ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

{Із змінами, внесеними згідно із Законами
№ 2469-VIII від 21.06.2018*, ВВР, 2018, № 31, ст.241*
№ 720-IX від 17.06.2020*, ВВР, 2020, № 47, ст.408*
№ 912-IX від 17.09.2020
№ 1591-IX від 30.06.2021*, ВВР, 2023, №№ 10-11, ст.26 - вводиться в дію з* 01.08.2022
№ 1882-IX від 16.11.2021*, ВВР, 2023, № 5, ст.13*
№ 1907-IX від 18.11.2021*, ВВР, 2023, № 11, ст.27*
№ 1953-IX від 14.12.2021*, ВВР, 2023, № 3-4, ст.10*
№ 2130-IX від 15.03.2022*, ВВР, 2023, № 16, ст.63*
№ 2470-IX від 28.07.2022
№ 3549-IX від 16.01.2024*, ВВР, 2024, № 18, ст.76*
№ 3783-IX від 05.06.2024*, ВВР, 2024, № 40, ст.252*
№ 4070-IX від 20.11.2024
№ 4336-IX від 27.03.2025*}*

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.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

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;

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 під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

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; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

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;

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;

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

{Пункт 7 частини першої статті 1 в редакції Закону № 4336-IX від 27.03.2025}

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;

9) кіберзлочинність - сукупність кіберзлочинів;

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;

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 даних;

12) кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура - сукупність об'єктів критичної інформаційної інфраструктури;

{Пункт 16 частини першої статті 1 виключено на підставі Закону № 1882-IX від 16.11.2021}

17) Національна електронна комунікаційна мережа - сукупність спеціальних електронних комунікаційних мереж, спеціальних інформаційно-комунікаційних систем, систем спеціального зв'язку, інших електронних комунікаційних систем, які використовуються в інтересах державних органів та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначених для передавання, приймання, створення, оброблення, зберігання та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим користувачам;

{Пункт 17 частини першої статті 1 в редакції Закону № 4070-IX від 20.11.2024}

18) 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;

18[1]) Національний центр резервування державних інформаційних ресурсів - організована сукупність об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання

національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій;

{Частину першу статті 1 доповнено пунктом 18[1] згідно із Законом № 1907-IX від 18.11.2021}

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

{Пункт 19 частини першої статті 1 в редакції Закону № 4336-IX від 27.03.2025}

20) система управління технологічними процесами (далі - технологічна система) - автоматизована або 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;

21) 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-комунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних;

{Пункт 21 частини першої статті 1 із змінами, внесеними згідно із Законом № 4070-IX від 20.11.2024}

22) система активної протидії агресії у кіберпросторі - сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

{Частину першу статті 1 доповнено пунктом 22 згідно із Законом № 2470-IX від 28.07.2022}

23) активна протидія агресії у кіберпросторі - дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України;

{Частину першу статті 1 доповнено пунктом 23 згідно із Законом № 2470-IX від 28.07.2022}

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

{Частину першу статті 1 доповнено пунктом 24 згідно із Законом № 4336-IX від 27.03.2025}

25) реагування на кіберінциденти - структурована сукупність дій, спрямованих на підготовку до кіберінцидентів, їх виявлення та аналіз, мінімізацію шкоди від кіберінциденту та запобігання їх повторенню у майбутньому.

{Частину першу статті 1 доповнено пунктом 25 згідно із Законом № 4336-IX від 27.03.2025}

Терміни "національна безпека", "національні інтереси", "загрози національній безпеці" вживаються в цьому Законі у значенні, визначеному Законом України "Про основи національної безпеки України". Термін "об'єкт критичної інфраструктури" вживається в цьому Законі у значенні, визначеному Законом України "Про критичну інфраструктуру".

{Частина друга статті 1 із змінами, внесеними згідно із Законом № 1882-IX від 16.11.2021}

Термін "платіжний ринок" вживається в цьому Законі у значенні, наведеному в Законі України "Про платіжні послуги".

{Статтю 1 доповнено частиною третьою згідно із Законом № 1591-IX від 30.06.2021 - вводиться в дію з 01.08.2022}

Терміни "спеціальна електронна комунікаційна мережа", "спеціальна інформаційно-комунікаційна система" вживаються в цьому Законі у значеннях, наведених у Законі України "Про Національну систему конфіденційного зв'язку".

{Статтю 1 доповнено частиною четвертою згідно із Законом № 4070-IX від 20.11.2024}

Стаття 2. Принципи застосування Закону

1. Цей Закон не поширюється на:

1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

{Пункт 2 частини першої статті 2 виключено на підставі Закону № 4336-IX від 27.03.2025}

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;

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).

2. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

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;

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;

3) забезпечення захисту прав користувачів інформаційно-комунікаційних систем, послуг із захисту інформації та кіберзахисту, споживачів електронних комунікаційних послуг, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

{Пункт 3 частини другої статті 2 в редакції Закону № 4070-IX від 20.11.2024}

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);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

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:

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;

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;

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.

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону.

Стаття 3. Правові основи забезпечення кібербезпеки України

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.

Стаття 4. Об'єкти кібербезпеки та кіберзахисту

1. Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

2. Об'єктами кіберзахисту є:

1) інформаційні, електронні комунікаційні та інформаційно-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;

{Пункт 1 частини другої статті 4 із змінами, внесеними згідно із Законом № 4336-IX від 27.03.2025}

2) об'єкти критичної інформаційної інфраструктури;

3) інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

{Пункт 3 частини другої статті 4 із змінами, внесеними згідно із Законом № 4336-IX від 27.03.2025}

3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури 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.

{Абзац перший частини третьої статті 4 із змінами, внесеними згідно із Законом № 4336-IX від 27.03.2025}

Повноваження щодо формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, регулювання та нагляд за діяльністю на яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг покладаються на Національний банк України.

{Абзац другий частини третьої статті 4 із змінами, внесеними згідно із Законом № 1953-IX від 14.12.2021}

4. Обов'язковою умовою використання програмного забезпечення та комунікаційного (мережевого) обладнання в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також на об'єктах критичної інформаційної інфраструктури є відсутність таких продуктів та обладнання у відкритому переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання.

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

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

{Статтю 4 доповнено частиною четвертою згідно із Законом № 4336-IX від 27.03.2025}

Стаття 5. Суб'єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та загальний контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, загальну

координацію суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози; подає до Ради національної безпеки і оборони України пропозиції щодо оголошення кризової ситуації в кібербезпеці; координує реалізацію Стратегії кібербезпеки України, подає до Ради національної безпеки і оборони України пропозиції щодо формування та уточнення Стратегії, у тому числі з урахуванням положень Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2 Directive); визначає пріоритети, розробляє концептуальні засади та вносить Президентові України пропозиції щодо проведення кібероперацій стратегічного рівня в інтересах національної безпеки і оборони та забезпечує координацію суб'єктів сектору безпеки і оборони щодо їх проведення; координує стратегічні комунікації у сфері кібербезпеки.

{Частина друга статті 5 в редакції Закону № 4336-IX від 27.03.2025}

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; затверджує національний план реагування; затверджує загальні вимоги з кіберзахисту об'єктів критичної інфраструктури; затверджує порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (крім систем та об'єктів банків); встановлює порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, з правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності.

{Частина третя статті 5 із змінами, внесеними згідно із Законом № 1953-IX від 14.12.2021; в редакції Закону № 4336-IX від 27.03.2025}

4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

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

{Пункт 7 частини четвертої статті 5 в редакції Закону № 4336-IX від 27.03.2025}

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.

5. Суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Стаття 5[1]. Підрозділи з кіберзахисту, керівники з кіберзахисту

1. В органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, утворюються підрозділи з кіберзахисту та призначаються керівники з кіберзахисту, яким безпосередньо підпорядковуються такі підрозділи, а в органах місцевого самоврядування - особи, які виконують їхні функції та завдання.

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

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

У разі ненадання Державною службою спеціального зв’язку та захисту інформації України протягом одного календарного місяця з дня отримання нею звернення вмотивованої відмови у погодженні призначення керівника з кіберзахисту із зазначенням підстави, визначеної відповідним порядком, таке погодження вважається наданим.

2. Керівники з кіберзахисту або відповідальні особи, які виконують функції та завдання керівника з кіберзахисту, здійснюють керівництво, координацію та контроль з питань кіберзахисту відповідного об’єкта критичної інформаційної інфраструктури або органу державної влади, органу місцевого самоврядування, що є власником або розпорядником

інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, у тому числі в разі введення воєнного стану.

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

{Закон доповнено статтею 5[1] згідно із Законом № 4336-IX від 27.03.2025}

Стаття 6. Кіберзахист критичної інфраструктури

1. Посадові особи операторів критичної інфраструктури, власників або розпорядників об'єктів критичної інформаційної інфраструктури зобов'язані забезпечувати дотримання вимог з кіберзахисту, повідомляти в установленому порядку про кіберінциденти, кібератаки, кіберзагрози, виконувати інші зобов'язання щодо захисту інформації та кіберзахисту відповідно до законодавства, а також несуть відповідальність за невиконання таких вимог згідно із законом.

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

{Стаття 6 із змінами, внесеними згідно із Законами № 1591-IX від 30.06.2021, № 1882-IX від 16.11.2021; в редакції Закону № 4336-IX від 27.03.2025}

Стаття 7. Принципи забезпечення кібербезпеки

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

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;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

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;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Стаття 8. Національна система кібербезпеки

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.

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

{Абзац перший частини другої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

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

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

{Пункт 1 частини другої статті 8 із змінами, внесеними згідно із Законом № 2470-IX від 28.07.2022; в редакції Закону № 4336-IX від 27.03.2025}

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

{Пункт 2 частини другої статті 8 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020; в редакції Закону № 4336-IX від 27.03.2025}

3) Служба безпеки України відповідно до закону здійснює заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки України, миру і безпеки людства, а також кримінальних правопорушень терористичної спрямованості, що вчиняються у кіберпросторі або з його використанням; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом, кібердиверсіями та кібершпигунством; координує діяльність суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям; негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки;

{Пункт 3 частини другої статті 8 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020; в редакції Закону № 4336-IX від 27.03.2025}

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, міжнародними організаціями та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз;

{Пункт 4 частини другої статті 8 в редакції Законів № 3549-IX від 16.01.2024, № 3783-IX від 05.06.2024}

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

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

{Пункт 6 частини другої статті 8 в редакції Законів № 1591-IX від 30.06.2021, № 4336-IX від 27.03.2025}

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

{Частину другу статті 8 доповнено пунктом 7 згідно із Законом № 4336-IX від 27.03.2025}

{Частина друга статті 8 із змінами, внесеними згідно із Законом № 4070-IX від 20.11.2024}

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

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

{Пункт 1 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

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

{Пункт 2 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

{Пункт 3 частини третьої статті 8 виключено на підставі Закону № 4336-IX від 27.03.2025}

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

{Пункт 4 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

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

{Пункт 5 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

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

{Пункт 6 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

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

{Пункт 7 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

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

{Пункт 8 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

{Пункт 10 частини третьої статті 8 виключено на підставі Закону № 4336-IX від 27.03.2025}

11) створення та забезпечення функціонування Національної електронної комунікаційної мережі;

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

{Пункт 12 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

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 за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

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

{Пункт 15 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

16) встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

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

правових актів у сфері кібербезпеки, а також для вирішення інших завдань у сфері кібербезпеки, що можуть бути вирішені шляхом державно-приватної взаємодії;

{Пункт 17 частини третьої статті 8 в редакції Закону № 4336-IX від 27.03.2025}

18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кримінальних правопорушень 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 Інтернет у воєнних цілях;

{Пункт 21 частини третьої статті 8 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020}

22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

23) обмеження участі у заходах із забезпечення інформаційної безпеки 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 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;

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;

25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки;

{Частина третя статті 8 із змінами, внесеними згідно із Законом № 4070-IX від 20.11.2024}

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

{Частину третю статті 8 доповнено пунктом 26 згідно із Законом № 4336-IX від 27.03.2025}

27) проведення інструктажів та систематичних тренінгів щодо кібергігієни для членів уряду України, народних депутатів України, працівників патронатних служб, депутатів місцевих рад, державних службовців, військовослужбовців, працівників органів державної влади та державних органів, керівників та працівників державних підприємств, установ та організацій, систематичність та порядок проведення яких встановлюються Кабінетом Міністрів України.

{Частину третю статті 8 доповнено пунктом 27 згідно із Законом № 4336-IX від 27.03.2025}

4. Порядок функціонування Національної електронної комунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної електронної комунікаційної мережі затверджуються Кабінетом Міністрів України.

{Частина четверта статті 8 із змінами, внесеними згідно із Законом № 4070-IX від 20.11.2024}

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

1) системи захищеного доступу державних органів до мережі Інтернет;

2) Національного центру резервування державних інформаційних ресурсів;

3) Центру антивірусного захисту інформації;

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

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

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

{Частина п'ята статті 8 в редакції Закону № 4336-IX від 27.03.2025}

6. Органи державної влади, військові формування, утворені відповідно до законів України, державні підприємства, установи та організації з метою усунення можливих наслідків кіберінцидентів та кібератак створюють резервні копії національних електронних інформаційних ресурсів, що перебувають у їх володінні або розпорядженні та є критичними для їх сталого функціонування, та передають їх на зберігання до Національного центру резервування державних інформаційних ресурсів, крім тих, передача яких обмежена законодавством. Порядок передачі, збереження і доступу до зазначених копій визначається Кабінетом Міністрів України.

Національний центр резервування державних інформаційних ресурсів забезпечує:

1) безперервність роботи відповідного національного електронного інформаційного ресурсу, резервного копіювання інформації та відомостей національного електронного інформаційного ресурсу через єдині основний та резервний захищені центри обробки даних (дата-центри), призначені для обробки національних електронних інформаційних ресурсів, резервного копіювання національних електронних інформаційних ресурсів;

2) надійне функціонування серверного обладнання, системи зберігання даних, активного мережевого обладнання, архітектурно-технічних рішень щодо резервного копіювання й дублювання інформаційних систем, постійно працюючої інженерної інфраструктури;

3) здійснення обов'язкового контролю за статистичними даними роботи з фізичного захисту об'єктів, системи управління та моніторингу інформаційних систем, комплексу організаційних заходів;

{Пункт 4 частини шостої статті 8 виключено на підставі Закону № 4336-IX від 27.03.2025}

5) переміщення протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування резервних копій національних електронних інформаційних ресурсів до електронних комунікаційних мереж закордонних дипломатичних установ України в порядку, встановленому Кабінетом Міністрів України.

{Частину шосту статті 8 доповнено пунктом 5 згідно із Законом № 2130-IX від 15.03.2022}

{Статтю 8 доповнено частиною шостою згідно із Законом № 1907-IX від 18.11.2021}

7. Розроблення та застосування платних, безоплатних умов пошуку та/або виявлення потенційних вразливостей в інформаційно-комунікаційних системах, в яких обробляються

державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також на об'єктах критичної інформаційної інфраструктури здійснюються відповідно до порядку пошуку та/або виявлення потенційних вразливостей, встановленого Кабінетом Міністрів України.

Складовою порядку пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також на об'єктах критичної інформаційної інфраструктури мають бути порядок розроблення та проведення програм пошуку і виявлення вразливостей за винагороду та порядок узгодженого розкриття вразливостей.

{Статтю 8 доповнено частиною сьомою згідно із Законом № 4336-IX від 27.03.2025}

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

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

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

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

1) CERT-UA - національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (національний CSIRT), діяльність якої забезпечується Державною службою спеціального зв'язку та захисту інформації України та завданнями якої є:

моніторинг, накопичення та проведення аналізу даних про кіберінциденти, кібератаки, кіберзагрози на національному, галузевому, регіональному рівнях, динамічний аналіз ризиків та ситуаційної обізнаності;

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

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

надання у встановленому порядку сервісу у зв’язку з реагуванням, рекомендацій з реагування на кіберінциденти, кібератаки, кіберзагрози власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторам критичної інфраструктури, власникам або розпорядникам критичної інформаційної інфраструктури, іншим суб’єктам (у разі потреби);

виконання функції координатора з метою узгодженого розкриття вразливостей;

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

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

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

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

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

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

виконання функцій національного контактного центру відповідно до Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2 Directive);

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

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

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

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

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

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

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

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

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

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

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

Державна служба спеціального зв'язку та захисту інформації України має право надавати вимоги про усунення порушень у діяльності галузевого, регіонального CSIRT у разі невідповідності вимогам щодо організаційно-технічної спроможності або порушення

порядку функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози або національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.

Команда реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT-NBU, що входить до складу Центру кіберзахисту Національного банку України, є галузевим CSIRT та діє у складі національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та національної системи реагування на кіберінциденти, кібератаки, кіберзагрози з урахуванням постанов Національного банку України в частині, що не суперечить цьому Закону.

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

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

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

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

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

Державна служба спеціального зв'язку та захисту інформації України та Служба безпеки України з метою вжиття заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози в межах своїх повноважень можуть надавати обов'язкові до виконання вимоги про реагування власникам або розпорядникам інформаційних,

електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури, операторам критичної інфраструктури.

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

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

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

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

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

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

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

{Стаття 9 в редакції Закону № 4336-IX від 27.03.2025}

Стаття 9[1]. Національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози

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

2. Уповноваженим органом, що забезпечує функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, є Державна служба спеціального зв'язку та захисту інформації України (далі - Уповноважений орган).

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

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

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

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

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

Суб'єкти, для яких законом не встановлені зобов'язання щодо надання обов'язкових повідомлень про кіберінциденти, кібератаки, мають право приєднатися до національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та здійснювати

добровільний обмін відповідною інформацією згідно із національною таксономією кіберінцидентів у порядку, визначеному Уповноваженим органом.

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

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

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

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

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

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

{Закон доповнено статтею 9[1] згідно із Законом № 4336-IX від 27.03.2025}

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, IT-компаніями з метою виконання заходів кібероборони в кіберпросторі.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.

Стаття 11. Сприяння суб'єктам забезпечення кібербезпеки України

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.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

{Стаття 12 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020}

Стаття 13. Фінансове забезпечення заходів кібербезпеки

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.

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

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.

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".

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.

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.

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

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.

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 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 Верховною Радою України.

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

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

{Статтю 15 доповнено частиною четвертою згідно із Законом № 4336-IX від 27.03.2025}

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.

2. Внести зміни до таких законів України:

1) статтю 7 Закону України "Про Національний банк України" (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами) 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; утворює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;

33) забезпечує формування та ведення переліку об'єктів критичної інфраструктури, а також реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України, визначає критерії та порядок віднесення об'єктів у банківській системі України до об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України";

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) друге речення частини другої статті 4 доповнити словами "у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі";

{Підпункт 3 пункту 2 розділу втратив чинність на підставі Закону № 912-IX від 17.09.2020}

{Підпункт 4 пункту 2 розділу втратив чинність на підставі Закону № 2469-VIII від 21.06.2018}

5) абзац шостий статті 3 Закону України "Про Службу зовнішньої розвідки України" (Відомості Верховної Ради України, 2006 р., № 8, ст. 94) після слів "національній безпеці України" доповнити словами "у тому числі у кіберпросторі";

6) 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 першустатті 2 та абзац другийчастини першої статті 3 після слів "криптографічного та технічного захисту інформації" доповнити словом "кіберзахисту";

б) у частині першій статті 14:

пункт 39 після слів "забезпечення функціонування" доповнити словом "урядової";

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 Державного центру кіберзахисту".

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

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

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

забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

Президент України **П.ПОРОШЕНКО**

м. Київ
5 жовтня 2017 року
№ 2163-VIII

Публікації документа

- **Голос України** від 09.11.2017 — № 208

- **Відомості Верховної Ради України** від 10.11.2017 — 2017 р., № 45, стор. 42, стаття 403
- **Урядовий кур'єр** від 15.11.2017 — № 215
- **Офіційний вісник України** від 21.11.2017 — 2017 р., № 91, стор. 31, стаття 2765, код акта 87903/2017