режиму функціонування таких систем".		під загрозу безпеку (захищеність) електронних інформаційних ресурсів;
		-7- Н.д.Гуляєв В.О. (Реєстр.картка №140) Викласти в такій редакції: «Кібернетичний інцидент (кіберінцидент) – подія, пов'язана з реалізацією або спробою реалізації кібератаки в кіберпросторі;»	Відхилено	
6.	кібератака — спрямовані (навмисні) дії в кіберпросторі, що становлять кіберзагрозу об'єкту (об'єктам) кіберзахисту, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні й технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що оброблюються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого і надійного функціонування, штатного режиму функціонування комунікаційних та/або технологічних систем; застосування комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;	***-8- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У статті 1 у терміні "кібератака" виключити слова "що становлять кіберзагрозу об'єкту (об'єктам) кіберзахисту.	Враховано	4) кібератака — спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; застосування комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;
		-9- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) У статті 1 у терміні "кібератака" слова "сталого і надійного функціонування, штатного режиму функціонування" замінити словами "сталого, надійного та штатного режиму функціонування"; .	Враховано	
		-10- Н.д.Ківалов С.В. (Реєстр.картка №135) Абзац 3 статті 1 викласти у такій редакції: «кібератака – втручання в сферу безпеки обігу комп'ютерної інформації, роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		модифікація комп'ютерних даних, а також інші діяння, зроблені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв з вбудованими процесорами і контролерами, які можуть мати доступ до інформаційного простору.»		
		-11- Н.д.Гуляєв В.О. (Реєстр.картка №140) Абзац 2 статті 1 викласти у такій редакції: «кібератака – цілеспрямоване втручання в роботу компонентів інформаційно-телекомунікаційних систем та їх програмного забезпечення або несанкціоновану модифікацію комп'ютерних даних, що здійснюється через інформаційно-телекомунікаційні мережі з метою дезорганізації роботи їх елементів.»	Відхилено	
7.	кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;	***-12- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Абзац четвертий частини першої статті 1 проекту Закону викласти в такій редакції: «кібербезпека — стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави при використанні кіберпростору, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;».	Враховано частково	5) кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;
		-13- Н.д.Ківалов С.В. (Реєстр.картка №135) Абзац 4 статті 1 законопроекту викласти у такій редакції: «Кібербезпека – стан захищеності суспільних відносин, що складають сферу безпеки обігу комп'ютерної інформації у кіберпросторі.»	Відхилено	
		-14- Н.д.Гуляєв В.О. (Реєстр.картка №140) Абзац 3 статті 1 викласти у такій редакції: «Кібернетична безпека	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		(кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави при використанні кіберпростору».		
8.	кіберзагроза — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, мають негативний та/або послаблюючий вплив на стан кібербезпеки України, кібербезпеку та кіберзахист її об'єктів;	***-15- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У статті 1 у терміні "кіберзагроза" слова "та/або послаблюючий" вилучити.	Враховано	6) кіберзагроза — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;
		-16- Н.д.Сольвар Р.М. (Реєстр.картка №91) У статті 1 проекту Закону у визначенні терміну "кіберзагроза" слова "та/або послаблюючий" необхідно виключити.	Враховано	
		-17- Н.д.Козир Б.Ю. (Реєстр.картка №127) У статті 1 проекту Закону у визначенні терміну "кіберзагроза" слова "та/або послаблюючий" необхідно виключити.	Враховано	
9.	кіберзахист — сукупність організаційних, нормативно-правових, технічних та інших заходів оперативного виявлення, реагування, попередження, запобігання, нейтралізації кіберінцидентів та кібератак, ліквідації їх наслідків та відновлення сталості і надійності функціонування комунікаційних, технологічних систем;	***-18- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У статті 1 термін «кіберзахист» викласти у такій редакції: «кіберзахист – сукупність організаційних, правових, інженерно-технічних, включаючи заходи криптографічного та технічного захисту інформації, спрямованих на попередження кіберінцидентів, виявлення та захист від кібератак, ліквідації їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем»;	Враховано редакційно	7) кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;
		-19- Н.д.Гуляєв В.О. (Реєстр.картка №140) Абзац 4 статті 1 викласти у такій редакції: «Кібернетичний захист (кіберзахист) – сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямованих на забезпечення кібербезпеки, включаючи попередження кібернетичних загроз,	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		протистояння кібератакам, та відновлення та усунення наслідків кібернетичних інцидентів;»		
		-20- Н.д.Сольвар Р.М. (Реєстр.картка №91) У статті 1 проекту Закону термін “кіберзахист” викласти у такій редакції: “кіберзахист – система організаційних, правових, інженерно-технічних, криптографічних заходів, спрямованих на захист від кіберзагроз”.	Відхилено	
		-21- Н.д.Козир Б.Ю. (Реєстр.картка №127) Термін «кіберзахист» викласти в такій редакції: «кіберзахист – система організаційних, правових, інженерно-технічних, криптографічних заходів, виявлення, реагування, попередження, запобігання, нейтралізації кіберінцидентів та кібератак, ліквідації їх наслідків та відновлення сталості і надійності функціонування комунікаційних, технологічних систем;»	Враховано редакційно	
10.	кіберзлочин — суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачено законодавством України про кримінальну відповідальність та/або визнано злочином міжнародним законодавством;	***-22- Н.д.Лук’янчук Р.В. (Реєстр.картка №243)*** У статті 1 термін «кіберзлочин» має бути узгоджений із Кримінальним кодексом України, який містить окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», де використовується термін «комп’ютерний злочин». При цьому слід брати до уваги, що навіть Конвенція про кіберзлочинність 2001 року і додаткові протоколи до неї оперують поняттями «комп'ютерна система», «комп'ютерні дані» та передбачають встановлення відповідальності за «правопорушення проти конфіденційності, цілісності та	Враховано	8) кіберзлочин (комп’ютерний злочин) — суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		доступності комп'ютерних даних і систем; за навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп'ютерної системи» тощо. ***-23- Н.д.Ківалов С.В. (Реєстр.картка №135)*** Абзац 7 статті 1 законопроекту викласти в такій редакції: «кіберзлочин – це винне суспільне небезпечне кримінальне каране втручання в сферу безпеки обігу комп'ютерної інформації, роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, зроблені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв з вбудованими процесорами і контролерами, які можуть мати доступ до інформаційного простору». ***-24- Н.д.Левченко Ю.В. (Реєстр.картка №223)*** У абзаці 7 частини 1 статті 1 розділу 1 законопроекту після слова-терміну «кіберзлочин» доповнити словами «(комп'ютерний злочин)», далі за текстом. ***-25- Н.д.Сольвар Р.М. (Реєстр.картка №91)*** Доповнити терміном: «кіберзлочинність – сукупність кіберзлочинів;» ***-26- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Доповнити статтю 1 абзацом наступного змісту: «кіберзлочинність –– злочинна

Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
Відхилено	
Враховано	
Враховано	
Враховано	9) кіберзлочинність — сукупність кіберзлочинів;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		діяльність, що провадиться у кіберпросторі або з його використанням»; (ІЗ) або «кіберзлочинність – сукупність кіберзлочинів». ***-27- Н.д.Козир Б.Ю. (Реєстр.картка №127)*** Статтю 1 доповнити новими термінами: кіберзлочинність – сукупність кіберзлочинів; ***-28- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Доповнити статтю 1 абзацом наступного змісту: «кібероборона - сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на захист суверенітету держави та забезпеченні її обороноздатності, запобігання збройному конфлікту та відсіч збройній агресії»;
11.	кіберпростір — середовище (віртуальний простір), яке надає можливості (послуговує) здійсненню комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та/або інших глобальних мереж передачі даних;	***-29- Н.д.Ківалов С.В. (Реєстр.картка №135)*** Абзац 8 статті 1 законопроекту викласти в такій редакції: «кіберпростір – інформаційний простір взаємодії між людьми та пристроями, який утворений мережею інфраструктури інформаційних технологій і включає в себе Інтернет, телекомунікаційні мережі, комп'ютерні системи і пристрої з вбудованими процесорами і контролерами.» ***-30- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У статті 1 визначення кіберпростору завершити словами «... та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж

Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
Враховано	
Враховано	10) кібероборона — сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;
Відхилено	
Враховано	11) кіберпростір — середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		передачі даних».		даних;
		-31- Н.д.Гуляєв В.О. (Реєстр.картка №140) Абзац 7 статті 1 викласти у такій редакції: «Кібернетичний простір (кіберпростір) – це віртуальний простір, який створюється за допомогою апаратного і програмного забезпечення, інформаційних систем, електромагнітного спектра (включаючи телекомунікаційні мережі та Інтернет) і відповідних фізичних інфраструктур, а також користувачів та відносин між ними;»	Відхилено	
		-32- Н.д.Сольвар Р.М. (Реєстр.картка №91) У статті 1 проекту Закону термін “ кіберпростір ” викласти у такій редакції: “кіберпростір – віртуальний простір, що виникає внаслідок функціонування електронних пристроїв електронних комунікаційних, інформаційних, інформаційно-комунікаційних систем і мереж, а також призначена для його створення інфраструктура”.	Враховано редакційно	
		-33- Н.д.Козир Б.Ю. (Реєстр.картка №127) Термін «кіберпростір» викласти в такій редакції: «кіберпростір – віртуальний простір, що виникає внаслідок функціонування електронних пристроїв електронних комунікаційних, інформаційних, інформаційно-комунікаційних систем і мереж, а також призначена для його створення інфраструктура».	Враховано редакційно	
		-34- Н.д.Сольвар Р.М. (Реєстр.картка №91) Статтю 1 проекту закону слід доповнити наступними термінами: «кіберрозвідка – сукупність розвідувальних органів і підрозділів, що застосовують технічні та програмні	Враховано редакційно	12) кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		засоби для конспіративного здобування у кіберпросторі іншої держави інформації, яку неможливо отримати офіційним шляхом, знищення, викривлення або блокування важливих для цієї держави електронних інформаційних ресурсів;		
		-35- Н.д.Козир Б.Ю. (Реєстр.картка №127) Статтю 1 доповнити новими термінами: «кіберрозвідка – сукупність розвідувальних органів і підрозділів, що застосовують технічні та програмні засоби для конспіративного здобування у кіберпросторі іншої держави інформації, яку неможливо отримати офіційним шляхом, знищення, викривлення або блокування важливих для цієї держави електронних інформаційних ресурсів;	Враховано редакційно	
		-36- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Доповнити статтю 1 абзацом наступного змісту: «кібертероризм — терористична діяльність, що провадиться у кіберпросторі або з його використанням») або «кібертероризм – використання кіберпростору у терористичних цілях».	Враховано редакційно	13) кібертероризм — терористична діяльність, що здійснюється у кіберпросторі або з його використанням;
		-37- Н.д.Сольвар Р.М. (Реєстр.картка №91) Статтю 1 проекту закону слід доповнити наступними термінами: «кібертероризм – використання кіберпростору в терористичних цілях;»	Враховано редакційно	
		-38- Н.д.Козир Б.Ю. (Реєстр.картка №127) Статтю 1 доповнити новими термінами: кібертероризм – використання кіберпростору у терористичних цілях;	Враховано редакційно	
		-39- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Доповнити статтю 1 визначенням терміну «кібершпигунство».	Враховано	14) кібершпигунство — шпигунство, що здійснюється у кіберпросторі або з його використанням;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-40- Н.д.Козир Б.Ю. (Реєстр.картка №127) Статтю 1 доповнити новими термінами: кібершпигунство – застосування технічних та програмних засобів для несанкціонованого здобування у кіберпросторі іншої держави інформації, яку неможливо отримати офіційним шляхом;	Враховано редакційно	
		-41- Н.д.Сольвар Р.М. (Реєстр.картка №91) Статтю 1 проекту закону слід доповнити наступними термінами: «кібершпигунство – застосування технічних та програмних засобів для несанкціонованого здобування в кіберпросторі іншої держави інформації, яку неможливо отримати офіційним шляхом;»	Враховано редакційно	
		-42- Н.д.Сольвар Р.М. (Реєстр.картка №91) Статтю 1 проекту закону слід доповнити наступними термінами: «кібервійна (бойові дії в кіберпросторі) – застосування військових формувань для відкритої міждержавної боротьби в кіберпросторі, спрямованої на досягнення політичних цілей;»	Відхилено	
		-43- Н.д.Козир Б.Ю. (Реєстр.картка №127) Статтю 1 доповнити новими термінами: кібервійна (бойові дії у кіберпросторі) – застосування військових формувань для відкритої міждержавної боротьби у кіберпросторі, спрямованої на досягнення політичних цілей;	Відхилено	
12.	критично важливі об’єкти інфраструктури (критичні інфраструктурні об’єкти) — підприємства, установи та організації незалежно від форм власності, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати негативний вплив на національну безпеку і оборону України, природне середовище,	***-44- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Абзац дев’ятий частини першої статті 1 проекту Закону викласти в такій редакції: «критично важливі об’єкти інфраструктури (критичні інфраструктурні об’єкти) — ті установки,	Враховано редакційно	15) критично важливі об’єкти інфраструктури (далі - об’єкти критичної інфраструктури) — підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	призвести до великих фінансових збитків та значних людських жертв;	системи, об'єкти, мережі підприємств, установ та організацій незалежно від форми власності, які забезпечують функції, процеси та послуги, що є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або порушення функціонування яких може мати негативний вплив на національну безпеку і оборону України, природне середовище, призвести до великих фінансових збитків та значних людських жертв;».		функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;
		-45- Н.д.Сольвар Р.М. (Реєстр.картка №91) Статтю 1 проекту закону слід доповнити наступними термінами: «критична інформаційна інфраструктура – сукупність електронних комунікаційних, інформаційних, інформаційно-комунікаційних систем і мереж об'єкта критичної інфраструктури, порушення працездатності яких завдасть істотної шкоди функціонуванню об'єкта;»	Враховано редакційно	16) критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури;
		-46- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні зміни по тексту: замінити словосполучення «критично важливі об'єкти інформаційної інфраструктури» замінити на словосполучення «об'єкти критичної інформаційної інфраструктури».	Враховано	
		-47- Н.д.Козир Б.Ю. (Реєстр.картка №127) Статтю 1 доповнити новими термінами: критична інформаційна інфраструктура – сукупність електронних комунікаційних, інформаційних, інформаційно-комунікаційних систем і мереж об'єкта критичної інфраструктури, порушення працездатності яких завдасть істотної шкоди функціонуванню об'єкта;	Враховано редакційно	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
13.	національні електронні інформаційні ресурси (національні інформресурси) — систематизовані електронні інформаційні ресурси, які містять інформацію, незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію державної, комунальної, приватної власності), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація та дані, або їх сукупність, що створені, записані, оброблені або збережені у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;	***-48- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** 1. У статті 1 в тлумаченні терміну «національні електронні ресурси» слова «та дані, або їх сукупність» вилучити.	Враховано	17) національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) — систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;
14.	національна телекомунікаційна мережа — сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до законів України, яка призначена для обігу (передавання, приймання, створення, оброблення, зберігання) національних інформресурсів, забезпечення захищених електронних комунікацій, надання спектру сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, є мережею (системою) подвійного призначення, з використанням частини її ресурсу для надання послуг, зокрема із кіберзахисту, іншим споживачам;	***-49- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У статті 1 у терміні "національна телекомунікаційна мережа" після слів "(передавання, приймання, створення, оброблення, зберігання)" додати слова "та захисту";	Враховано	18) Національна телекомунікаційна мережа — сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;
		-50- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) У статті 1 визначення «національна телекомунікаційна мережа» має починатися із заголовної літери. Внести аналогічні правки по всьому	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		тексту законопроекту.		
		-51- Н.д.Сольвар Р.М. (Реєстр.картка №91)	Враховано редакційно	19) об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;
		Статтю 1 проекту закону слід доповнити наступними термінами: «об'єкт критичної інформаційної інфраструктури – електронна комунікаційна, інформаційна, інформаційно-комунікаційна система або мережа об'єкта критичної інфраструктури, порушення працездатності якої завдасть істотної шкоди функціонуванню об'єкта";»		
		-52- Н.д.Козир Б.Ю. (Реєстр.картка №127)	Враховано редакційно	
		Статтю 1 доповнити новими термінами: об'єкт критичної інформаційної інфраструктури – електронна комунікаційна, інформаційна, інформаційно-комунікаційна система або мережа об'єкта критичної інфраструктури, порушення працездатності якої завдасть істотної шкоди функціонуванню об'єкта".		
15.	система електронних комунікацій (комунікаційна система) — системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі тією мірою, в якій вони використовуються для цілей передачі сигналів), що забезпечують передачу електронних інформаційних ресурсів, у тому числі комп'ютери, інша комп'ютерна техніка, засоби і пристрої зв'язку, інформаційно-телекомунікаційні системи, які мають доступ (підключені) до Інтернет та/або інших глобальних мереж передачі даних;	***-53- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У статті 1 у терміні "система електронних комунікацій (комунікаційна система)" після слів "в якій вони використовуються для цілей передачі сигналів)" наступні слова викласти у редакції: "що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ (підключені) до Інтернет та/або інших глобальних мереж передачі даних»;	Враховано	20) системи електронних комунікацій (далі - комунікаційні системи) — системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних;
16.	система управління технологічними процесами (технологічна система) — автоматизована або	***-54- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)***	Враховано	21) система управління технологічними процесами (далі - технологічна система) — автоматизована або

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі, приймання електронних інформаційних ресурсів, що організаційно, технічно та функціонально поєднані в єдине ціле, яка призначена (застосовується) для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання та інші технічні і технологічні засоби), незалежно від наявності або відсутності доступу (підключення) системи до Інтернет та/або інших глобальних мереж передачі даних.	У статті 1 визначення «система управління технологічними процесами (далі - технологічна система)» не доповнювати словами «організаційно, технічно та функціонально поєднаних електронних інформаційних ресурсів».		автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;
		-55- Н.д.Бондар В.В. (Реєстр.картка №191) Частину першу статті 1 Законопроекту доповнити абзацом такого змісту: «система хмарних обчислень - система, в якій реалізується модель забезпечення доступу на вимогу до спільної сукупності динамічно розподілюваних налаштовуваних обчислювальних ресурсів (включаючи внутрішньосистемні мережі, сервери, сховища даних, прикладні програми та послуги), що можуть бути оперативно надані і вивільнені, через глобальні мережі передачі даних із мінімальними управлінськими заходами та/або мінімальною взаємодією з надавачем хмарних послуг;».	Відхилено	
17.	Терміни "національна безпека", "національні інтереси", "загрози національній безпеці" в цьому законі вживаються у значенні, визначеному Законом України "Про основи національної безпеки України".			Терміни "національна безпека", "національні інтереси", "загрози національній безпеці" вживаються в цьому Законі у значенні, визначеному Законом України "Про основи національної безпеки України".
18.	Стаття 2.Мета і принципи застосування Закону	***-56- Н.д.Данченко О.І. (Реєстр.картка №362)*** В назві статті 2 вилучити слово «Мета».	Враховано	Стаття 2. Принципи застосування Закону
19.	1. Метою цього Закону є врегулювання відносин, пов'язаних із забезпеченням кібербезпеки, як	***-57- Н.д.Данченко О.І. (Реєстр.картка №362)***	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	складової національної безпеки України, провадженням діяльності із захисту національних інтересів та національних інформресурсів у кіберпросторі, кіберзахистом систем електронних комунікацій органів державної влади та місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до законів України, комунікаційних та технологічних систем, які використовуються критичними інфраструктурними об'єктами.	Вилучити пункт перший статті 2.		
20.	2. Цей Закон не поширюється на:			1. Цей Закон не поширюється на:
21.	1) відносини та послуги, пов'язані із змістом інформації, що передається (обробляється, зберігається) в системах електронних комунікацій та/або в системах управління технологічними процесами;			1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;
22.	2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;	***-58- Н.д.Козир Б.Ю. (Реєстр.картка №127)*** Пункт другий частини другої статті другої вилучити.	Відхилено	2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;
23.	3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані із функціонуванням таких мереж і ресурсів;			3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;
24.	4) системи електронних комунікацій, які не взаємодіють з публічними мережами електронних комунікацій, не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних.	***-59- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** В пункті четвертому частини 2 статті 2 після слів "з публічними мережами електронних комунікацій" додати в дужках слова "(електронними мережами загального користування)" і далі за текстом;	Враховано	4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).
		-60- Н.д.Козир Б.Ю. (Реєстр.картка №127) Пункт четвертий частини другої статті другої вилучити.	Враховано частково	
25.	3. Застосування законодавства у сфері кібербезпеки та рішення (заходи) суб'єктів владних			2. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	повноважень, прийняті на виконання норм цього Закону, мають відповідати таким принципам:			на виконання норм цього Закону здійснюється з додержанням принципів:
26.	1)мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети та завдань, визначених цим Законом;			1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення **мети** і завдань, визначених цим Законом;
27.	2)об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права до кіберпростору, зокрема Міжнародного гуманітарного права;	***-61- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У частині 3 статті 2 слова «зокрема Міжнародного гуманітарного права» вилучити».	Враховано	2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;
		-62- Н.д.Мирний І.М. (Реєстр.картка №402) У частині третій статті 2: - у абзаці третьому слова: «максимально можливого застосування національного та міжнародного права до кіберпростору, зокрема Міжнародного гуманітарного права» замінити словами «щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, осіб та громадян у сфері кібербезпеки»;	Враховано редакційно	
28.	3)забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій та/або послуг із захисту інформації, кіберзахисту, у тому числі, прав щодо невтручання в приватне життя і захисту персональних даних;			3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;
29.	4)прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності;			4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);
30.	5)збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між	***-63- Н.д.Мирний І.М. (Реєстр.картка №402)*** У частині третій статті 2:	Відхилено	5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту з одного боку та введенням надмірних вимог та обмежень – з іншого;	- у абзаці шостому слова: «вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту з одного боку та введенням надмірних вимог та обмежень – з іншого» замінити словами «згідно з яким вимоги (заходи) щодо забезпечення кібербезпеки та кіберзахисту мають бути достатніми, але не надмірними з точки зору співрозмірності кіберзагроз та витрат на кіберзахист, і відповідати передбаченим для цього обсягам фінансування».		встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;
31.	6)недискримінації, згідно з яким рішення, дії, бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:			6) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:
32.	відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;			відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;
33.	таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;			таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;
34.	7)еквівалентності вимог до забезпечення кібербезпеки критичних інфраструктурних об'єктів, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем критичних інфраструктурних об'єктів, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.			7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.
35.	Зазначені принципи застосовуються без переваги			Зазначені принципи застосовуються без переваги

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	будь-якого з них, з урахуванням мети і завдань цього Закону.			будь-якого з них з урахуванням мети і завдань цього Закону.
36.	Стаття 3.Правові основи забезпечення кібербезпеки України			Стаття 3. Правові основи забезпечення кібербезпеки України
37.	Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.	***-64- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Статтю 3 проекту Закону викласти в такій редакції: «1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України. 2. Якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж ті правила, які передбачені цим Законом, застосовуються положення міжнародного договору України.».	Враховано	1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України. 2. Якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.
38.	Стаття 4.Об'єкти кібербезпеки та кіберзахисту			Стаття 4. Об'єкти кібербезпеки та кіберзахисту
39.	1. Об'єктами кібербезпеки є:			1. Об'єктами кібербезпеки є:
40.	людина і громадянин, їхні конституційні права і свободи;	***-65- Н.д.Ківалов С.В. (Реєстр.картка №135)*** Абзац 2 частини першої статті 4 законопроекту викласти в такій редакції: «конституційні права, свободи людини і громадянина».	Враховано	1) конституційні права, права і свободи людини і громадянина;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
41.	суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;			2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
42.	держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканість;			3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
43.	національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави.			4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
		-66- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) До частини 1 статті 4 додати новий абзац такого змісту: "критично важливі об'єкти інфраструктури";	Враховано редакційно	5) об'єкти критичної інфраструктури.
44.	2. Об'єктами кіберзахисту є:			2. Об'єктами кіберзахисту є:
45.	комунікаційні системи державної, комунальної, інших форм власності, в яких оброблюються національні інформресурси та/або які використовуються в інтересах органів державної влади та місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до законів України;	***-67- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Абзац другий частини другої статті 4 проекту Закону викласти в такій редакції: «комунікаційні системи усіх форм власності, в яких оброблюються національні інформресурси та/або які використовуються в інтересах органів державної влади та місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до законів України;».	Враховано	1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;
		-68- Н.д.Ківалов С.В. (Реєстр.картка №135) Абзац 2 частини 2 статті 4 викласти в такій редакції: «Об'єктами кіберзахисту є об'єкти критичної інформаційної інфраструктури та інші інформаційно-телекомунікаційні системи, в яких здійснюється обробка та зберігання інформації державного органу або державного підприємства або інформації, вимога щодо захисту якої встановлена законом».	Відхилено	
46.	комунікаційні та технологічні системи критичних	***-69- Н.д.Лук'янчук Р.В. (Реєстр.картка***	Враховано	2) об'єкти критичної інформаційної

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	інфраструктурних об'єктів;	***№243)*** Словосполучення «комунікаційні та технологічні системи критичних інфраструктурних об'єктів» замінити на словосполучення «об'єкти критичної інформаційної інфраструктури».		інфраструктури;
47.	комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.			3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.
48.	3. Об'єкти кіберзахисту у сукупності складають критичну інформаційною інфраструктуру і підлягають внесенню до державного реєстру об'єктів критичної інформаційної інфраструктури. Порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджується Кабінетом Міністрів України.	***-70- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Частину 3 статті 4 викласти у наступній редакції: "Критерії та порядок віднесення об'єктів кіберзахисту до об'єктів критичної інформаційної інфраструктури, порядок внесення таких об'єктів до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджується Кабінетом Міністрів України";	Враховано редакційно	3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, перелік таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України. Повноваження щодо формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.
		-71- Н.д.Данченко О.І. (Реєстр.картка №362) У частині третій статті 4: перше речення доповнити словами "а щодо таких об'єктів у банківській системі України – до реєстру критичних інфраструктурних об'єктів у банківській системі України"; доповнити новим реченням такого змісту: "Формування та забезпечення функціонування реєстру критичних інфраструктурних об'єктів у банківській системі України покладається на Національний банк України".	Враховано редакційно	
		-72- Н.д.Бондар В.В. (Реєстр.картка №191) Статтю 4 Законопроекту доповнити	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		частиною четвертою такого змісту: «4. Об'єкти кіберзахисту (в тому числі авторизовані електронні майданчики, зокрема, з використанням систем хмарних обчислень) повинні **одночасно** відповідати вимогам щодо захисту інформації, встановленим частинами другою та третьою статті 8, статтею 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» **та мати належний захист інформації в системах де використовується технологія хмарних обчислень».**		
49.	Стаття 5.Суб'єкти забезпечення кібербезпеки			Стаття 5. Суб'єкти забезпечення кібербезпеки
50.	1. Президент України здійснює загальне керівництво у сфері кібербезпеки України, як складової національної безпеки, визначає стратегію кібербезпеки України, пріоритети та напрями її забезпечення.	***-73- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Частину першу статті 5 викласти у такій редакції: «1. Координація діяльності у сфері кібербезпеки України як складової національної безпеки здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.	Враховано	1. Координація діяльності у сфері кібербезпеки, як складової національної безпеки України, здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.
		-74- Н.д.Семенуха Р.С. (Реєстр.картка №379) Частину першу статті 5 проекту Закону викласти у такій редакції: «1. Відповідно до пункту 7 статті 116 Конституції України, Кабінет Міністрів України здійснює загальне керівництво у сфері кібербезпеки України, як складової національної безпеки, визначає стратегію кібербезпеки України, пріоритети та напрями її забезпечення.»	Враховано редакційно	
51.	2. Рада національної безпеки і оборони України здійснює координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України, створює з цією метою Національний координаційний центр кібербезпеки, як робочий орган Ради національної	***-75- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Частину другу статті 5 викласти у такій редакції: «2. Національний координаційний	Враховано	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, вносить Президентові України пропозиції щодо формування та

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	безпеки і оборони України; з урахуванням реального стану кібербезпеки України та загроз національній безпеці у кіберпросторі вносить Президенту України пропозиції щодо формування та уточнення стратегії кібербезпеки України.	центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України».		уточнення Стратегії кібербезпеки України.
		-76- Н.д.Семенуха Р.С. (Реєстр.картка №379) Частину другу статті 5 проекту Закону виключити. Частини третю-шосту вважати, відповідно, частинами другою-п'ятою.	Відхилено	
52.	3. Кабінет Міністрів України забезпечує формування та реалізовує державну політику у сфері кібербезпеки України, забезпечення прав і свобод людини і громадянина, захисту національних інтересів України у кіберпросторі, боротьби з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки критичних інфраструктурних об'єктів.	***-77- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У частині третій статті 5 слова «у сфері кібербезпеки України» замінити словами «у сфері кіберзахисту».	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; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).
		-78- Н.д.Семенуха Р.С. (Реєстр.картка №379) Частину третю статті 5 проекту Закону викласти у такій редакції: «2. Кабінет Міністрів України визначає міністерства, які забезпечують формування державної політики та центральні органи виконавчої влади, які забезпечать реалізацію державної політики у сфері кібербезпеки України, забезпечення прав і свобод людини і громадянина, захисту національних інтересів України у кіберпросторі, боротьби з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки критичних	Враховано частково	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		інфраструктурних об'єктів.» ***-79- Н.д.Данченко О.І. (Реєстр.картка №362)*** У статті 5: у частині третій: доповнити словами у дужках "(крім банків)"; доповнити новим абзацом такого змісту: "Національний банк України встановлює вимоги та забезпечує функціонування системи аудиту інформаційної безпеки критичних інфраструктурних об'єктів у банківській системі України";	Враховано редакційно	
		-80- Н.д.Сольвар Р.М. (Реєстр.картка №91) У ч. 3 ст. 5 проекту слова "у сфері кібербезпеки України" видається логічним замінити словами "у сфері кіберзахисту".	Відхилено	
		-81- Н.д.Козир Б.Ю. (Реєстр.картка №127) У частині 3 статті 5 слова «у сфері кібербезпеки України» замінити словами «у сфері кіберзахисту».	Відхилено	
		-82- Н.д.Данченко О.І. (Реєстр.картка №362) У статті 5 у частині третій: доповнити словами у дужках "(крім об'єктів критичної інфраструктури у банківській системі України)";	Враховано	
53.	4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є			4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:
54.	міністерства та інші центральні органи виконавчої влади;	***-83- Н.д.Данченко О.І. (Реєстр.картка №362)*** абзац другий частини четвертої доповнити словами "Національний банк України".	Враховано	1) міністерства та інші центральні органи виконавчої влади;
55.	місцеві державні адміністрації та органи місцевого самоврядування;			2) місцеві державні адміністрації; 3) органи місцевого самоврядування;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
56.	правоохоронні, розвідувальні і контррозвідувальні органи України, суб'єкти оперативно-розшукової діяльності;			4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;
57.	Збройні Сили України, інші військові формування, утворені відповідно до законів України;			5) Збройні Сили України, інші військові формування, утворені відповідно до закону;
		-84- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Доповнити частину 4 статті 5 абзацом «Національний банк України».	Враховано	6) Національний банк України;
		-85- Н.д.Данченко О.І. (Реєстр.картка №362) У статті 5 абзац другий частини четвертої доповнити словами "Національний банк України".	Враховано	
58.	підприємства, установи та організації, віднесені до критично важливих об'єктів інфраструктури;			7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;
59.	суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.			8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.
		-86- Н.д.Бондар В.В. (Реєстр.картка №191) У частині четвертій статті 5 Законопроекту: Абзац сьомий доповнити словами «авторизовані електронні майданчики»;	Відхилено	
		-87- Н.д.Бондар В.В. (Реєстр.картка №191) У частині четвертій статті 5 Законопроекту: Частину четверту доповнити абзацом такого змісту: «Інформаційно-телекомунікаційна система (авторизований електронний майданчик) самостійно визначає необхідність та види забезпечення гарантій виконання зобов'язань володільцем інформації (у тому числі шляхом страхування цивільно-правової	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		відповідальності) відповідно до цивільного законодавства..»		
60.	5. Суб'єкти забезпечення кібербезпеки діють у межах повноважень, визначених Конституцією України, цим Законом, іншими законами України у відповідних сферах діяльності, а також нормативно-правовими актами, що прийняті на виконання законів України.	***-88- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Частину 6 статті 5 вилучити.	Враховано	
61.	6. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, терористичних та інших протиправних і злочинних цілях, виявлення й реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують попереджувальні, організаційні, освітні та інші заходи у сфері кібербезпеки та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.	***-89- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У частині 6 статті 5 після слів «та інші заходи у сфері кібербезпеки» додати слово «кібероборони» і далі за текстом.	Враховано	6. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях, виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.
		-90- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) У частині 6 статті 5 після слова «воєнних» додати слово «розвідувально-підривних» і далі за текстом.	Враховано	
		-91- Н.д.Мирний І.М. (Реєстр.картка №402) У частині шостій статті 5 слова «воєнних, терористичних та інших протиправних і злочинних цілях» замінити словами «у злочинних цілях»;	Відхилено	
		-92- Н.д.Мирний І.М. (Реєстр.картка №402) У частині шостій статті 5 слова «інформаційний обмін щодо реалізованих та потенційних кіберзагроз» замінити словами «обмін інформацією про інциденти кібербезпеки»	Відхилено	
		-93- Н.д.Сольвар Р.М. (Реєстр.картка №91) У ч. 6 ст. 5 проекту після слова "воєнних"	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		доповнити новим словом “розвідувально-підривних”.		
		-94- Н.д.Козир Б.Ю. (Реєстр.картка №127) У частині 6 статті 5 після слова «воєнних» додати слово «розвідувально-підривних» і далі за текстом.	Враховано	
62.	Стаття 6. Критично важливі об’єкти інфраструктури			Стаття 6. Об’єкти критичної інфраструктури
63.	1. До критичних інфраструктурних об’єктів можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:	***-95- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Частину першу статті 6 проекту Закону викласти у такій редакції: «1. До критичних інфраструктурних об’єктів можуть бути віднесені ті установки, системи, об’єкти, мережі підприємств, установ та організацій незалежно від форми власності, які забезпечують функції, процеси та послуги:	Враховано редакційно	1. До об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:
64.	1) здійснюють діяльність та надають послуги у галузях енергетики, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторі,	***-96- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Викласти в такій редакції: 1) у галузі енергетики, нафтогазовій галузі, галузях транспорту, зв’язку, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторі;	Відхилено	1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторі;
		-97-Н.д.Бондар В.В. (Реєстр.картка №191) Пункт 1 частини першої статті 6 Законопроекту після слів «електронних комунікацій» доповнити словами ***«(у тому числі із застосуванням авторизованих електронних майданчиків та/або веб-порталів органів державної влади)»***	Відхилено	
		-98- Н.д.Лук’янчук Р.В. (Реєстр.картка №243) Частину першу пункту першого статті 6 викласти в такій редакції: «здійснюють діяльність та надають послуги у галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		технологій, електронних комунікацій, у банківському та фінансовому секторі.		
65.	2) здійснюють діяльність та надають послуги, пов'язані із функціонуванням систем життєзабезпечення населення, зокрема систем водопостачання, виробництва і постачання продуктів харчування, охорони здоров'я;	***-99- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У пункті другому частини 1 статті 6 після слів "зокрема систем водопостачання" додати слова "та водовідведення, постачання електроенергії і газу";	Враховано	2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;
		-100- Н.д.Семенуха Р.С. (Реєстр.картка №379) Пункт другий частини першої статті 6 проекту викласти в такій редакції: «2) у сферах життєзабезпечення населення, зокрема у сферах водопостачання, виробництва продуктів харчування, сільського господарства, охорони здоров'я;»	Враховано	
66.	3) виконують функції комунальних, аварійних та рятувальних служб, служб екстреної допомоги населенню;	***-101- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Пункт третій частини першої статті 6 викласти в такій редакції: «3) як комунальні, аварійні та рятувальні служби, служби екстреної допомоги населенню;».	Враховано	3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;
67.	4) включені до переліку підприємств, які мають стратегічне значення для економіки і безпеки держави;	***-102- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У пункті четвертому частини 1 статті 6 після слів ", які мають стратегічне значення для економіки" додати слово "оборони" і далі за текстом.	Відхилено	4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;
		-103- Н.д.Семенуха Р.С. (Реєстр.картка №379) Пункт четвертий частини першої статті 6 законопроекту викласти в такій редакції: «4) як установки, системи, об'єкти, мережі підприємств, включених до переліку підприємств, які мають стратегічне значення для економіки і безпеки держави;».	Враховано редакційно	
68.	5) є об'єктами потенційно небезпечних технологій і виробництв.	***-104- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Пункт п'ятий частини першої статті 6 законопроекту викласти в такій редакції: «5) як установки, системи, об'єкти, мережі підприємств, які є об'єктами потенційно небезпечних технологій і	Враховано редакційно	5) є об'єктами потенційно небезпечних технологій і виробництв.

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		виробництв.».		
69.	2. Критерії та порядок віднесення об'єктів до критично важливих об'єктів інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту та проведення аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України.	***-105- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Частину другу статті 6 проекту Закону викласти такій редакції: «2. Критерії та порядок віднесення об'єктів до критично важливих об'єктів інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту затверджуються Кабінетом Міністрів України. При затвердженні критеріїв для віднесення об'єктів до критично важливих об'єктів інфраструктури обов'язково враховуються наступні чинники: чисельність прямих, непрямих, проміжних споживачів послуг (процесів, функцій), якими забезпечує відповідний об'єкт; ступінь залежності інших секторів (галузей, сфер), зазначених в частині першій цієї статті, від послуг (процесів, функцій), якими забезпечує відповідний об'єкт; ступінь та тривалість можливого негативного впливу на стан соціально - економічної безпеки держави, суспільно-політичну ситуацію в державі або на інші сфери у разі виведення з ладу або порушення функціонування відповідного об'єкта; частка на ринку відповідних товарів, робіт, послуг, яку займає підприємство, установа, організація, що на праві власності або іншому законному праві володіє об'єктом, який можна віднести до критично важливих об'єктів інфраструктури; географічні межі поширення можливих негативних наслідків виведення з ладу або порушення функціонування відповідного об'єкта;	Відхилено	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 Кабінетом Міністрів України, а в банківській системі України – Національним банком України.

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		значення конкретного об'єкта для забезпечення належного та достатнього рівня послуг (процесів, функцій) та доступність і придатність альтернативних об'єктів для забезпечення відповідними послугами (процесами, функціями). При затвердженні критеріїв для віднесення об'єктів до критично важливих об'єктів інфраструктури застосовуються міжнародні (європейські) стандарти, зокрема методології Європейського агентства з питань мережевої та інформаційної безпеки (ENISA), з урахуванням особливостей їх застосування в Україні. Кабінет Міністрів України переглядає критерії та порядок віднесення об'єктів до критично важливих об'єктів інфраструктури не рідше ніж один раз за два роки та за необхідності вносить відповідні зміни». ***-106- Н.д.Данченко О.І. (Реєстр.картка №362)*** Частину другу статті 6 доповнити словами "а у банківській системі України – Національним банком України". ***-107- Н.д.Мирний І.М. (Реєстр.картка №402)*** У статті 6: - у частині другій після слова «кіберзахисту» доповнити через кому словами «у тому числі щодо застосування індикаторів кіберзагроз», далі – за текстом; ***-108- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** Статтю 6 проекту Закону доповнити новою частиною третьою такого змісту: «3. Методичне регулювання незалежного аудиту ефективності системи інформаційної безпеки критично важливих об'єктів інфраструктури здійснюється у відповідних нормативно-правових актах з аудиту ефективності інформаційної безпеки, що

Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
Враховано	
Враховано	
Враховано редакційно	3. Вимоги і порядок проведення незалежного аудиту системи інформаційної безпеки на об'єктах критичної інфраструктури встановлюється відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України. Розроблення нормативно–правових актів з незалежного аудиту системи інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		затверджуються Кабінетом Міністрів України. Розроблення нормативно – правових актів з незалежного аудиту ефективності системи інформаційної безпеки здійснюється на засадах міжнародних (європейських) стандартів аудиту. До їх розроблення залучаються заінтересовані органи державної влади, громадські організації у сфері кібербезпеки, незалежні аудитори та експерти, наукові установи».		Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, громадських організацій та наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки.
		-109- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) У частині 3 статті 4 заміть слів «Порядок регулювання незалежного аудиту системи інформаційної безпеки" записати «Вимоги і порядок проведення незалежного аудиту системи інформаційної безпеки".	Враховано	
		-110- Н.д.Данченко О.І. (Реєстр.картка №362) Частину другу статті 6 доповнити словами "а у банківській системі України - Національним банком України".	Враховано	
70.	3. Відповідальність за забезпечення кіберзахисту комунікаційних та технологічних систем критичних інфраструктурних об'єктів, організацію проведення аудиту інформаційної безпеки таких об'єктів покладається на власників та/або керівників підприємств, установ та організацій, віднесених до критично важливих об'єктів інфраструктури.	***-111- Н.д.Семенуха Р.С. (Реєстр.картка №379)*** У зв'язку з цим частину третю статті 6 проекту Закону вважати відповідно частиною четвертою.	Враховано	4. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події в Україні CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.
		-112- Н.д.Семенуха Р.С. (Реєстр.картка №379) Частину четверту статті 6 проекту Закону викласти в такій редакції: «4. Відповідальність за забезпечення	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		кіберзахисту комунікаційних та технологічних систем критичних інфраструктурних об'єктів покладається на власників та/або керівників підприємств, установ та організацій, установки, системи, об'єкти, мережі яких віднесено до критично важливих об'єктів інфраструктури (далі – суб'єкти критичної інформаційної інфраструктури). Суб'єкти критичної інформаційної інфраструктури мають право: безоплатно отримувати від суб'єктів національної системи кібербезпеки інформацію та дані, необхідні для забезпечення належного рівня захисту об'єктів критичної інформаційної інфраструктури, у тому числі, але не виключно інформацію щодо потенційних та реальних загроз для відповідних об'єктів, можливих механізмів та процедур реагування тощо; самостійно розробляти заходи щодо забезпечення інформаційної безпеки об'єктів критичної інформаційної інфраструктури, що не суперечать вимогам цього Закону та прийнятим на його виконання нормативно-правовим актам. Суб'єкти критичної інформаційної інфраструктури зобов'язані: утворювати та забезпечувати функціонування структурних підрозділів (або визначати відповідальних осіб) з питань внутрішнього аудиту ефективності системи інформаційної безпеки відповідних об'єктів критичної інформаційної інфраструктури та забезпечувати організаційну і функціональну незалежність таких структурних підрозділів внутрішнього аудиту (відповідальних осіб); щороку проводити незалежні аудити ефективності системи інформаційної безпеки об'єктів критичної інформаційної інфраструктури з залученням незалежних аудиторів, які мають рівень кваліфікації, підтверджений сертифікатами міжнародного зразка з кібербезпеки, інформаційної безпеки або аудиту інформаційних технологій;

Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		щороку надавати державному центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України звіт про результати незалежного аудиту ефективності системи інформаційної безпеки об'єктів критичної інформаційної інфраструктури; невідкладно інформувати державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України про спроби вчинення кібератак та інші несанкціоновані дії стосовно об'єктів критичної інформаційної інфраструктури, а також здійснювати заходи щодо блокування, усунення або локалізації їх негативних наслідків. Один і той самий аудитор не має права проводити аудит ефективності системи інформаційної безпеки одного й того ж об'єкта критичної інформаційної інфраструктури більше ніж три роки поспіль.» ***-113- Н.д.Гуляєв В.О. (Реєстр.картка №140)*** Частину 3 статті 6 доповнити абзацом такого змісту: «»Власники та/або керівники підприємств, установ та організацій, віднесених до критично важливих об'єктів інфраструктури незалежно від форми власності зобов'язані: - проводити незалежні аудити ефективності системи кіберзахисту з залученням незалежних аудиторів та/або експертів які мають рівень кваліфікації, підтверджений сертифікати міжнародного зразка з кібербезпеки, інформаційної безпеки або аудиту інформаційних технологій; - надавати суб'єктам забезпечення кібербезпеки постійної готовності, в установленому законодавством порядку, відомості про власні об'єкти критичної інформаційної інфраструктури; - призначати члена наглядової ради (в разі, якщо підприємство має наглядову раду), та керівника підприємства бо його заступника, відповідальним за кібербезпеку; - створювати в своїй структурі підрозділ забезпечення кібербезпеки або

Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції

Відхилено

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		уповноважувати окремих осіб чи організації виконувати функції такого підрозділу та забезпечувати їх функціонування. Такий підрозділ має підпорядковуватися безпосередньо особі, відповідальній за кібербезпку; - створювати в своїй структурі підрозділ внутрішнього аудиту кібербезпеки, або уповноважувати окремих осіб чи організації виконувати функції такого підрозділу, забезпечити їх функціонування. Такий підрозділ має підпорядковуватися безпосередньо керівнику організації, звітувати власнику та/або уповноваженому ним органу, та галузевому регулятору з кібербезпеки відповідної галузі; - організовувати негайне інформування галузевого центра реагування та обміну інформацією з кібербезпеки та відповідного цій галузі суб'єкта забезпечення кібербезпеки постійної готовності про спроби вчинення кібератак та інших несанкціонованих дій стосовно об'єктів кібербезпеки, а також здійснювати заходи щодо блокування, усунення або локалізації їх негативних наслідків. 1. Незалежні аудитори та експерти звітують власникам об'єктів критичної інформаційної інфраструктури, відповідальним за кібербезпеку на підприємстві, галузевим регуляторам з кібербезпеки відповідних галузей та суб'єктам забезпечення кібербезпеки постійної готовності щодо результатів аудиту.»		
		-114- Н.д.Мирний І.М. (Реєстр.картка №402) У статті 6: - у частині третій після слів «інфраструктурних об'єктів» доповнити словами через кому «обмін інформацією про інциденти кібербезпеки», далі за текстом;	Враховано	
		-115- Н.д.Мирний І.М. (Реєстр.картка	Враховано частково	5. Обмін інформацією про інциденти

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		№402)		кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України «Про захист персональних даних».
		У статті 6: доповнити новою частиною четвертою такого змісту:		
		«4. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України «Про захист персональних даних». Порядок обміну інформацією про інциденти кібербезпеки визначається Кабінетом Міністрів України за погодженням з Уповноваженим Верховної Радою України з прав людини».		
		-116- Н.д.Сольвар Р.М. (Реєстр.картка №91)	Відхилено	
		Частину 3 ст. 6 проекту доповнити реченням такого змісту:		
		“Державний контроль за станом інформаційної безпеки критичних інформаційних об’єктів здійснюється Державною службою спеціального зв’язку та захисту інформації України”.		
		-117- Н.д.Козир Б.Ю. (Реєстр.картка №127)	Відхилено	
		Частину 3 ст. 6 проекту доповнити реченням такого змісту:		
		“Державний контроль за станом інформаційної безпеки критичних інформаційних об’єктів здійснюється Державною службою спеціального зв’язку та захисту інформації України”.		
71.	Стаття 7.Принципи забезпечення кібербезпеки України			Стаття 7. Принципи забезпечення кібербезпеки
72.	1. Забезпечення кібербезпеки ґрунтується на принципах:			1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:
73.	верховенства права, законності, поваги до основних прав і свобод та захисті особистих свобод, особистої інформації та особистості;	***-118- Н.д.Мирний І.М. (Реєстр.картка №402)***	Враховано	1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту у порядку, визначеному законом;
		У частині першій статті 7:		
		- у абзаці другому слова «основних прав і свобод та захисті особистих свобод, особистої інформації та		

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		особистості» замінити на слова «прав людини і основоположних свобод та їх захисту у порядку, визначеному законом»;		
74.	забезпечення національних інтересів України;			2) забезпечення національних інтересів України;
75.	відкритості, доступності, стабільності та захищеності кіберпростору, розвитку Інтернет та відповідального поводження в кіберпросторі;			3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;
76.	державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;	***-119- Н.д.Мирний І.М. (Реєстр.картка №402)*** У частині першій статті 7 у абзаці п'ятому після слів «у сфері забезпечення кібербезпеки та кіберзахисту» доповнити словами «зокрема шляхом обміну інформацією про інциденти кібербезпеки, спільні наукові та дослідницькі проекти, навчання та підвищення кваліфікації кадрів у сфері кібербезпеки»;	Враховано редакційно	4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, спільні наукові та дослідницькі проекти, навчання та підвищення кваліфікації кадрів у цій сфері;
77.	пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист у разі вчинення певних агресивних дій у кіберпросторі;	***-120- Н.д.Мирний І.М. (Реєстр.картка №402)*** У частині першій статті 7 у абзаці шостому після слів «певних агресивних дій у кіберпросторі» доповнити словами «відповідно до норм міжнародного права»;	Враховано	5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;
78.	пріоритетності запобіжних заходів;			6) пріоритетності запобіжних заходів;
79.	невідворотності покарання за вчинення кіберзлочинів;			7) невідворотності покарання за вчинення кіберзлочинів;
80.	пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;			8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;
81.	міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;			9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;
82.	забезпечення демократичного цивільного контролю над утвореними відповідно до законів	***-121- Н.д.Мирний І.М. (Реєстр.картка №402)***	Враховано	10) забезпечення демократичного цивільного контролю над утвореними відповідно до закону

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.	У частині першій статті 7 у абзаці одинадцятому слова «що діють», замінити словами «що здійснюють діяльність».		України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.
83.	2. Державна політика у сфері кібербезпеки ґрунтується на повазі до норм і принципів міжнародного права, захисті фундаментальних цінностей, визначених Конституцією та законами України, забезпеченні національних інтересів України у кіберпросторі. Кібербезпека є складовою частиною національної безпеки України.	***-122- Н.д.Данченко О.І. (Реєстр.картка №362)*** Вилучити пункт 2 статті 7 проекту.	Враховано	
84.	3. Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки електронних комунікацій та національних інформресурсів є одним з пріоритетів розвитку інформаційного суспільства та цифрового комунікативного простору України, складовою державної політики у сферах електронних комунікацій та інформатизації.	***-123- Н.д.Данченко О.І. (Реєстр.картка №362)*** Вилучити пункт 3 статті 7 проекту.	Враховано	
85.	Стаття 8.Національна система кібербезпеки України			Стаття 8. Національна система кібербезпеки
86.	1.Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів організаційного, правового, політичного, соціально-економічного, науково-технічного, правоохоронного, оборонного, інформаційного, освітнього характеру, заходів із захисту інформації та кіберзахисту.	***-124- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Частину 1 статті 8 викласти у такій редакції: «1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних організаційних, правових, кримінально-процесуальних, оперативно-розшукових, розвідувальних, контррозвідувальних, інженерно-технічних, криптографічних, оборонних заходів, а також заходів політичного, науково-технічного, інформаційного та освітнього характеру».	Враховано редакційно	1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.
		-125- Н.д.Козир Б.Ю. (Реєстр.картка №127) Частину 1 статті 8 викласти у такій редакції: 1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних організаційних,	Враховано редакційно	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		правових, кримінально-процесуальних, оперативно-розшукових, розвідувальних, контррозвідувальних, інженерно-технічних, криптографічних, оборонних заходів, а також заходів політичного, науково-технічного, інформаційного та освітнього характеру.		
87.	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, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:	***-126- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У частині 2 статті 8 та у частині 2 статті 9 (за новою нумерацією) слова «Державна служба спеціального зв'язку та захисту інформації України» замінити на «спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації».	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 органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:
88.	Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту комунікаційних та технологічних систем критичних інфраструктурних об'єктів, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування національної телекомунікаційної мережі, упровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем критичних інфраструктурних об'єктів на вразливість; забезпечує функціонування з цією метою державного центру кіберзахисту;	***-127- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Абзац другий пункту другого статті 8 викласти в такій редакції: «Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, упровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них;	Враховано редакційно	1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування національного

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		забезпечує впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування державного центру кіберзахисту, а також урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.».		центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події в Україні CERT-UA;
		-128- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) У частинах 2 та 5 статті 8, а також у пункті 92 частини 1 статті 14 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" слова «Державний центр кіберзахисту» замінити словами «національний центр кіберзахисту».	Враховано	
		-129- Н.д.Мирний І.М. (Реєстр.картка №402) У статті 8: - у абзаці другому частини другої слова «координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем критичних інфраструктурних об'єктів на вразливість» замінити словами «призначає органи з оцінки відповідності, що здійснюють аудит комунікаційних і технологічних систем критичних інфраструктурних об'єктів на відповідність міжнародним стандартам захищеності від вразливості», слова «функціонування з цією метою державного центру кіберзахисту» замінити словами «функціонування державного центру кіберзахисту для оперативного реагування на	Відхилено	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		кіберінциденти»;		
		-130- Н.д.Сольвар Р.М. (Реєстр.картка №91) В абзаці другому у частині 2 статті 8 проекту слова “захисту у кіберпросторі” замінити словом “кіберзахисту”, а слово “кіберзахисту” після слів “встановлена законом” виключити.	Відхилено	
		-131- Н.д.Бондар В.В. (Реєстр.картка №191) У статті 8 абзац другий частини другої доповнити словами та реченням такого змісту: «у випадку невідповідності та/або відсутності у авторизованого електронного майданчика комплексної системи захисту інформації з підтвердженою відповідністю та/або невикористання засобів захисту інформації відповідно до вимог частин другої та третьої статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», - надсилає подання про скасування авторизації. Орган, що здійснює авторизацію електронних майданчиків, впродовж 3 робочих днів зобов’язаний скасувати авторизацію такого електронного майданчика.».	Відхилено	
		-132- Н.д.Козир Б.Ю. (Реєстр.картка №127) В абзаці другому частини 2 статті 8 слова «захисту у кіберпросторі» замінити словом «кіберзахисту».	Відхилено	
89.	Національна поліція України забезпечує захист прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;	***-133- Н.д.Лук’янчук Р.В. (Реєстр.картка №243)*** Абзацом третім частини 2 статті 8 законопроекту пропонується встановити, що Національна поліція забезпечує захист прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в	Відхилено	2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		кіберпросторі. З огляду на статус та повноваження Національної поліції, визначені статтею 1 і 23 Закону України "Про Національну поліцію" слова "підвищення поінформованості громадян про безпеку в кіберпросторі" пропонується виключити та доповнити нормою, яка б дозволяла здійснювати під час досудового розслідування оперативно-розшукові заходи із запобігання, виявлення та припинення кіберзлочинів.		
90.	Служба безпеки України здійснює заходи з попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні, оперативно-розшукові заходи, інші заходи оперативного реагування та протидії проявам застосування у кіберпросторі засобів та методів розвідувальних операцій (кіберрозвідка), використання Інтернету для цілей терористичної діяльності, зокрема технологічного тероризму (кібертероризм); протидіє кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу національним інтересам України;	***-134- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Абзац четвертий частини 2 статті 8 викласти в такій редакції: «Служба безпеки України здійснює попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які 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, можливі наслідки якої безпосередньо створюють загрозу життєво-важливим інтересам України; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;»	Враховано	3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які 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, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;
		-135- Н.д.Сольвар Р.М. (Реєстр.картка №91) Абзац четвертий у частині 2 статті 8 проекту икласти у такій редакції: «Служба безпеки України здійснює попередження, виявлення, припинення та розкриття злочинів проти	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		миру і безпеки людства, які 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, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на комп'ютерні інциденти у сфері державної безпеки;»		
		-136- Н.д.Козир Б.Ю. (Реєстр.картка №127)	Враховано частково	
		Абзац четвертий частини 2 статті 8 викласти в такій редакції:		
		«Служба безпеки України формує та реалізує державну політику щодо запобігання розвідувально-підривним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, організацій і окремих осіб на кібернетичну безпеку держави; здійснює добування та аналітичну обробку інформації про загрози кібернетичній безпеці України, їх джерела, умови та чинники, що сприяють їх реалізації; проводить контррозвідувальні та оперативно-розшукові заходи з протидії кібершпигунству, кібертероризму, злочинам проти миру і безпеки людства, що вчиняються у кіберпросторі; з використанням форм, методів, засобів		

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		контррозвідувальної діяльності забезпечує контроль стану захищеності від кіберзагроз державних електронних інформаційних ресурсів, іншої електронної інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, розслідування кіберінцидентів та кібератак, розшук осіб, причетних до їх здійснення; розробляє і реалізовує заходи щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян у кіберпросторі».		
91.	Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО, пов'язану з безпекою кіберпростору та сумісним захистом від кіберзагроз;	***-137- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Абзац п'ятий частини 2 статті 8 законопроекту щодо повноважень Міноборони пропонується викласти у редакції: "Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи кібероборони з метою захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройної агресії у кіберпросторі; здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери, пов'язану з безпекою кіберпростору та сумісним захистом від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану".	Враховано частково	4) Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;
92.	розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;			5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;
93.	Національний банк України формує вимоги щодо кібербезпеки критичних інфраструктурних об'єктів в банківській сфері та проведення аудиту інформаційної безпеки таких об'єктів.	***-138- Н.д.Данченко О.І. (Реєстр.картка №362)*** Абзац сьомий частини другої статті 8 викласти в такій редакції:	Враховано редакційно	6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		"Національний банк України визначає критерії та порядок віднесення об'єктів до критичних інфраструктурних об'єктів у банківській системі України, встановлює перелік таких об'єктів, вимоги щодо їх кіберзахисту та аудиту інформаційної безпеки, а також забезпечує проведення аудиту захищеності інформаційно-телекомунікаційних систем критичних інфраструктурних об'єктів у банківській системі України".		їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінки стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.
		-139- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) У пункті 6 частини другої статті 8 та пункті «а» підпункту 1 пункту 2 розділу «Прикінцеві та перехідні положення» проекту, де йдеться про створення Національним банком України «Центру кіберзахисту Національного банку України» слово «центр» записати з маленької літери.	Враховано	
		-140- Н.д.Данченко О.І. (Реєстр.картка №362) Абзац сьомий частини другої статті 8 викласти в такій редакції:: "Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює Центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінки стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України."	Враховано	
94.	3.Функціонування національної системи			3 Функціонування національної системи

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	кібербезпеки забезпечується шляхом:			кібербезпеки забезпечується шляхом:
95.	вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами ЄС та НАТО;			1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;
96.	створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;			2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;
		-141- Н.д.Семенуха Р.С. (Реєстр.картка №379) Частину третю статті 8 проекту Закон після абзацу третього доповнити новим абзацом такого змісту: «встановлення обов'язкових вимог щодо інформаційної безпеки об'єктів критичної інформаційної інфраструктури України, у тому числі при їх створенні, введенні в експлуатацію, експлуатації та модернізації, відповідно до міжнародних (європейських) стандартів та з урахуванням специфіки конкретної галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;».	Враховано редакційно	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;
97.	формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;			4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;
98.	залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;			5) залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;
99.	проведення навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;			6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;
100.	функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;			7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;
101.	розвитку мережі команд реагування на			8) розвитку мережі команд реагування на

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	комп'ютерні надзвичайні події;			комп'ютерні надзвичайні події;
102.	розвитку та вдосконалення системи технічного і криптографічного захисту інформації;			9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;
103.	забезпечення виконання вимог із захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;	***-142- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** В абзаці 10 частини 3 статті 8 після слів "вимога щодо захисту якої встановлена законом" додати слова "згідно вимог законодавства щодо захисту інформації в інформаційно-телекомунікаційних системах";	Враховано редакційно	10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;
104.	створення та забезпечення функціонування національної телекомунікаційної мережі;			11) створення та забезпечення функціонування Національної телекомунікаційної мережі;
		-143- Н.д.Мирний І.М. (Реєстр.картка №402) У статті 8 у частині третій після абзацу восьмого доповнити новим абзацом такого змісту: «обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;	Враховано	12) обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;
		-144- Н.д.Мирний І.М. (Реєстр.картка №402) У статті 8 у частині третій після абзацу восьмого доповнити новим абзацом такого змісту: впровадження єдиної (універсальної) системи індикаторів кіберзагроз відповідно до міжнародних стандартів з питань кібербезпеки та кіберзахисту;	Враховано редакційно	13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;
		-145- Н.д.Мирний І.М. (Реєстр.картка №402) У статті 8 у частині третій після абзацу восьмого доповнити новим абзацом такого змісту: підготовки фахівців освітніх рівнів	Враховано редакційно	14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		«бакалавр» і «магістр» за державним замовленням в обсязі необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації, проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за дотримання правил кібербезпеки на критичних інфраструктурних об'єктах у відповідності з міжнародними стандартами».		за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;
105.	упровадження організаційно-технічної моделі національної системи кібербезпеки, як комплексу заходів, сил та засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, що здатні зменшити вразливості комунікаційних систем;			15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;
106.	встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;			16) встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;
107.	державно-приватного партнерства у запобіганні кіберзагрозам критичним інфраструктурним об'єктам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;			17) державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;
108.	періодичного проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки;			18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;
109.	стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;			19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;
110.	розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які	***-146- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Внести редакційні правки по тексту: словосполучення «сфера забезпечення кібербезпеки» та/або «сфера забезпечення кіберзахисту» замінити відповідно на словосполучення «сфера кіберзахисту» та	Враховано	20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглибленню співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	проводяться під егідою ОБСЄ;	«сфера кібербезпеки».		кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;
111.	здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, проявам застосування у кіберпросторі засобів та методів розвідувальних операцій, використання Інтернету для цілей терористичної діяльності та у військових цілях;	***-147- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** В абзаці 18 частини 3 статті 8 слова «для цілей терористичної діяльності та» виключити, а слова «проявам застосування у кіберпросторі засобів та методів розвідувальних операцій» замінити словами «розвідувально-підривній, терористичній та іншій діяльності на шкоду інтересам України у кіберпросторі»;	Враховано	21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернету у військових цілях;
		-148- Н.д.Козир Б.Ю. (Реєстр.картка №127) В абзаці 18 частини 3 статті 8 слова «проявам застосування у кіберпросторі засобів та методів розвідувальних операцій, використання Інтернету для цілей терористичної діяльності» замінити словами «розвідувально-підривній, терористичній та іншій діяльності на шкоду інтересам України у кіберпросторі;»	Враховано	
		-149- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні правки по тексту законопроекту: словостполучення «у кіберпросторі» замінити на словосполучення «при використанні у кіберпросторі» з урахуванням змісту.	Враховано	
112.	здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони у кіберпросторі, створення, розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі;	***-150- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Внести редакційні правки по тексту законопроекту: словостполучення «у кіберпросторі» замінити на словосполучення «при використанні у кіберпросторі» з урахуванням змісту.	Враховано	22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення, розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;
113.	обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора, визнаної Верховною Радою України, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України,			23) обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю у цій сфері.			агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;
		-151- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Частину 3 статті 8 доповнити новим абзацом такого змісту: «розвитку системи контррозвідувального забезпечення кібербезпеки держави, яку призначено для попередження, своєчасного виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України у кіберпросторі. Усунення умов, що їм сприяють, та причин їх виникнення».	Враховано	24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;
		-152- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні правки по тексту законопроекту: словостполучення «у кіберпросторі» замінити на словосполучення «при використанні у кіберпросторі» - за замістом.	Враховано	
		-153- Н.д.Данченко О.І. (Реєстр.картка №362) частину третю статті 8 законопроекту доповнити новим пунктом 22 такого змісту: «22) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;».	Враховано	25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.
114.	4.Порядок функціонування національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.	***-154- Н.д.Бондар В.В. (Реєстр.картка №191)*** У частині четвертій: після слів «їх тарифікації для користувачів бюджетної сфери» доповнити словами (крім тарифікації послуг недержавних інформаційно-телекомунікаційних систем	Відхилено	4.Порядок функціонування Національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		(авторизованих електронних майданчиків)».
		-155- Н.д.Бондар В.В. (Реєстр.картка №191)
		Частину четверту статті 8 доповнити абзацом такого змісту:
		«У разі, якщо інформаційно-телекомунікаційна система (авторизований електронний майданчик) є власністю держави, Кабінет Міністрів України має право здійснювати тарифікацію надання послуг (державне регулювання цін). В інших випадках тарифікація (ціноутворення) здійснюється вільно, відповідно до вимог законодавства..»
		-156- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)
		Статтю 8 доповнити новою частиною 5 наступного змісту:
		"Упровадження організаційно-технічної моделі національної системи кібербезпеки здійснюється державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до Інтернет, системи антивірусного захисту національних інформресурсів, системи аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розроблює сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань."
		-157- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)
		Доповнити законопроект статтею такого змісту:

Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
Відхилено	
Враховано редакційно	4. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, системи аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, 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.
Враховано	Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA 1. Завданнями CERT-UA є:

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		«Стаття. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA 1. Завданнями CERT-UA є: накопичення та аналіз даних про кіберінциденти, здійснення ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів стосовно цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки, а також власників об'єктів кіберзахисту; підготовка та висвітлення через власний веб-сайт рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у форумі команд реагування на інциденти безпеки FIRST (Forum of Incident Response and Security Team) із сплатою щорічних членських внесків; взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до законів України, підприємствам, установам і організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам. 2. Забезпечення функціонування CERT-UA

Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у форумі команд реагування на інциденти безпеки FIRST (Forum of Incident Response and Security Team) із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		здійснює Державна служба спеціального зв'язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.». Внести відповідні зміни в нумерацію статей.		
115.	Стаття 9.Державно-приватна взаємодія у сфері кібербезпеки			Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки
116.	1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:			1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:
117.	створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;			1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;
118.	підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадження державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;			2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадження державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;
119.	обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичним інфраструктурним об'єктам, інших кіберзагроз, кібератак та кіберінцидентів;			3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;
120.	партнерства та координації команд реагування на комп'ютерні надзвичайні події;			4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;
121.	залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових і галузевих проектів та нормативних документів у сфері кібербезпеки;			5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;
122.	надання консультативної та практичної допомоги з питань реагування на кібератаки.			6) надання консультативної та практичної допомоги з питань реагування на кібератаки;
123.	формування ініціатив та створення авторитетних консультаційних пунктів для громадян, промисловості та бізнесу з метою забезпечення безпеки в Інтернеті;			7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;
124.	запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;			8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;
125.	періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їх ролі у сприянні кращому управлінню			9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	ризиками у сфері кібербезпеки;			управлінню ризиками у сфері кібербезпеки;
126.	створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки.			10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;
		-158- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Доповнити частину 1 статті 9 новим абзацом наступного змісту: «тісної взаємодії з цивільними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою реалізації заходів кібероборони щодо недопущення та відбиття збройної агресії в кіберпросторі»;	Враховано редакційно	11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.
		-159- Н.д.Левченко Ю.В. (Реєстр.картка №223) Доповнити частину 1 статті 9 новим реченням такого змісту: «План та порядок державно-приватної взаємодії у сфері кібербезпеки визначає Кабінет Міністрів України.»	Відхилено	
127.	2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.			2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.
128.	Стаття 10.Сприяння суб'єктам забезпечення кібербезпеки України			Стаття 11. Сприяння суб'єктам забезпечення кібербезпеки України
129.	Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки України, повідомляти дані,			Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.
130.	що стали їм відомі, щодо загроз національній	***-160- Н.д.Лук'янчук Р.В. (Реєстр.картка***	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	безпеці у кіберпросторі, або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації її наслідків.	***№243)*** Внести редакційні правки по тексту законопроекту: словосполучення «у кіберпросторі» замінити на словосполучення «при використанні у кіберпросторі» - за змістом.		
131.	Стаття 11.Відповідальність за порушення законодавства у сфері кібербезпеки			Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки
132.	Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації у яких кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.			Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.
133.	Стаття 12.Фінансове забезпечення заходів кібербезпеки України			Стаття 13. Фінансове забезпечення заходів кібербезпеки
134.	Джерелами фінансування робіт і заходів щодо забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити комерційних банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.			Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.
135.	Стаття 13.Міжнародне співробітництво у сфері кібербезпеки			Стаття 14. Міжнародне співробітництво у сфері кібербезпеки
136.	1.Україна відповідно до укладених нею міжнародних договорів співробітничає в галузі кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.			1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.
137.	2. Керуючись інтересами забезпечення безпеки особи, суспільства і держави, Україна переслідує на своїй території осіб, причетних до кіберзлочинів та/або злочинів терористичної спрямованості у кіберпросторі та/або з його використанням, у тому числі у випадках, коли такі злочини або планувалися або були вчинені поза межами України, але завдають шкоди Україні, та в інших випадках, передбачених міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою	***-161- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Частину 2 статті 13 вилучити.	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	України.			
		-162- Н.д.Левченко Ю.В. (Реєстр.картка №223) Частину 2 статті 13 вилучити.	Враховано	
138.	3.Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах кіберзахисту, зокрема проведенні спільних навчань суб'єктів сектору безпеки і оборони, у рамках заходів колективної оборони з дотриманням вимог законів України "Про порядок направлення підрозділів Збройних Сил України до інших держав" та "Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України".	***-163- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У частині 3 статті 13 слово «кіберзахисту» замінити словами «забезпечення кібербезпеки».	Враховано	2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України "Про порядок направлення підрозділів Збройних Сил України до інших держав" та "Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України".
		-164- Н.д.Козир Б.Ю. (Реєстр.картка №127) У частині 3 статті 13 слово «кіберзахисту» замінити словами «забезпечення кібербезпеки».	Враховано	
139.	4.Відповідно до законодавства України у сфері зовнішніх зносин, суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.			3. Відповідно до законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.
140.	5.Інформацію іноземній державі з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана і без попереднього запиту іноземної держави, якщо це не зашкоджує проведенню досудового розслідування чи судового розгляду справи і може допомогти компетентним органам іноземної держави у припиненні кібератаки, оперативній протидії кримінальному злочину у кіберпросторі.	***-165- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У другому реченні частини 5 статті 13 слова «оперативній протидії кримінальному злочину» замінити словами «своєчасному виявленню і припиненню кримінального правопорушення».	Враховано	4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.
		-166- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні правки по тексту законопроекту: словостполучення «у кіберпросторі» замінити на словосполучення «при використанні у кіберпросторі» - за змістом.	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		-167- Н.д.Козир Б.Ю. (Реєстр.картка №127) У другому реченні частини 5 статті 13 слова «оперативній протидії кримінальному злочину у кіберпросторі» замінити словами «своєчасному виявленню і припиненню кримінального правопорушення у кіберпросторі».	Враховано	
141.	Стаття 14.Контроль за законністю заходів із забезпечення кібербезпеки України			Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України
142.	1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.			1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.
		-168- Н.д.Мирний І.М. (Реєстр.картка №402) Доповнити частину першу статті 14 другим реченням такого змісту: «Парламентський контроль за дотримання законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснює Уповноважений Верховної Ради України з прав людини».	Враховано	Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснює Уповноважений Верховної Ради України з прав людини.
143.	2. Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України.			2. Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України.
		-169- Н.д.Семенуха Р.С. (Реєстр.картка №379) Статтю 14 проекту Закону доповнити новою частиною третьою такого змісту, змінивши відповідно нумерацію наступної частини цієї статті: «3. Незалежний аудит діяльності основних суб'єктів національної кібербезпеки, визначених у частині другій статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щорічно за міжнародними стандартами аудиту.	Враховано редакційно	3. Незалежний аудит діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту. Звіти про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап'ятиденний строк після закінчення

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		Звіти про результати незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених у частині другій статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у 45-денний строк після закінчення календарного року. Комітет Верховної Ради України, до предмету відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмету відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених у частині другій статті 8 цього Закону, про результати незалежного аудиту їх діяльності щодо ефективності системи забезпечення кібербезпеки держави. Верховна Рада на пленарному засіданні один раз на рік розглядає звіти основних суб'єктів національної кібербезпеки, визначених у частині другій статті 8 цього Закону, про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати незалежного аудиту їх діяльності. Верховна Рада за пропозицією Голови Верховної Ради України, або за пропозицією одного з комітетів, зазначених в абзаці третьому цієї частини статті, або не менш як однієї третини народних депутатів від конституційного складу Верховної Ради, може в будь-який час прийняти рішення про заслуховування позачергового звіту суб'єкта національної кібербезпеки, визначеного у частині другій статті 8

Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції

календарного року.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб'єктів національної кібербезпеки Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, може порушити питання про розгляд цих питань на засіданні Верховної Ради України.

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		цього Закону, про стан виконання ним заходів з питань забезпечення кібербезпеки держави, віднесених до його компетенції.».		
		-170- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) **У частині 3 статті 14 (15) уточнити, хто саме проводить незалежний аудит діяльності основних суб'єктів національної кібербезпеки.**	На розгляд Комітету	
		-171- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) **У частині 3 статті 14 (15) уточнити, що собою являють «міжнародні стандарти аудиту»**	На розгляд Комітету	
		-172- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) **Привести частину 3 статті 14 (15) у відповідність до вимог Конституції України та рішень Конституційного Суду України у частині повноважень Комітетів Верховної Ради України.**	На розгляд Комітету	
144.	3. Нагляд за додержанням вимог законодавства державними органами, які беруть участь в забезпеченні кібербезпеки, здійснюється Генеральним прокурором України та уповноваженими ним прокурорами в порядку, визначеному законами України.	***-173- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Частину 3 статті 14 вилучити.	Враховано	
		-174- Н.д.Семенуха Р.С. (Реєстр.картка №379) Частину четверту статті 14 проекту Закону (відповідно до нумерації частин статті 14 проекту з урахуванням зазначеної вище пропозиції № 10) виключити.	Враховано	
		-175- Н.д.Левченко Ю.В. (Реєстр.картка №223) Частину 3 статті 14 вилучити.	Враховано	
		-176- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні зміни по тексту проекту:	Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		замінити словосполучення «критично важливі об'єкти інфраструктури» замінити на словосполучення «об'єкти критичної інфраструктури».		
		-177- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні зміни по тексту законопроекту: замінити словосполучення «державно-приватне партнерство» на словосполучення «державно-приватна взаємодія».	Враховано	
		-178- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні зміни по тексту: словостполучення «сфера забезпечення кібербезпеки» чи «сфера забезпечення кіберзахисту» замінити на «сфера кібербезпеки» чи «сфера кіберзахисту»	Враховано	
		-179- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Внести редакційні правки по тексту законопроекту: словостполучення «у кіберпросторі» замінити на словосполучення «при використанні у кіберпросторі».	Враховано	
145.	ПРИКІНЦЕВІ ПОЛОЖЕННЯ			ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ
146.	1. Цей Закон набирає чинності через шість місяців з дня його опублікування.			1. Цей Закон набирає чинності через шість місяців з дня його опублікування.
147.	2. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:			2. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:
148.	привести власні нормативно-правові акти у відповідність із цим Законом;			забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону;
149.	видати нормативно-правові акти, що випливають із цього Закону;			привести свої нормативно-правові акти у відповідність із цим Законом;
150.	забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону, видання зазначеними органами актів, що випливають із цього Закону.			забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.
151.	3. Внести наступні зміни до Закону України "Про основи національної безпеки України" (Відомості Верховної Ради України, 2003, № 39, ст.351, 2006, № 14, ст.116, 2010, № 40, ст.527, 2013, № 14, ст.89, 2013, № 38, ст.499, 2014, № 10, ст.119, 2014, № 22, ст.816, 2015, № 4, ст.13, 2015, № 16, ст.110, 2015, №	***-180- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Оскільки стаття 1 запроваджує нову термінологію, розділ «Прикінцеві положення» доповнити відповідними змінами до Законів України «Про засади	Відхилено	3. Внести зміни до таких законів України:

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
	39, ст.375):	внутрішньої і зовнішньої політики», «Про основи національної безпеки України» та «Про боротьбу з тероризмом».		
		-181- Н.д.Семенуха Р.С. (Реєстр.картка №379) Пункт 3 Прикінцевих положень проекту Закону виключити.	Відхилено	1) у Законі України "Про основи національної безпеки України" (Відомості Верховної Ради України, 2003 р., № 39, ст. 351, 2006 р., № 14, ст. 116, 2010 р., № 40, ст. 527; 2015 р., № 16, ст. 110):
152.	1)у абзаці третьому статті 1 після слів "інформаційної безпеки," додати слова "кібербезпеки та кіберзахисту,";			а) в абзац другий статті 1 після слів "інформаційної безпеки" доповнити словами "кібербезпеки та кіберзахисту";
153.	2)у абзаці третьому статті 2 перше і друге речення після слів "Стратегія національної безпеки України" доповнити словами "Стратегія кібербезпеки України";			б) частину другу статті 2 після слів "Стратегія національної безпеки України" доповнити словами "Стратегія кібербезпеки України";
154.	3) абзац п'ятий статті 9 після слів "Стратегії національної безпеки України" доповнити словами "Стратегії кібербезпеки України";			в) абзац четвертий статті 9 та абзац другий статті 10 після слів "Стратегії національної безпеки України" доповнити словами "Стратегії кібербезпеки України".
155.	4)абзац третій статті 10 після слів "Стратегії національної безпеки України" доповнити словами "Стратегії кібербезпеки України".			
		-182- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) В розділі «Прикінцеві положення» внести наступні зміни до Закону України «Про оборону України»: Статтю 3 Закону України «Про оборону України» доповнити абзацом наступного змісту: «здійснення заходів з кібероборони (активного кіберзахисту) держави для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії». Абзац третій статті 4 Закону України «Про оборону України» після слів «розпочинають воєнні дії» доповнити словами «… у тому числі проведення в кіберпросторі спеціальних (розвідувальних, інформаційно-психологічних та кібер) операцій».	Враховано	2) у Законі України "Про оборону України" (Відомості Верховної Ради України, 2000 р., № 49, ст. 420; 2011 р., № 4, ст. 27; 2015 р., № 16, ст. 110; 2016 р., № 33, ст. 564): а) статтю 3 після абзацу дев'ятнадцятого доповнити новим абзацом такого змісту: «здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії». У зв'язку з цим абзац двадцятий вважати абзацом двадцять першим; б) частину другу статті 4 доповнити словами «у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі»;

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		-183- Н.д.Лук'янчук Р.В. (Реєстр.картка №243) Оскільки статтею 8 проекту на суб'єктів національної системи кібербезпеки покладені певні завдання у сфері кібербезпеки, розділ «Прикінцеві положення» доповнити змінами до базових законодавчих актів, які регулюють діяльність вказаних суб'єктів, зокрема - Законів України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про Національну поліцію України», «Про Службу безпеки України», «Про Збройні Сили України», «Про розвідувальні органи України», «Про Національний банк України». ***-184- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** В розділі «Прикінцеві положення» внести

Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
Враховано частково	3) у Законі України "Про Державну службу спеціального зв'язку та захисту інформації України" (Відомості Верховної Ради України, 2014 р., № 25, ст. 890, № 29, ст. 946): а) частину першу статті 2 та абзац другий частини першої статті 3 після слів «криптографічного та технічного захисту інформації» доповнитии словом «кіберзахисту»; б) у частині першій статті 14 пункту 39 після слів «забезпечення функціонування» доповнити словом «урядової», далі за текстом; доповнити пунктами 85-92 такого змісту: «85) формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах; 86) координація діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту; 87) забезпечення створення та функціонування Національної телекомунікаційної мережі; 88) впровадження організаційно-технічної моделі кіберзахисту, здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; 89) інформування про кіберзагрози та відповідні методи захисту від них; 90) забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації); 91) координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; 92) забезпечення функціонування національного центру кіберзахисту»;
Враховано	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		наступні зміни до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»: «Внести наступні зміни до Законі України "Про Державну службу спеціального зв'язку та захисту інформації, 2006, № 51, ст.519, 2007, № 33, ст.442, 2008, № 5-6, № 7-8, ст.78, 2009, № 24, ст.296, 2009, № 32-33, ст.485, 2009, № 41, ст.601, 2010, № 33, ст.471, 2011, № 10, ст.63, 2012, № 7, ст.53, 2013, № 14, ст.89, 2014, № 11, ст.132, 2014, № 12, ст.178, 2014, № 22, ст.811, 2014, № 12, ст.189, 2014, № 17, ст.593, 2014, № 20-21, ст.745, 2014, № 22, ст.816, 2014, № 25, ст.890, 2014, № 29, ст.946, 2015, № 35, ст.339, 2015, № 52, ст.482): 1) в частині першій статті 2 та в абзаці другому частини першої статті 3 після слів «криптографічного та технічного захисту інформації» додати слово «кіберзахисту»; 2) частину першу статті 14 доповнити новими абзацами XX такого змісту: «86) формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах; 87) координація діяльності суб'єктів кібербезпеки щодо кіберзахисту; 88) забезпечення створення та функціонування національної телекомунікаційної мережі, упровадження організаційно-технічної моделі кіберзахисту; 89) здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; 90) інформування про кіберзагрози та відповідні методи захисту від них; 91) координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; 92) забезпечення функціонування

Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		Державного центру кіберзахисту та протидії кіберзагрозам. ***-185- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** У пункті 92 частини 1 статті 14 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" слова «Державний центр кіберзахисту» замінити словами «національний центр кіберзахисту». ***-186- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** В розділі «Прикінцеві положення» внести наступні зміни до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»: «Внести наступні зміни до Закону України "Про інформацію" (Відомості Верховної Ради України, 2011 р., № 32, ст. 313): 1). статтю 10 після абзацу десятого доповнити новим абзацом такого змісту: "технологічна інформація;". У зв'язку з цим абзац одинадцятий вважати абзацом дванадцятим. 2). Доповнити Закон статтею 191 такого змісту: "Стаття 191. Технологічна інформація 1. Технологічна інформація — документовані відомості про склад, кількісні та якісні показники, особливості технологічних процесів, які застосовуються для керування об'єктами виробничого та невиробничого призначення у різних галузях господарства протягом їх життєвого циклу, а також дані автоматизованих систем керування зазначеними об'єктами та систем управління технологічними процесами на таких об'єктах. 2. Правовий режим технологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України. 3. Технологічна інформація щодо об'єктів життєзабезпечення, транспортної, інформаційної та/або телекомунікаційної

Висновки, обгрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
Враховано	
Враховано	4) у Законі України “Про інформацію” (Відомості Верховної Ради України, 2011 р., № 32, ст. 313 із наступними змінами): а) статтю 10 після абзацу десятого доповнити новим абзацом такого змісту: “технологічна інформація”. У зв’язку з цим абзац одинадцятий вважати абзацом дванадцятим; б) доповнити статтею 19^1 такого змісту: “Стаття 19^1. Технологічна інформація 1. Технологічна інформація — це документовані відомості про склад, кількісні та якісні показники, особливості технологічних процесів, які застосовуються для керування об’єктами виробничого та невиробничого призначення у різних галузях господарства протягом їхнього життєвого циклу, а також дані автоматизованих систем керування зазначеними об’єктами та систем управління технологічними процесами на таких об’єктах. 2. Правовий режим технологічної інформації визначається законами та міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України. 3. Технологічна інформація щодо об’єктів життєзабезпечення, транспортної, інформаційної та/або телекомунікаційної інфраструктури, об’єктів підвищеної небезпеки, інших об’єктів, порушення сталого функціонування яких може спричинити аварії та/або надзвичайні ситуації, негативно вплинути на стан здоров’я та безпеку людей, умови їхнього життя, становлять підвищену небезпеку для обороноздатності держави, стану навколишнього природного

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		інфраструктури, об'єктів підвищеної небезпеки, інших об'єктів, порушення сталого функціонування яких може спричинити аварії та/або надзвичайні ситуації, негативно вплинути на стан здоров'я та безпеку людей, умови їх життя, несе підвищену небезпеку для обороноздатності держави, стану довкілля, економічної, політичної, соціальної стабільності суспільних відносин або провадження суб'єктами господарювання діяльності, підлягає захисту згідно із законодавством. Технологічна інформація щодо окремих об'єктів (груп чи типів об'єктів) може бути віднесена у порядку, передбаченому законом, до інформації з обмеженим доступом.». ***-187- Н.д.Лук'янчук Р.В. (Реєстр.картка №243)*** Відповідне доповнення у «Прикінцевих положеннях» необхідно внести до Закону України «Про боротьбу з тероризмом». ***-188- Н.д.Данченко О.І. (Реєстр.картка №362)*** "Прикінцеві положення" доповнити новим пунктом такого змісту. "4. У Законі України "Про Національний банк України" (Відомості Верховної Ради України, 1999, N 29 (23.07.99), ст. 238 із подальшими змінами та доповненнями): 1) статтю 7 доповнити новими пунктами 32-33 такого змісту: "32) визначає критерії та порядок віднесення об'єктів до критичних інфраструктурних об'єктів у банківській системі України, встановлює перелік таких об'єктів, вимоги щодо їх кіберзахисту та аудиту інформаційної безпеки, а також забезпечує проведення аудиту захищеності інформаційно-телекомунікаційних систем критичних інфраструктурних об'єктів у банківській

Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції

середовища, економічної, політичної, соціальної стабільності суспільних відносин або провадження суб'єктами господарювання діяльності, підлягає захисту згідно із законодавством.

Технологічна інформація щодо окремих об'єктів (груп чи типів об'єктів) може бути віднесена до інформації з обмеженим доступом у порядку, передбаченому законом»;

Відхилено

Враховано редакційно

5) у Законі України "Про Національний банк України" (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами):

а) статтю 7 доповнити пунктами 32 і 33 такого змісту:

«32) визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;

33) забезпечує формування та ведення реєстру об'єктів критичної інфраструктури у банківській системі України; визначає критерії та порядок віднесення об'єктів у банківській системі України до об'єктів критичної інфраструктури; забезпечує проведення оцінки стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		системі України; 33) створює та забезпечує функціонування системи кіберзахисту в банківській системі України. 2) частину третю статті 22 викласти у такій редакції: “Для перевезення цінностей, охорони цінностей та належних йому об’єктів Національний банк має право створювати підрозділ відомчої охорони та підрозділи перевезення цінностей, озброєні бойовою вогнепальною зброєю. Підрозділ відомчої охорони та підрозділи перевезення цінностей в межах повноважень, наданих цим Законом, мають право застосовувати заходи фізичного впливу, спеціальні засоби оборони і бойову вогнепальну зброю в порядку, передбаченому частиною першою статті 42, статтями 43, 44, частиною першою, підпунктом «а» пункту 2, підпунктом «а» пункту 3, підпунктом «а» пункту 6 частини третьої, пунктом 1 частини четвертої статті 45, пунктами 1, 4, 6, 7 частини четвертої, частиною п’ятою, пунктами 1, 2, 4, 5 частини шостої, частинами сьомою-тринадцятою статті 46 Закону України “Про Національну поліцію”.		інфраструктури у банківській системі України”;» б) частину четверту статті 22 викласти в такій редакції: “Для перевезення цінностей, охорони цінностей та належних йому об’єктів Національний банк має право створювати підрозділ відомчої охорони та підрозділи перевезення цінностей, озброєні бойовою вогнепальною зброєю. Підрозділ відомчої охорони та підрозділи перевезення цінностей в межах повноважень, наданих цим Законом, мають право застосовувати заходи фізичного впливу, спеціальні засоби оборони і бойову вогнепальну зброю в порядку, передбаченому частиною першою статті 42, статтями 43, 44, частиною першою, підпунктом «а» пункту 2, підпунктом «а» пункту 3, підпунктом «а» пункту 6 частини третьої, пунктом 1 частини четвертої статті 45, пунктами 1, 4, 6, 7 частини четвертої, частиною п’ятою, пунктами 1, 2, 4, 5 частини шостої, частинами сьомою - тринадцятою статті 46 Закону України “Про Національну поліцію”;
		-189- Н.д.Лук’янчук Р.В. (Реєстр.картка №243) У пункті «а» підпункту 1 пункту 2 розділу «Прикінцеві та перехідні положення» проекту, де йдеться про створення Національним банком України «Центру кіберзахисту Національного банку України» слово «центр» записати з маленької літери.	Враховано	
		-190- Н.д.Лук’янчук Р.В. (Реєстр.картка №243) Вилучити з Прикінцевих та перехідних положень внесення змін до частини 4 статті 22	На розгляд Комітету	

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Закону України "Про Національний банк України".		
		-191- Н.д.Данченко О.І. (Реєстр.картка №362)	Враховано частково	
		Пропозиції НБУ		
		"Прикінцеві положення" доповнити новим пунктом такого змісту.	На розгляд Комітету	
		"4. У Законі України "Про Національний банк України" (Відомості Верховної Ради України, 1999, N 29 (23.07.99), ст. 238 із подальшими змінами та доповненнями):	Пункт другий цієї поправки	
		1) статтю 7 доповнити новими пунктами 32-33 такого змісту:		
		"32) визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює Центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;		
		33) забезпечує формування та ведення реєстру об'єктів критичної інфраструктури у банківській системі України; визначає критерії та порядок віднесення об'єктів у банківській системі України до об'єктів критичної інфраструктури; забезпечує проведення оцінки стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України";		
		2) частину четверту статті 22 викласти в такій редакції:		
		"Для перевезення цінностей, охорони цінностей та належних йому об'єктів Національний банк має право створювати підрозділ відомчої охорони та підрозділи перевезення цінностей, озброєні бойовою вогнепальною зброєю. Підрозділ відомчої охорони та підрозділи перевезення цінностей в межах повноважень, наданих цим Законом,		

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту
		мають право застосовувати заходи фізичного впливу, спеціальні засоби оборони і бойову вогнепальну зброю в порядку, передбаченому частиною першою статті 42, статтями 43, 44, частиною першою, підпунктом «а» пункту 2, підпунктом «а» пункту 3, підпунктом «а» пункту 6 частини третьої, пунктом 1 частини четвертої статті 45, пунктами 1, 4, 6, 7 частини четвертої, частиною п'ятою, пунктами 1, 2, 4, 5 частини шостої, частинами сьомою - тринадцятою статті 46 Закону України "Про Національну поліцію" ***-192- Н.д.Бондар В.В. (Реєстр.картка №191)*** Прикінцеві положення Законопроекту доповнити пунктами 4-5 такого змісту: «4. У частині другій статті 15 Закону України «Про електронні документи та електронний документообіг» (Відомості Верховної Ради України, 2003 р., № 36, ст. 275) після слів «державні інформаційні ресурси» доповнити словами «(у тому числі в електронних майданчиках з/без використання системи хмарних обчислень), слова «відповідно до законодавства» замінити словами «відповідно до вимог частин другої та третьої статті 8, статті 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» **та одночасно мати належний захист інформації в системах де використовується технологія хмарних обчислень.** 5. До приведення законодавства у відповідність із цим Законом закони України та інші нормативно-правові акти застосовуються в частині, що не суперечить цьому Закону.». ***-193- Н.д.Данченко О.І. (Реєстр.картка №362)***

Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
Відхилено	
Враховано	6) у Законі України «Про розвідувальні органи України» (Відомості Верховної Ради України, 2001, № 19, ст. 94 із наступними змінами):

	Редакція, прийнята в першому читанні	Пропозиції та поправки до проекту	Висновки, обґрунтування	Законопроект, запропонований головним комітетом в остаточній редакції
		Доповнити підпунктами такого змісту: «7) у Законі України «Про розвідувальні органи України» (Відомості Верховної Ради України, 2001, № 19, ст. 94 із наступними змінами): а) абзац другий статті 1 після слів «за межами України» доповнити словами «у тому числі у кіберпросторі»; б) абзац шостий статті 4 після слів «національній безпеці України» доповнити словами «у тому числі у кіберпросторі»; 8) абзац шостий статті 3 Закону України «Про Службу зовнішньої розвідки України» (Відомості Верховної Ради України, 2006, № 8, ст. 94 із наступними змінами) після слів «національній безпеці України» доповнити словами «у тому числі у кіберпросторі».		а) абзац другий статті 1 після слів «за межами України» доповнити словами «у тому числі у кіберпросторі»; б) абзац шостий статті 4 після слів «національній безпеці України» доповнити словами «у тому числі у кіберпросторі»; 7) абзац шостий статті 3 Закону України «Про Службу зовнішньої розвідки України» (Відомості Верховної Ради України, 2006, № 8, ст. 94 із наступними змінами) після слів «національній безпеці України» доповнити словами «у тому числі у кіберпросторі».

156. **Голова Верховної Ради України**