Урядовий офіс координації європейської та євроатлантичної інтеграції
Секретаріату Кабінету Міністрів України

Переклад затверджений

Генеральний директор Урядового офісу
координації європейської та
євроатлантичної інтеграції
Секретаріату Кабінету Міністрів України
(найменування посади)

(підпис)

О.В. Стефанішина
(ініціали та прізвище)

15 травня 2018 р.

19.07.2016 UA Офіційний вісник Європейського Союзу L 194/1

ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/1148

від 6 липня 2016 року

про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про функціонування Європейського Союзу, зокрема його статтю 114,

Беручи до уваги пропозицію Європейської Комісії,

Після передачі проекту законодавчого акта національним парламентам,

Беручи до уваги висновок Європейського економічно-соціального комітету (1),

Діючи згідно зі звичайною законодавчою процедурою (2),

Оскільки:

(1) Мережеві та інформаційні системи та послуги відіграють важливу роль у суспільстві. Їхня надійність та безпека суттєва для економічної та соціальної діяльності і, зокрема, для функціонування внутрішнього ринку.

(2) Масштаб, частота та вплив інцидентів, пов'язаних з безпекою, зростають та становлять велику загрозу для функціонування мережевих та інформаційних систем. Такі системи можуть також ставати об'єктом умисних шкідливих дій, мета яких — пошкодити такі системи або завадити їх експлуатації. Такі інциденти можуть перешкоджати здійсненню економічної діяльності, завдавати значних фінансових збитків, підривати довіру користувачів та спричиняти значну шкоду економіці Союзу.

(3) Мережеві та інформаційні системи і, в першу чергу, інтернет, відіграють важливу роль у сприянні транскордонному руху товарів, послуг та людей. Через транснаціональний характер, значні порушення функціонування таких систем, як навмисні, так і ненавмисні, а також незалежно від місця здійснення, можуть впливати на окремі держави- члени та Союз у

ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/1148

від 6 липня 2016 року

про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про функціонування Європейського Союзу, зокрема його статтю 114,

Беручи до уваги пропозицію Європейської Комісії,

Після передачі проекту законодавчого акта національним парламентам,

Беручи до уваги висновок Європейського економічно-соціального комітету [1],

Діючи згідно зі звичайною законодавчою процедурою [2],

Оскільки:

(1) Мережеві та інформаційні системи та послуги відіграють важливу роль у суспільстві. Їхня надійність та безпека суттєва для економічної та соціальної діяльності і, зокрема, для функціонування внутрішнього ринку.

(2) Масштаб, частота та вплив інцидентів, пов'язаних з безпекою, зростають та становлять велику загрозу для функціонування мережевих та інформаційних систем. Такі системи можуть також ставати об'єктом умисних шкідливих дій, мета яких — пошкодити такі системи або завадити їх експлуатації. Такі інциденти можуть перешкоджати здійсненню економічної діяльності, завдавати значних фінансових збитків, підривати довіру користувачів та спричиняти значну шкоду економіці Союзу.

(3) Мережеві та інформаційні системи і, в першу чергу, інтернет, відіграють важливу роль у сприянні транскордонному руху товарів, послуг та людей. Через транснаціональний характер, значні порушення функціонування таких систем, як навмисні, так і ненавмисні, а також незалежно від місця здійснення, можуть впливати на окремі держави- члени та Союз у цілому. Таким чином, безпека мережевих та інформаційних систем суттєва для безперебійного функціонування внутрішнього ринку.

(4) Спираючись на значний прогрес у рамках Європейського форуму держав- членів у сприянні обговоренням та обмінам належними практиками в політиці, у тому числі розробки принципів для європейського співробітництва з питань кібер-кризи, необхідно створити Групу співпраці, що складатиметься з представників держав- членів, Комісії та Європейського агентства з питань мережевої та інформаційної безпеки («ENISA»), для підтримки та сприяння стратегічній співпраці між державами- членами щодо безпеки мережевих та інформаційних систем. Для того, щоб така група була дієвою та інклюзивною, суттєво, щоб всі держави-члени мали мінімальні можливості та стратегію, що забезпечує високий рівень безпеки мережевих та інформаційних систем на їхній території. Крім того, необхідно застосовувати вимоги до безпеки та повідомлення до операторів основних послуг та надавачів цифрових послуг щоби просувати культуру управління ризиками та забезпечити звітування про найсерйозніші інциденти.

(5) Існуючих можливостей недостатньо для забезпечення високого рівня безпеки мережевих та інформаційних систем в межах Союзу. Держави-члени мають дуже різні рівні підготованості, що призвело до фрагментованості підходів у Союзі. Це спричиняє неоднаковий рівень захисту споживачів та суб'єктів господарської діяльності і підриває загальний рівень безпеки мережевих та інформаційних систем в межах Союзу. В свою чергу, брак спільних вимог до операторів основних послуг та надавачів цифрових послуг унеможливлює заснування глобального та дієвого механізму співпраці на рівні Союзу. Університети та дослідницькі центри відіграють вирішальну роль у стимулюванні досліджень, розвитку та інновацій у таких сферах.

(6) Таким чином, результативна відповідь на виклики в сфері безпеки мережевих та інформаційних систем вимагає глобального підходу на рівні Союзу, що охоплюватиме спільні мінімальні вимоги до розбудови спроможності і планування, обмін інформацією, вимоги співпраці та спільні безпекові вимоги до операторів основних послуг та надавачів цифрових послуг. Однак, ніщо не перешкоджає операторам основних послуг та надавачам цифрових послуг впроваджувати інструменти безпеки, суворіші за інструменти, передбачені в цій Директиві.

(7) Для того, щоб охопити всі відповідні інциденти та ризики, цю Директиву необхідно застосовувати як до операторів основних послуг, так і до надавачів цифрових послуг. Однак, зобов'язання, що покладаються на операторів основних послуг та надавачів цифрових послуг, не можна застосовувати до підприємств, що надають мережі зв'язку загального користування або загальнодоступні послуги електронного зв'язку у розумінні Директиви Європейського Парламенту і Ради 2002/21/ЄС (3), до яких застосовують спеціальні вимоги безпеки та цілісності, встановлені у зазначеній Директиві, а також їх не можна застосовувати до надавачів довірчих послуг у значенні Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 (4), до яких застосовують вимоги безпеки, встановлені в зазначеному Регламенті.

(8) Ця Директива не повинна обмежувати можливість кожної держави- члена вживати необхідних заходів для забезпечення захисту суттєвих інтересів її безпеки, для охорони публічного порядку та забезпечення громадської безпеки, а також щоби уможливити розслідування, розкриття та кримінальне переслідування кримінальних правопорушень. Відповідно до статті 346 Договору про функціонування Європейського Союзу (TFEU), жодна держава- член не може бути зобов'язана надавати інформацію, розкриття якої, на її думку, суперечитиме суттєвим інтересам її безпеки. У цьому контексті мають значення Рішення Ради 2013/488/ЄС (5) та угоди про нерозкриття або неформальні угоди про нерозкриття інформації, такі як протокол «Світлофор» (TLP).

(9) Певні сектори економіки вже регулюють або можуть регулювати у майбутньому галузеві правові акти Союзу, що включають правила, які стосуються безпеки мережевих та інформаційних систем. Коли такі правові акти Єсоюзу містять положення, що накладають вимоги відносно безпеки мережевих та інформаційних систем або повідомлень про інциденти, такі положення необхідно застосовувати, якщо вони містять вимоги, які щонайменше рівноцінні по суті зобов'язанням, що містяться в цій Директиві. В такому разі, держави- члени повинні застосовувати положення таких секторальних правових актів Союзу, у тому числі положення відносно юрисдикції, а також не повинні визначати операторів основних послуг, згідно з порядком, встановленим в цій Директиві. У цьому контексті, держави- члени повинні надавати Комісії інформацію про застосування таких положень *lex specialis*. Вирішуючи питання, чи вимоги до безпеки мережевих та інформаційних систем та до повідомлення про інциденти, що містяться у секторальних правових актах Союзу, рівноцінні вимогам, що містяться в цій Директиві, необхідно враховувати лише положення відповідних правових актів Союзу та їх застосування у державах- членах.

(10) У секторі водного транспорту безпекові вимоги до компаній, кораблів, портових споруд, портів та служб руху суден відповідно до правових актів Союзу охоплюють всі операції, у тому числі системи радіо- та електрозв'язку, комп'ютерні системи та мережі. Частина обов'язкових процедур, яких необхідно дотримуватися, включає звітування про всі інциденти і, таким чином, повинна вважатися *lex specialis*, настільки наскільки такі вимоги щонайменше рівноцінні відповідним положенням цієї Директиви.

(11) Визначаючи операторів у секторі водного транспорту, держави- члени повинні враховувати існуючі та майбутні міжнародні кодекси та настанови, розроблені, зокрема, Міжнародною морською організацією, з метою забезпечення узгодженого підходу для окремих морських операторів.

(12) Регулювання та нагляд у банківському секторі та секторі інфраструктур фінансового ринку високою мірою гармонізовані на рівні Союзу за допомогою первинного та вторинного законодавства Союзу та стандартів, розроблених разом з європейськими наглядовими органами. В рамках банківського союзу застосування таких вимог та нагляд за їх виконанням забезпечує єдиний наглядовий механізм. Для держав- членів, які не належать до

банківського союзу — це забезпечують відповідні банківські регуляторні органи держав- членів. В інших сферах регулювання фінансового сектору, Європейська система фінансового нагляду також забезпечує високий ступінь спільності та конвергенції наглядових практик. Європейський орган з цінних паперів та ринків (ESMA) також відіграє роль прямого нагляду за певними суб'єктами, а саме кредитно-рейтинговими агентствами та реєстрами трансакцій.

(13) Операційний ризик є важливою частиною пруденційного регулювання та нагляду у банківському секторі та секторі інфраструктур фінансового ринку. Він охоплює всі операції, у тому числі безпеку, цілісність та стійкість мережевих та інформаційних систем. Вимоги відносно таких систем, які часто перевищують вимоги, передбачені в цій Директиві, викладені у низці правових актів Союзу, у тому числі: правилах щодо доступу до діяльності кредитних установ та пруденційного нагляду за кредитними установами та інвестиційними компаніями, та правилах щодо пруденційних вимог до кредитних установ та інвестиційних компаній, котрі включають вимоги відносно операційного ризику; правилах щодо ринків фінансових інструментів, котрі включають вимоги стосовно оцінювання ризику для інвестиційних компаній та регульованих ринків; правилах щодо позабіржових похідних фінансових інструментів, центральних контрагентів та реєстрів трансакцій, що включають вимоги відносно операційного ризику для центральних контрагентів та реєстрів трансакцій; правилах щодо вдосконалення розрахунків за цінними паперами у Союзі та щодо центральних депозитаріїв цінних паперів, котрі включають вимоги відносно операційного ризику. Крім того, вимоги до повідомлення про інциденти входять до звичайної наглядової практики у фінансовому секторі та часто містяться у посібниках з нагляду. Держави- члени повинні брати до уваги такі правила та вимоги у їхньому застосуванні *lex specialis*.

(14) Як відмітив Європейський Центральний Банк у своєму рішенні від 25 липня 2014 року [(6)], ця Директива не впливає на режим нагляду за платіжними системами та системами розрахунків Євросистеми відповідно до законодавства Союзу. Було би доцільно для органів, відповідальних за такий нагляд, обмінюватися досвідом щодо питань стосовно безпеки мережевих та інформаційних систем, з компетентними органами відповідно до цієї Директиви. Така ж увага приділяється членам Європейської системи центральних банків з країн, що не входять до зони євро, що здійснюють такий нагляд за платіжними та розрахунковими системами на основі національних нормативно-правових актів.

(15) Електронний торговий майданчик дозволяє споживачам та торговцям укладати онлайн договори продажу або надання послуг з торговцями і є кінцевим пунктом для укладання таких договорів. Він не повинен включати онлайнові послуги, що слугують лише посередником для послуг третіх сторін, за допомогою яких можна врешті укласти договір. Таким чином, він не повинен включати онлайнові послуги, що порівнюють ціну різних торговців на певні продукти або послуги, а потім перенаправляють користувача до торговця, якому надається перевага, для купівлі продукту. Обчислювальні послуги, які надають електронні торгові майданчики, можуть включати опрацювання трансакцій, агрегацію даних або створення облікових записів користувачів. Сховища програм, які функціонують як інтернет-магазини, що уможливлюють цифрове розповсюдження програм або програмного забезпечення третіх сторін, необхідно розуміти як один з типів електронних торгових майданчиків.

(16) Електронна пошукова система дозволяє користувачеві здійснювати пошук, в принципі, по всім веб-сайтам за запитом на будь-яку тему. Також пошук може бути орієнтований на веб-сайти певною мовою. Означення пошукової системи, передбачене в цій Директиві, не повинне охоплювати пошукові функції, обмежені контентом конкретного веб-сайту, незалежно від того, чи таку пошукову функцію надає зовнішня електронна пошукова система. Також воно не повинне охоплювати інтернет-послуги, що порівнюють ціну різних торговців на певні продукти або послуги, а потім перенаправляють користувача до торговця, якому надається перевага, для купівлі продукту.

(17) Послуги хмарних обчислень включають широке розмаїття видів діяльності, що можуть надаватись відповідно до різних моделей. Для цілей цієї Директиви, термін «послуги хмарних обчислень» охоплює послуги, що дозволяють доступ до масштабовного та еластичного пулу обчислювальних ресурсів спільного користування. Такі обчислювальні

ресурси включають такі ресурси як мережі, сервери або іншу інфраструктуру, сховища, програми та послуги. Термін «масштабовний» означає, що надавач хмарної послуги гнучко розподілив обчислювальні ресурси незалежно від географічного розташування ресурсів для того, щоб справлятися з коливаннями попиту. Термін «еластичний пул» використовується для опису таких обчислювальних ресурсів, які вводять в дію та дозволяють до використання відповідно до попиту щоби швидко збільшувати та зменшувати доступні ресурси залежно від навантаження. Термін «спільного користування» використовується для опису обчислювальних ресурсів, котрі надаються багатьом користувачам зі спільним доступом до послуги, але опрацювання здійснюється для кожного користувача окремо, хоча послуга надається з одного й того ж електронного обладнання.

(18)Функція точки обміну інтернет-трафіком (IXP) полягає у взаємоз'єднанні мереж. IXP не надає доступу до мережі та не діє як транзитний провайдер або передавач. Також IXP не надає інших послуг, не пов'язаних із взаємоз'єднанням, хоча це не стає на заваді IXP-операторові надавати непов'язані послуги. IXP існує для взаємоз'єднання технічно та організаційно відокремлених мереж. Термін «автономна система» використовується для опису технічно автономної мережі.

(19)Держави- члени повинні нести відповідальність за визначення суб'єктів, які відповідають критеріям означення оператора основних послуг. Для того, щоб забезпечити узгоджений підхід, всі держави- члени повинні послідовно застосовувати означення оператора основних послуг. З цією метою, ця Директива передбачає оцінювання суб'єктів, що діють у конкретних секторах та підсекторах, створення списку основних послуг, розгляд спільного списку міжгалузевих факторів щоби визначити, чи може потенційний інцидент мати значний негативний вплив, процес консультацій із залученням відповідних держав- членів у випадку суб'єктів, що надають послуги у декількох державах- членах, та підтримку Групи співпраці у процесі визначення. Для забезпечення точного відображення можливих змін на ринку, держави- члени повинні регулярно переглядати список визначених операторів та оновлювати його мірою необхідності. Врешті, держави- члени повинні надати Комісії інформацію, необхідну для оцінення межі узгодженого застосування державами- членами такого означення, яку дозволила ця спільна методологія.

(20)У процесі визначення операторів основних послуг, держави- члени повинні оцінити, щонайменше для кожного підсектора, вказаного в цій Директиві, які послуги необхідно вважати основними для підтримки критичної соціально-економічної діяльності, а також чи суб'єкти, перелічені в секторах та підсекторах, вказаних у цій Директиві, що надають такі послуги, відповідають критеріям визначення операторів. Здійснюючи оцінювання питання, чи надає суб'єкт послугу, що є основною для підтримки критичної соціально-економічної діяльності, достатньо перевірити чи такий суб'єкт надає послугу, що включена до списку основних послуг. Крім того, необхідно довести, що надання такої основної послуги залежить від мережевих та інформаційних систем. Врешті, здійснюючи оцінювання питання, чи може інцидент мати значний негативний вплив на надання послуги, держави- члени повинні враховувати певні міжсекторальні чинники, а також, якщо доречно, секторальні чинники.

(21)Для цілей визначення операторів основних послуг, створення у державі- члені вимагає дієвого та реального здійснення діяльності на основі стабільного впорядкування. Адміністративно-правова форма такого впорядкування, чи то відділення чи то дочірнє підприємство що володіє правосуб'єктністю, не є визначальним чинником у цьому відношенні.

(22)Можливо, що такі суб'єкти, що діють у секторах та підсекторах, вказаних у цій Директив, надають як основні, так і неосновні послуги. Наприклад, у секторі повітряного транспорту аеропорти надають послуги, які держава- член може вважати основними, наприклад управління злітно-приземлювальною смугою, але також певні послуги, які можуть вважатися неосновними, наприклад забезпечення торгових зон. Оператори основних послуг повинні виконувати конкретні безпекові вимоги лише стосовно таких послуг, які вважаються основними. З метою визначення операторів держави- члени повинні створити список послуг, які вважаються основними.

(23)Список послуг повинен містити всі послуги, що надаються на території певної держави- члена та відповідають вимогам згідно з цією Директивою. Держави- члени повинні

мати змогу доповнювати існуючий список, додаючи нові послуги. Список послуг повинен слугувати орієнтиром для держав- членів, дозволяючи визначення операторів основних послуг. Його метою є визначення типів основних послуг у будь-якому певному секторі, вказаному у цій Директиві, таким чином відрізняючи їх від неосновної діяльності, за яку суб'єкт, який здійснює діяльність у відповідному секторі, може бути відповідальним. Список послуг, складений кожною державою- членом, слугуватиме додатковим внеском в оцінювання регуляторної практики кожної держави- члена з метою забезпечення загального рівня узгодженості процесу визначення серед держав- членів.

(24)Для цілей процесу визначення, якщо суб'єкт надає основну послугу у двох або більше державах- членах, такі держави- члени повинні долучатися до двосторонніх або багатосторонніх обговорень одна з одною. Такий консультаційний процес має на меті допомогти їм оцінити критичність оператора стосовно транскордонного впливу, дозволяючи кожній залученій державі- члену представити свої погляди стосовно ризиків, пов'язаних з послугами, що надаються. Відповідні держави- члени повинні враховувати погляди одна одної в цьому процесі та повинні мати змогу звертатися по допомогу до Групи співпраці з цього приводу.

(25)Як результат процесу визначення, держави-члени повинні ухвалювати національні інструменти щоби встановити, до яких суб'єктів застосовуються зобов'язання щодо безпеки мережевих та інформаційних систем. Цього результату можна досягти за допомогою ухвалення списку, що містить перелік всіх операторів основних послуг, або за допомогою ухвалення національних інструментів, що включають об'єктивні кількісно вимірювані критерії такі, як результативність оператора або кількість користувачів, що дає можливість встановити, до яких суб'єктів застосовуються зобов'язання щодо безпеки мережевих та інформаційних систем. Національні інструменти, які вже існують або ухвалені у контексті цієї Директиви, повинні включати всі правові інструменти, адміністративні інструменти та політики, що дозволяють визначення операторів основних послуг згідно з цією Директивою.

(26)Для того, щоб охарактеризувати важливість — відносно відповідного сектора — визначених операторів основних послуг, держави- члени повинні враховувати кількість та розмір таких операторів, наприклад, щодо частки ринку або обсягу виробництва або перевезення, без зобов'язання розголошувати інформацію, що може виявити, яких операторів було визначено.

(27)Для того, щоб визначити чи може інцидент мати значний негативний вплив на надання основної послуги, держави- члени повинні враховувати декілька різних чинників, таких як кількість користувачів, які залежать від такої послуги для особистих або професійних цілей. Використання такої послуги може бути пряме, непряме або за посередництва. Оцінюючи вплив, який може мати такий інцидент, відповідно до його ступеню та тривалості, на економічну та соціальну діяльність або громадську безпеку, держави- члени повинні також оцінювати час, що імовірно пройде до того, як таке порушення безперервності почне мати негативний вплив.

(28)Окрім міжсекторальних чинників, необхідно враховувати також і специфічні для сектора чинники для того, щоб визначити, чи матиме інцидент значний негативний вплив на надання основної послуги. Що стосується постачальників енергії, то такі чинники можуть включати обсяг або частку виробленої енергії на національному рівні; для постачальників нафти — добовий обсяг; для повітряного транспорту, у тому числі аеропортів та авіаперевізників, залізничного транспорту та морських портів — частку обсягу національного руху та річна кількість пасажирів або вантажних операцій; для інфраструктур банківського та фінансових ринків — їхню системну важливість, що базується на загальному обсягу активів або співвідношенні такого загального обсягу активів до ВВП; для сектора охорони здоров'я — річна кількість пацієнтів під наглядом надавача (медичних послуг); для виробництва, підготування та постачання води — обсяг, кількість та типи користувачів, яким було здійснене постачання, у тому числі, наприклад, лікарні, комунальні служби або фізичні особи, та існування альтернативних джерел води для охоплення тієї самої географічної місцевості.

(29)Для того, щоб досягти та підтримувати високий рівень безпеки мережевих та інформаційних систем, кожна держава- член повинна мати національну стратегію щодо безпеки мережевих

та інформаційних систем, що визначає стратегічні цілі та конкретні дії в сфері політики, які необхідно здійснити.

(30)З огляду на відмінності в структурах національного врядування та для охорони вже існуючого секторального впорядкування або наглядових та регуляторних органів Союзу, а також щоб уникнути дублювання, держави- члени повинні мати змогу призначити більш ніж один національний компетентний орган, відповідальний за виконання завдань, пов'язаних із безпекою мережевих та інформаційних систем операторів основних послуг та надавачів цифрових послуг відповідно до цієї Директиви.

(31)Для сприяння транскордонної співпраці та комунікації, та для того, щоб уможливити результативну імплементацію цієї Директиви, необхідно для кожної держави- члена, не обмежуючи секторального регуляторного впорядкування, призначити єдиний національний контактний пункт, відповідальний за координацію питань, пов'язаних із безпекою мережевих та інформаційних систем та транскордонною співпрацею на рівні Союзу. Компетентні органи та єдині контактні пункти повинні мати належні технічні, фінансові та людські ресурси для забезпечення їх здатності виконувати завдання, поставлені перед ними, у результативний та ефективний спосіб і таким чином досягати цілей цієї Директиви. Оскільки ця Директива має на меті покращити функціонування внутрішнього ринку через створення повної довіри, органи держав- членів повинні мати змогу результативно співпрацювати з суб'єктами економічної діяльності та бути відповідним чином структурованими.

(32)Компетентні органи або групи реагування на інциденти, пов'язані з комп'ютерною безпекою («CSIRT»), повинні отримувати повідомлення про інциденти. Єдині контактні пункти не повинні прямо отримувати повідомлення про інциденти, крім випадків, коли вони також діють як компетентний орган або CSIRT. Однак, компетентний орган або CSIRT повинна мати можливість доручати єдиному контактному пункту надсилати повідомлення про інциденти єдиним контактним пунктам інших держав- членів, які піддаються негативній дії.

(33)Щоби забезпечити результативне надання інформації державам- членам та Комісії, єдиний контактний пункт повинен подати підсумковий звіт Групі співпраці; цей звіт повинен бути анонімним для того, щоб зберегти конфіденційність повідомлень та особи операторів основних послуг та надавачів цифрових послуг, оскільки інформація про особу суб'єктів, що повідомляють, не вимагається для обміну кращими практиками у Групі співпраці. Підсумковий звіт повинен містити інформацію про кількість отриманих повідомлень, а також зазначення характеру інцидентів, про які було надіслано повідомлення, такого як типи випадків порушення безпеки, їхня серйозність або їхня тривалість.

(34)Держави- члени повинні бути належним чином оснащені, з огляду на технічні та організаційні спроможності, для запобігання, виявлення, реагування на інциденти та ризики мережевих та інформаційних систем та усунення їхніх наслідків. Отже, держави- члени повинні забезпечувати наявність у себе надійно функціонуючі CSIRT, також відомі як групи реагування на комп'ютерні надзвичайні ситуації («CERT»), що відповідають основним вимогам гарантування результативних та сумісних спроможностей для подолання наслідків таких інцидентів та ризиків і забезпечення ефективної співпраці на рівні Союзу. Для того, щоби всі типи операторів основних послуг та надавачів цифрових послуг користувалися перевагами таких спроможностей та співпраці, держави- члени повинні забезпечувати, щоби призначена CSIRT була передбачена для всіх типів. Враховуючи важливість міжнародної співпраці з питань кібербезпеки, CSIRT повинні мати можливість брати участь у мережах міжнародної співпраці окрім мережі CSIRT, заснованої цією Директивою.

(35)Оскільки більшість мережевих та інформаційних систем експлуатують на приватній основі, співпраця між публічним та приватним секторами є суттєвим моментом. Операторів основних послуг та надавачів цифрових послуг необхідно заохочувати до розроблення своїх власних механізмів міжнародної співпраці для забезпечення безпеки мережевих та інформаційних систем. Група співробітництва повинна, за доречності, мати змогу запрошувати відповідних стейкхолдерів до обговорень. З метою забезпечення дієвого обміну інформацією та кращими практиками, необхідно забезпечувати відсутність дій на шкоду операторам основних послуг та надавачам цифрових послуг, які беруть участь у такому обміні,.

(36)ENISA повинне допомагати державам- членам та Комісії, надаючи експертні знання та консультації, а також сприяючи обміну кращими практиками. Зокрема, у застосування цієї Директиви Комісія повинна — а держави- члени повинні мати змогу — консультуватися з ENISA. Для нарощування потенціалу та знань держав- членів, Група співпраці повинна також слугувати інструментом обміну кращими практиками, обговорення спроможностей та підготованості держав- членів, а також добровільно допомагати її членам в оцінюванні національних стратегій з безпеки мережевих та інформаційних систем, нарощування потенціалу та оцінювання завдань, що стосуються безпеки мережевих та інформаційних систем.

(37)За доцільності, держави- члени повинні мати змогу використовувати або адаптовувати існуючі організаційні структури або стратегії, у застосуванні цієї Директиви.

(38)Відповідні завдання Групи співпраці та ENISA є взаємозалежними та доповняльними. В цілому, ENISA повинне допомагати Групі співпраці у виконанні її завдань відповідно до цілі ENISA, встановленої в Регламенті Європейського Парламенту і Ради (ЕС) № 526/2013 [7], а саме допомагати установам, органам, офісам та агентствам Союзу та державам- членам в реалізації політик, необхідних для дотримання правових та нормативних вимог безпеки мережевих та інформаційних систем відповідно до існуючих та майбутніх законодавчих актів Союзу. Зокрема, ENISA повинне надавати допомогу в таких сферах, які відповідають її власним завданням, як викладено в Регламенті (ЄС) № 526/2013, а саме: в аналізі стратегій безпеки мережевих та інформаційних систем, підтримці організації та здійснення завдань Союзу стосовно безпеки мережевих та інформаційних систем, обміні інформацією та кращими практиками щодо підвищення обізнаності й навчання. ENISA також необхідно залучати до розроблення настанов для секторальних критеріїв визначення вагомості впливу інциденту.

(39)Для того, щоб просувати додаткову безпеку мережевих та інформаційних систем, Група співпраці повинна, у відповідних випадках, співпрацювати з відповідними установами, органами, офісами та агентствами Союзу для обміну ноу-хау та кращими практиками, а також для консультування щодо аспектів безпеки мережевих та інформаційних систем, що можуть мати вплив на їхню роботу, дотримуючись при цьому існуючого порядку та умов обміну інформацією з обмеженим доступом. Співпрацюючи з правоохоронними органами стосовно аспектів безпеки мережевих та інформаційних систем, що можуть впливати на їхню роботу, Група співпраці повинна враховувати наявні канали інформації та створені мережі.

(40)Інформація про інциденти дедалі стає важливішою для громадськості та суб’єктів господарської діяльності, особливо для малих та середніх підприємств. У деяких випадках, така інформація вже надається за допомогою веб-сайтів на національному рівні мовою конкретної країни, вона орієнтована головним чином на інциденти та події національного масштабу. З огляду на те, що суб’єкти господарської діяльності дедалі більше діяльності працюють через кордони і громадяни використовують онлайн послуги, інформацію про інциденти необхідно надавати комплексно на рівні Союзу. Секретаріат мережі CSIRT заохочують підтримувати веб-сайт або розміщати виділену сторінку на існуючому веб-сайті, де оприлюднюють загальну інформацію про значні інциденти, які трапилися на території Союзу, з особливою увагою до інтересів та потреб суб’єктів господарської діяльності. CSIRT, які беруть участь у мережі CSIRT, заохочують добровільно надавати інформацію, що буде опублікована на такому веб-сайті, за винятком конфіденційної або чутливої інформації.

(41)Якщо інформація вважається конфіденційною відповідно до правил Союзу або національних правил щодо комерційної таємниці, необхідно забезпечувати таку таємницю, здійснюючи діяльність та досягаючи цілі, встановлені цією Директивою.

(42)Навчання із симуляцією сценаріїв інцидентів в реальному часі важливі для випробовування підготованості та співпраці держав- членів щодо безпеки мережевих та інформаційних систем. Цикл навчань «CyberEurope», який координує ENISA за участі держав- членів — корисний інструмент для випробування та розробки рекомендацій стосовно того, як повинне врегулювання інцидентів на рівні Союзу покращитися з часом. Враховуючи те, що держави- члени наразі не зобов’язані планувати навчання або брати участь у них, створення мережі CSIRT відповідно до цієї Директиви повинне уможливити держави- члени брати

участь у навчаннях на основі точного планування та стратегічних рішень. Група співпраці, створена згідно з цією Директивою, повинна обговорювати стратегічні рішення щодо навчань, зокрема, але не виключно, стосовно регулярності навчань та розробки сценаріїв. ENISA повинне, відповідно до свого мандату, підтримувати організацію та виконання навчань у масштабах всього Союзу, надаючи свої експертні знання та консультації Групі співпраці та мережі CSIRT.

(43) Враховуючи глобальний характер проблем безпеки, що впливають на мережеві та інформаційні системи, існує потреба в тіснішій міжнародній співпраці для покращення стандартів безпеки та інформаційного обміну та для сприяння спільному глобальному підходу до питань безпеки.

(44) Відповідальність за забезпечення безпеки мережевих та інформаційних систем лежить, значною мірою, на операторах основних послуг та надавачах цифрових послуг. Необхідно сприяти культурі управління ризиками, у тому числі оцінюванню ризику та реалізації інструментів безпеки, відповідних ризикам, що постають наразі, та розвивати її за допомогою належних регуляторних вимог та добровільних галузевих практик. Створення надійних однакових умов конкуренції також важливо для результативного функціонування Групи співпраці та мережі CSIRT для забезпечення результативної співпраці всіх держав- членів.

(45) Цю Директиву застосовують лише до публічних адміністрацій, визначених операторами основних послуг. Таким чином, держави- члени несуть відповідальність за забезпечення безпеки мережевих та інформаційних систем публічних адміністрацій, які не підпадають під сферу застосування цієї Директиви.

(46) Інструменти управління ризиками включають інструменти для визначення ризиків інцидентів, для запобігання, виявлення та врегулювання інцидентів, а також зменшення їхнього впливу. Безпека мережевих та інформаційних систем включає безпеку збережених, переданих та опрацьованих даних.

(47) Компетентні органи повинні зберігати можливість ухвалювати національні настанови щодо обставин, за яких оператори основних послуг повинні повідомляти про інциденти.

(48) Багато суб’єктів господарської діяльності в Союзі залежать від надавачів цифрових послуг у наданні своїх послуг. Оскільки деякі цифрові послуги можуть бути важливим ресурсом для користувачів, у тому числі операторів основних послуг, і такі користувачі не завжди можуть мати доступні альтернативи, цю Директиву також необхідно застосовувати до надавачів таких послуг. Безпека, неперервність та надійність типу цифрових послуг, зазначеного в цій Директиві — основа безперебійного функціонування багатьох суб’єктів господарської діяльності. Перебої такої цифрової послуги можуть перешкоджати наданню інших послуг, які залежать від неї і, таким чином, впливати на ключову економічну та соціальну діяльність у Союзі. Такі цифрові послуги можуть мати вирішальне значення для безперебійного функціонування суб’єктів господарської діяльності, що залежать від них і, більше того, для участі таких суб’єктів у внутрішньому ринку та транскордонній торгівлі в межах Союзу. Зазначені надавачі цифрових послуг, на яких розповсюджується дія цієї Директиви, вважаються такими, що пропонують цифрові послуги, від яких дедалі більше залежить багато суб’єктів господарської діяльності в Союзі.

(49) Надавачі цифрових послуг повинні забезпечити рівень безпеки, співмірний з рівнем ризику, що виникає для безпеки цифрових послуг, які вони надають, враховуючи важливість інших послуг для операцій інших суб’єктів господарської діяльності в межах Союзі. На практиці, ступінь ризику для операторів основних послуг, які часто є істотними для підтримки важливої соціальної та економічної діяльності, є вищим ніж для надавачів цифрових послуг. Таким чином, вимоги до безпеки для надавачів цифрових послуг повинні бути менш суворими. Надавачі цифрових послуг повинні мати свободу вживати заходів, які вони вважають належними для управління ризиками, що виникають для безпеки їхніх мережевих та інформаційних систем. Через свій транскордонний характер, надавачі цифрових послуг повинні підлягати більш гармонізованому підходу на рівні Союзу. Імплементаційні акти повинні сприяти конкретизації та реалізації таких заходів.

(50) Хоча виробники апаратного забезпечення та розробники програмного забезпечення не є

операторами основних послуг і надавачами цифрових послуг, їхні продукти посилюють безпеку мережевих та інформаційних систем. Таким чином, вони відіграють важливу роль у забезпеченні можливості операторів основних послуг та надавачів цифрових послуг убезпечити їхні мережеві та інформаційні системи. На такі продукти апаратного та програмного забезпечення вже розповсюджуються існуючі правила щодо відповідальності за продукт.

(51) Технічні та організаційні інструменти, введені щодо операторів основних послуг та надавачів цифрових послуг, не повинні вимагати певної комерційної інформації та певного способу проектування, розроблення або виготовлення продукту технологій зв'язку.

(52) Оператори основних послуг та надавачі цифрових послуг повинні забезпечувати безпеку мережевих та інформаційних систем, які вони використовують. Це, в першу чергу, приватні мережеві та інформаційні системи, якими управляє їхній внутрішній ІТ-персонал або безпеку яких забезпечують сторонні організації. Вимоги до безпеки та повідомлення необхідно застосовувати до відповідних операторів основних послуг та надавачів цифрових послуг незалежно від того, чи здійснюють вони технічне обслуговування своїх мережевих та інформаційних систем самостійно чи доручають це стороннім організаціям.

(53) Для того, щоб уникнути покладання непропорційного фінансового та адміністративного тягаря на операторів основних послуг та надавачів цифрових послуг, вимоги повинні бути пропорційними ризику, зв'язаному з відповідною мережевою та інформаційною системою, враховуючи сучасний стан таких інструментів. У випадку надавачів цифрових послуг, такі вимоги не повинні застосовуватися до мікро- та малих підприємств.

(54) Якщо публічні адміністрації у державах- членах використовують послуги, запропоновані надавачами цифрових послуг, зокрема послугами хмарних обчислень, вони можуть захотіти вимагати від надавачів таких послуг додаткових заходів безпеки окрім тих, які надавачі цифрових послуг зазвичай запропонували би згідно з вимогами цієї Директиви. Вони повинні мати змогу робити це за допомогою договірних зобов'язань.

(55) Означення електронних торгових майданчиків, пошукових систем та послуг хмарних обчислень у цій Директиві слугують конкретній меті цієї Директиви і не обмежують будь-яких інших інструментів.

(56) Ця Директива не повинна перешкоджати державам- членам ухвалювати національні інструменти, що вимагають від державних організацій забезпечувати конкретні вимоги до безпеки коли вони укладають договори на послуги хмарних обчислень. Будь-які такі національні інструменти необхідно застосовувати до відповідної державної організації, а не до надавача послуги хмарних обчислень.

(57) Враховуючи фундаментальні відмінності між операторами основних послуг, зокрема їхній прямий зв'язок з фізичною інфраструктурою, та надавачами цифрових послуг, зокрема їхній транскордонний характер, ця Директива повинна застосовувати диференційований підхід відносно рівня гармонізації щодо цих двох груп суб'єктів. Стосовно операторів основних послуг, держави- члени повинні мати змогу визначати відповідних операторів та висувати суворіші вимоги ніж ті, що встановлено в цій Директиві. Держави- члени не повинні визначати надавачів цифрових послуг, оскільки цю Директиву в її сфері застосування необхідно застосовувати до всіх надавачів цифрових послуг. Крім цього, ця Директива та імплементаційні акти, ухвалені відповідно до неї, повинні забезпечувати високий рівень гармонізації для надавачів цифрових послуг відносно вимог до безпеки та повідомлення. Це повинне уможливити однакове ставлення до надавачів цифрових послуг у всьому Союзу у спосіб, пропорційний їхньому характеру та ступеню ризику, який може постати перед ними.

(58) Ця Директива не повинна перешкоджати державам- членам висувати вимоги до безпеки та повідомлення до суб'єктів, які не є надавачами цифрових послуг в рамках цієї Директиви, без обмеження зобов'язань держав- членів згідно із законодавством Союзу.

(59) Компетентні органи повинні звертати належну увагу на збереження неформальних та надійних каналів обміну інформацією. Розголошуючи інциденти, про які було повідомлено компетентним органам, необхідно належним чином забезпечувати баланс між інтересом громадськості в отриманні інформації про загрози та можливою шкодою репутації чи бізнесу операторів основних послуг та надавачів цифрових послуг, що повідомляють про

інциденти. Виконуючи зобов'язання щодо повідомлення, компетентні органи та CSIRT повинні звертати особливу увагу на необхідність зберігати сувору конфіденційність інформації про вразливості продукту поки не будуть видані відповідні виправлення безпеки.

(60) Надавачі цифрових послуг повинні бути об'єктом спрощеної та реакційної наглядової діяльності *ex post*, обґрунтованої характером їхніх послуг та операцій. Таким чином, відповідний компетентний орган повинен вживати заходів лише коли він має докази того, що надавач цифрових послуг не відповідає вимогам цієї Директиви, зокрема, в результаті інциденту, які надав, наприклад, сам надавач цифрових послуг, інший компетентний орган, у тому числі компетентний орган іншої держави- члена, або користувач послуги. Таким чином, компетентний орган не повинен мати загального обов'язки здійснювати нагляд за надавачами цифрових послуг.

(61) Компетентні органи повинні мати необхідні засоби для виконання своїх обов'язків, у тому числі повноваження отримувати достатню інформацію для оцінювання рівня безпеки мережевих та інформаційних систем.

(62) Інциденти можуть бути результатом злочинної діяльності, попередженню, розслідуванню та кримінальному переслідуванню яких сприяє координація та співпраця між операторами основних послуг, надавачами цифрових послуг, компетентними органами та правоохоронними органами. У разі підозри, що інцидент пов'язаний із серйозною злочинною діяльністю відповідно до національного законодавства або законодавства Союзу, держави- члени повинні заохочувати операторів основних послуг та надавачів цифрових послуг повідомляти відповідні правоохоронні органи про інциденти, щодо серйозного злочинного характеру яких виникає підозра. Якщо доречно, бажано, щоб координації компетентних органів та правоохоронних органів різних держав- членів сприяли Європейський центр боротьби з кіберзлочинністю (ЕСЗ) та ENISA.

(63) У багатьох випадках персональні дані викрадають у результаті інцидентів. З огляду на це, компетентні органи та органи з питань захисту даних повинні співпрацювати та обмінюватися інформацією щодо всіх відповідних питань, з метою боротьби з витоками персональних даних внаслідок інцидентів.

(64) Необхідно визнати юрисдикцію щодо надавачів цифрових послуг за державою- членом, в якій у відповідного надавач цифрових послуг має основний осідок в Союзі, який в принципі відповідає місцю, в якому надавач має головний офіс у Союзі. Осідок передбачає дієве та реальне здійснення діяльності за допомогою стабільного впорядкування. Адміністративно-правова форма такого впорядкування, незалежно від того чи це відділення, чи дочірня компанія, що володіє правосуб'єктністю, не є при цьому вирішальним чинником. Цей критерій не повинен залежати від того, чи мережеві та інформаційні системи фізично розташовані в даному місці; наявність та використання таких систем само по собі не становить такий основний осідок і, таким чином, не є критерієм визначення головного осідка.

(65) Якщо надавач цифрових послуг, заснований не в Союзі, пропонує послуги на території Союзу, він повинен призначити представника. Для того щоб визначити, чи такий надавач цифрових послуг пропонує послуги на території Союзу, необхідно впевнитися в очевидності його планів пропонувати послуги особам в одній чи декількох державах- членах. Однієї доступності на території Союзу веб-сайту, електронної адреси чи інших контактів надавача цифрових послуг або посередника, або використання мови, що загалом використовують у третій країні, в якій заснований надавач цифрових послуг, недостатньо для підтвердження такого наміру. Однак, такі чинники, як використання мови або валюти, що загалом використовують в одній або декількох державах- членах з можливістю замовлення послуг такою іншою мовою, або згадування клієнтів чи користувачів в Союзі, може вказувати на очевидність планів надавача цифрових послуг пропонувати послуги в межах Союзу. Представник повинен діяти від імені надавача цифрових послуг і компетентні органи або CSIRT повинні мати можливість контактувати з таким представником. Представник повинен бути безпосередньо призначений письмовим мандатом надавача цифрових послуг діяти від імені останнього щодо зобов'язань останнього відповідно до цієї Директиви, у тому числі звітування про інциденти.

(66) Стандартизація вимог до безпеки є обумовленим ринком процесом. Для забезпечення

збіжного застосування стандартів безпеки, держави- члени повинні заохочувати дотримання установлених стандартів або відповідність їм щоби забезпечити високий рівень безпеки мережевих та інформаційних систем на рівні Союзу. ENISA повинне допомагати державам- членам шляхом консультацій та настанов. З цією метою, може бути корисно розбити проект гармонізованих стандартів, що відповідатимуть Регламенту Європейського Парламенту і Ради (ЄС) № 1025/2012 ([8]).

(67) Суб'єкти, на яких не розповсюджується сфери застосування цієї Директиви, можуть зазнавати інцидентів, що матимуть значний вплив на послуги, які вони надають. Якщо вони вважатимуть, що повідомлення про настання таких інцидентів становить суспільний інтерес, вони повинні мати змогу добровільно повідомляти про них. Такі повідомлення повинен опрацьовувати компетентний орган або CSIRT, якщо таке опрацювання не становить непропорційний або неналежний тягар для відповідних держав- членів.

(68) Для того, щоб забезпечити єдині умови для імплементації цієї Директиви, необхідно покласти на Комісію виконавчі повноваження для встановлення процедурного порядку та умов, необхідних для функціонування Групи співпраці та вимог до безпеки та повідомлення, застосовних до надавачів цифрових послуг. Такі повноваження необхідно здійснювати відповідно до Регламенту Європейського Парламенту і Ради (ЄС) № 182/2011 ([9]). Ухвалюючи імплементаційні акти, пов'язані з процедурним порядком та умовами, необхідними для функціонування Групи співпраці, Комісія повинна враховувати позицію ENISA.

(69) Ухвалюючи імплементаційні акти щодо вимог до безпеки надавачів цифрових послуг, Комісія повинна враховувати позицію ENISA та повинна консультуватися із заінтересованими стейкхолдерами. Крім того, Комісію заохочують враховувати такі приклади: стосовно безпеки систем та устаткування: фізична безпека та безпека для довкілля, безпека постачання, контроль доступу до мережевих та інформаційних систем та цілісність мережевих та інформаційних систем; стосовно врегулювання інцидентів: процедури врегулювання інцидентів, спроможність виявляти інциденти, звітування та повідомлення про інциденти; стосовно управління безперервністю бізнесу: стратегія та плани на непередбачені випадки для забезпечення безперервності надання послуг, спроможності відновлення після аварій; та стосовно моніторингу, аудиту та випробування: політики моніторингу та ведення системних журналів, плани на випадок надзвичайних ситуацій, випробування мережевих та інформаційних систем, оцінювання безпеки та моніторинг відповідності.

(70) З метою імплементації цієї Директиви, Комісія повинна підтримувати, за доречності, зв'язки з відповідними секторальними комітетами та відповідними органами, заснованими на рівні Союзу у сферах, на які розповсюджується ця Директива.

(71) Комісія повинна періодично переглядати цю Директиву, консультуючись із заінтересованими стейкхолдерами, зокрема, щодо визначення потреби у змінах з огляду на зміни в соціальних, політичних, технологічних або ринкових умовах.

(72) Обмін інформацією щодо ризиків та інцидентів у межах Групи співпраці та мережі CSIRT та відповідність вимогам повідомляти про інциденти національним компетентним органам або CSIRT може вимагати опрацювання персональних даних. Таке опрацювання повинно відповідати Директиві Європейського Парламенту і Ради 95/46/ЄС ([10]) та Регламенту Європейського Парламенту і Ради (ЄС) № 45/2001 ([11]). З метою застосування цієї Директиви, Регламент Європейського Парламенту і Ради (ЄС) № 1049/2001 ([12]) необхідно застосовувати у відповідних випадках.

(73) З Європейським інспектором із захисту даних були проведені консультації відповідно до статті 28(2) Регламенту (ЄС) № 45/2001 і 14 червня 2013 року ([13]) він надав свій висновок.

(74) Оскільки держави-члени не можуть достатньо досягти мети цієї Директиви, а саме досягнення високого спільного рівня безпеки мережевих та інформаційних систем у Союзі, однак, через наслідки дій, її можна краще досягнути на рівні Союзу, Союзу може ухвалювати інструменти відповідно до принципу субсидіарності, як викладено в статті 5 Договору про функціонування Європейського Союзу. Відповідно до принципу

пропорційності, як викладено в зазначеній статті, ця Директива не виходить за межі необхідного для досягнення такої мети.

(75)Ця Директива поважає фундаментальні права та дотримується принципів, визнаних Хартією фундаментальних прав Європейського Союзу, зокрема права на повагу особистого життя та комунікацій, захисту персональних даних, свободи підприємництва, права власності, права дієвого правового захисту в суді та права бути вислуханим. Цю Директиву необхідно імплементувати відповідно до таких прав та принципів,

УХВАЛИЛИ ЦЮ ДИРЕКТИВУ:

ГЛАВА I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1

Предмет і сфера застосування

1. Ця Директива встановлює інструменти, маючи на меті досягти високого спільного рівня безпеки мережевих та інформаційних систем в межах Союзу для того, щоб покращити функціонування внутрішнього ринку.

2. З цією метою ця Директива:

(a) встановлює обов'язки для всіх держав- членів для ухвалення національної стратегії безпеки мережевих та інформаційних систем;

(b) створює Групу співпраці для підтримки та сприяння стратегічній співпраці та обміну інформацією серед держав- членів та розвитку повної довіри між ними;

(c) створює мережу груп реагування на інциденти, пов'язані з комп'ютерною безпекою («мережа CSIRT») з метою зміцнення повної довіри між державами- членами та сприяння швидкій та дієвій оперативній взаємодії;

(d) встановлює вимоги до безпеки та повідомлення для операторів основних послуг та надавачів цифрових послуг;

(e) встановлює обов'язки для держав- членів для призначення національних компетентних органів, єдиних контактних пунктів та CSIRT із завданнями, пов'язаними з безпекою мережевих та інформаційних систем.

3. Вимоги до безпеки та повідомлення, передбачені в цій Директиві, не повинні застосовуватися до підприємств, на які розповсюджуються вимоги статей 13a та 13b Директиви 2002/21/ЄС, або до надавачів довірчих послуг, на яких розповсюджуються вимоги статті 19 Регламенту (ЄС) № 910/2014.

4. Цю Директиву застосовують без обмеження Директиви Ради 2008/114/ЄС [(14)] та Директив Європейського Парламенту і Ради 2011/93/ЄС [(15)] та 2013/40/ЄС [(16)].

5. Без обмеження статті 346 TFEU, інформацією, яка є конфіденційною відповідно до правил Союзу та національних правил, таких як правила щодо комерційної таємниці, обмінюються з Комісією та іншими відповідними органами лише, якщо такий обмін необхідний для застосування цієї Директиви. Обсяг інформації для обміну обмежують до рівня, доцільного та пропорційного цілі такого обміну. Обмінюючись інформацією, необхідно зберігати її конфіденційність та захищати безпекові та комерційні інтереси операторів основних послуг та надавачів цифрових послуг.

6. Ця Директива не обмежує дій, що їх вживають держави- члени для охорони своїх істотних державних функцій, зокрема для забезпечення національної безпеки, у тому числі дій щодо захисту інформації, розкриття якої держави- члени вважають таким, що суперечить суттєвим інтересам їхньої безпеки, та для підтримки закону та порядку, зокрема щоби уможливити розслідування, розкриття та кримінальне переслідування кримінальних правопорушень.

7. Якщо секторальний правовий акт Союзу вимагає від операторів основних послуг чи надавачів цифрових послуг забезпечувати безпеку своїх мережевих та інформаційних систем або повідомляти про інциденти, за умови, що такі вимоги є щонайменше еквівалентними по суті обов'язкам, встановленим у цій Директиві, то необхідно застосовувати зазначені положення такого секторального правового акту ЄС.

Стаття 2

Опрацювання персональних даних

1. Опрацювання персональних даних відповідно до цієї Директиви необхідно здійснювати згідно з Директивою 95/46/ЄС.

2. Опрацювання персональних даних установами та органами Союзу відповідно до цієї Директиви необхідно здійснювати згідно з Регламентом (ЄС) № 45/2001.

Стаття 3

Мінімальна гармонізація

Без обмеження статті 16(10) та своїх зобов'язань відповідно до законодавства Союзу, держави- члени можуть ухвалювати або зберігати положення з метою досягнення вищого рівня безпеки мережевих та інформаційних систем.

Стаття 4

Терміни та означення

Для цілей цієї Директиви, застосовують такі терміни та означення:

(1) «мережева та інформаційна система» означає:

(a) мережу електронного зв'язку у розумінні пункту (a) статті 2 Директиви 2002/21/ЄС;

(b) будь-який пристрій або групу взаємоз'єднаних чи пов'язаних пристроїв, один або декілька з яких, відповідно до програми, здійснює автоматичне опрацювання цифрових даних; або

(c) цифрові дані, які зберігають, опрацьовують, видобувають або передають за допомогою елементів, згаданих в пунктах (a) та (b), для цілей їхньої експлуатації, використання, захисту та технічного обслуговування;

(2) «безпека мережевих та інформаційних систем» означає здатність мережевих та інформаційних систем витримувати — на певному рівні впевненості — будь-яку дію, що загрожує доступності, справжності, цілісності або конфіденційності збережених або переданих чи опрацьованих даних або пов'язаних послуг, які пропонують такі мережеві та інформаційні системи або які доступні за допомогою таких систем;

(3) «національна стратегія безпеки мережевих та інформаційних систем» означає рамки, що забезпечують стратегічні цілі та пріоритети безпеки мережевих та інформаційних систем на національному рівні;

(4) «оператор основних послуг» означає публічну або приватну організацію типу, вказаного в додатку II, що відповідає критеріям, встановленим у статті 5(2);

(5) «цифрова послуга» означає послугу у розумінні пункту (b) статті 1(1) Директиви Європейського Парламенту і Ради (ЄС) 2015/1535 [(17)], одного з типів, перелічених у додатку III;

(6) «надавач цифрових послуг» означає будь-яку юридичну особу, що надає цифрову послугу;

(7) «інцидент» означає будь-яку подію, що має фактичний негативний вплив на безпеку мережевих та інформаційних систем;

(8) «врегулювання інцидентів» означає всі процедури на підтримку виявлення, аналізу інциденту, обмеження його наслідків і реагування на нього;

(9) «ризик» означає будь-яку обставину чи подію, яку можна розумно виявити, що має потенційний негативний вплив на безпеку мережевих та інформаційних систем;

(10) «представник» означає будь-яку фізичну або юридичну особу, засновану в Союзі, явним чином призначену діяти від імені надавача цифрових послуг, заснованого не в Союзі, до якого можуть звертатися національний компетентний орган або CSIRT замість надавача цифрових послуг щодо обов'язків такого надавача цифрових послуг відповідно до цієї Директиви;

(11) «стандарт» означає стандарт у розумінні пункту (1) статті 2 Регламенту (ЄС) № 1025/2012;

(12) «специфікація» означає технічну специфікацію у розумінні пункту (4) статті 2 Регламенту (ЄС) № 1025/2012;

(13) «точка обміну інтернет-трафіком (IXP)» означає мережеве устаткування, що уможливлює взаємоз'єднання більше ніж двох незалежних автономних систем, насамперед з метою полегшення обміну інтернет-трафіком; IXP забезпечує взаємоз'єднання лише для автономних систем; IXP не вимагає від інтернет-трафіку, що проходить між будь-якою парою автономних систем-учасників, проходити через будь-яку третю автономну систему, а також вона не змінює такий трафік та не втручається у нього іншим чином;

(14) «система доменних імен (DNS)» означає ієрархічно розподілену систему імен у мережі, що стосується запитів доменних імен;

(15) «надавач послуг DNS» означає суб'єкт, який надає послуги DNS в інтернеті;

(16) «реєстр доменних імен верхнього рівня» означає суб'єкта, що керує реєстрацією доменних імен в інтернет у конкретному домені верхнього рівня (TLD) та адмініструє її;

(17) «електронний торговий майданчик» означає цифрову послугу, що дозволяє споживачам та/або торговцям, як відповідно визначено в пункті (a) та пункті (b) статті 4(1) Директиви Європейського Парламенту і Ради 2013/11/ЄС [(18)], укладати в інтернеті договори продажу або надання послуг з торговцями як на сайті електронного торгового майданчика, так і на веб-сайті торговця, який використовує комп'ютерні послуги, що їх надає електронний торговий майданчик;

(18) «електронна пошукова система» означає цифрову послугу, що дозволяє користувачам здійснювати пошук, в принципі, по всім веб-сайтам або по веб-сайтам конкретною мовою через запит за будь-якою темою у формі ключового слова, виразу чи іншого вводу, та видає посилання, за якими можна знайти інформацію, пов'язану із запитаним контентом;

(19) «послуга хмарних обчислень» означає цифрову послугу, що уможливлює доступ до масштабовного та еластичного пулу обчислювальних ресурсів спільного користування.

Стаття 5

Визначення операторів основних послуг

1. До 9 листопада 2018 року для кожного сектора та підсектора, зазначеного в додатку II, держави- члени повинні визначити операторів основних послуг із осідком на їхній території.

2. Критерії для визначення операторів основних послуг, як вказано в пункті (4) статті 4, такі:

(a) суб'єкт господарювання надає послугу, що є суттєвою для підтримки критичної соціальної та/або економічної діяльності;

(b) надання такої послуги залежить від мережевих та інформаційних систем; та

(c) інцидент матиме значний негативний вплив на надання такої послуги.

3. Для цілей параграфа 1, кожна держава- член повинна скласти список послуг, вказаних в пункті (a) параграфа 2.

4. Для цілей параграфа 1, якщо суб'єкт надає послугу, як вказано в пункті (a) параграфа 2 у двох або більше державах- членах, такі держави- члени повинні провести консультації одна з одною. Такі консультації проводять до того, як буде ухвалено рішення про визначення.

5. Держави- члени повинні регулярно — щонайменше кожні два роки після 9 травня 2018 року — переглядати та, за доцільності, оновлювати список визначених операторів основних послуг.

6. Роль Групи співпраці, відповідно до завдань, вказаних у статті 11 — підтримувати держав- членів у використанні послідовного підходу під час визначення операторів основних послуг.

7. Для цілей перегляду, вказаного в статті 23, до 9 листопада 2018 року (і кожні два роки після цього) держави-члени повинні подати Комісії інформацію, необхідну для надання Комісії можливості оцінити імплементацію цієї Директиви, зокрема послідовність підходів держав-членів до визначення операторів основних послуг. Така інформація повинна включати щонайменше:

(a) національні інструменти, що дозволяють визначати операторів основних послуг;

(b) список послуг, вказаних у параграфі 3;

(c) число операторів основних послуг, визначених для кожного сектора, вказаного в додатку II, та зазначення їхньої важливості відносно такого сектора;

(d) порогові значення, якщо вони існують, для визначення відповідного рівня постачання з урахуванням числа користувачів, які покладаються на таку послугу, як вказано в пункті (a) статті 6(1), або важливості такого конкретного оператора основних послуг, як вказано в пункті (f) статті 6(1).

З метою сприяння наданню порівнянної інформації, Комісія, максимально враховуючи позицію ENISA, може ухвалювати відповідні технічні настанови щодо параметрів інформації, вказаної в цьому параграфі.

Стаття 6

Значний негативний вплив

1. При визначенні вагомості негативного впливу, як вказано в пункті (c) статті 5(2), держави- члени повинні враховувати щонайменше такі міжсекторальні чинники:

(a) число користувачів, які залежать від послуги, яку надає відповідний суб’єкт;

(b) залежність інших секторів, вказаних у додатку II, від послуги, яку надає такий суб’єкт;

(c) вплив, який можуть мати інциденти, стосовно ступеню та тривалості, на економічну та соціальну діяльність або публічну безпеку;

(d) ринкова частка такого суб’єкта;

(e) географічне поширення стосовно місцевості, яка може піддаватися негативній дії інциденту;

(f) важливість суб’єкта для підтримки достатнього рівня послуги, враховуючи доступність альтернативних засобів для надання такої послуги.

2. Для того, щоб визначити чи інцидент матиме значний негативний вплив, держави члени повинні також, за доцільності, враховувати секторальні чинники.

ГЛАВА II
НАЦІОНАЛЬНІ РАМКИ ЩОДО БЕЗПЕКИ МЕРЕЖЕВИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Стаття 7

Національна стратегія щодо безпеки мережевих та інформаційних систем

1. Кожна держава- член ухвалює національну стратегію щодо безпеки мережевих та інформаційних систем, що визначає стратегічні цілі та доречну політику та регуляторні інструменти з метою досягнення та підтримання високого рівня безпеки мережевих та інформаційних систем та охоплення щонайменше секторів, вказаних у додатку II, та послуг,

вказаних у додатку III. Національна стратегія щодо безпеки мережевих та інформаційних систем стосується таких питань:

(a) цілі та пріоритети національної стратегії щодо безпеки мережевих та інформаційних систем;

(b) рамки врядування для досягнення цілей та пріоритетів національної стратегії щодо безпеки мережевих та інформаційних систем, у тому числі ролей та зобов'язань урядових органів та інших відповідних діячів;

(c) визначення інструментів, що стосуються підготованості, реагування та відновлення, у тому числі співпраці між публічним та приватним секторами;

(d) зазначення освітніх, навчальних програм, та програм підвищення поінформованості, що стосуються національної стратегії щодо безпеки мережевих та інформаційних систем;

(e) зазначення планів досліджень і розробок, що стосуються національної стратегії щодо безпеки мережевих та інформаційних систем;

(f) план оцінювання ризику для визначення ризиків;

(g) список різних діячів, залучених до реалізації національної стратегії щодо безпеки мережевих та інформаційних систем.

2. Держави- члени можуть вимагати допомоги ENISA у розроблянні національних стратегій щодо безпеки мережевих та інформаційних систем.

3. Держави- члени повинні надсилати Комісії свої національні стратегії щодо безпеки мережевих та інформаційних систем протягом трьох місяців після їх ухвалення. При цьому, держави- члени можуть вилучити елементи стратегії, що стосуються національної безпеки.

Стаття 8

Національні компетентні органи та єдиний контактний пункт

1. Кожна держава- член повинна призначити один або декілька національних компетентних органів щодо безпеки мережевих та інформаційних систем («компетентний орган»), що охоплює щонайменше сектори, вказані в додатку II, та послуги, вказані в додатку III. Держави- члени можуть покласти цю роль на існуючий орган чи органи.

2. Компетентні органи повинні здійснювати моніторинг застосування цієї Директиви на національному рівні.

3. Кожна держава- член повинна призначити єдиний національний контактний пункт щодо безпеки мережевих та інформаційних систем («єдиний контактний пункт»). Держави- члени можуть покласти цю роль на існуючий орган. Якщо держава- член призначає лише один компетентний орган, то такий компетентний орган також повинен бути єдиним контактним пунктом.

4. Єдиний контактний пункт повинен виконувати функцію зв'язку щоби забезпечувати транскордонну співпрацю органів держав- членів з відповідними органами в інших державах- членах, Групою співпраці, вказаною в статті 11, та мережею CSIRT, вказаною в статті 12.

5. Держави- члени повинні забезпечувати наявність у компетентних органів та єдиних контактних пунктів належних ресурсів для виконання призначених їм завдань у результативний та ефективний спосіб і досягнення таким чином цілей цієї Директиви. Держави- члени повинні забезпечувати результативну, ефективну та безпечну співпрацю призначених представників у Групі співпраці.

6. Компетентні органи та єдиний контактний пункт, якщо доцільно та відповідно до національного законодавства, повинні проводити консультації та співпрацювати з відповідними національними правоохоронними органами та національними органами з питань захисту даних.

7. Кожна держава- член повинна без затримки нотифікувати Комісії призначення компетентного органу та єдиного контактного пункту, їхні завдання та будь-які наступні зміни то до них. Кожна держава- член повинна оприлюднювати своє призначення компетентного органу

та єдиного контактного пункту. Комісія повинна публікувати список призначених єдиних контактних пунктів.

Стаття 9

Групи реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT)

1. Кожна держава- член повинна призначити одну або декілька CSIRT, що повинна відповідати вимогам, встановленим у пункті (1) додатка I, охоплюючи щонайменше сектори, вказані в додатку II, та послуги, вказані в додатку III, відповідальні за врегулювання ризиків та інцидентів відповідно до чітко визначеної процедури. CSIRT може бути створена в рамках компетентного органу.

2. Держави- члени повинні забезпечувати наявність в CSIRT належних ресурсів для результативного виконання своїх завдань, як визначено в пункті (2) додатка I.

Держави- члени повинні забезпечувати результативну, ефективну та безпечну співпрацю своїх CSIRT у мережі CSIRT, вказаної в статті 12.

3. Держави- члени повинні забезпечувати наявність у їхніх CSIRT доступу до належної, безпечної та стійкої інформаційно-комунікаційної інфраструктури на національному рівні.

4. Держави- члени повинні інформувати Комісію про обсяг завдань своїх CSIRT, а також про основні елементи процедури врегулювання інцидентів.

5. Держави- члени можуть вимагати допомоги ENISA у розвитку національних CSIRT.

Стаття 10

Співпраця на національному рівні

1. Якщо компетентний орган, єдиний контактний пункт та CSIRT однієї держави- члена є окремими, вони повинні співпрацювати для виконання зобов'язань, встановлених у цій Директиві.

2. Держави- члени забезпечують, щоб компетентні органи або CSIRT отримували повідомлення про інциденти, подані відповідно до цієї Директиви. Якщо держава- член вирішує, що CSIRT не повинні отримувати нотифікації, то CSIRT, в межах, необхідних для виконання своїх завдань, надається доступ до даних про інциденти, про які повідомляють оператори основних послуг, відповідно до статті 14(3) та (5), або надавачі цифрових послуг, відповідно до статті 16(3) та (6).

3. Держави- члени забезпечують, щоб компетентні органи або CSIRT інформували єдині контактні пункти про повідомлення про інциденти, подані відповідно до цієї Директиви.

До 9 серпня 2018 року та кожного року після цього єдиний контактний пункт подає Групі співпраці підсумковий звіт про отримані повідомлення, який включає число повідомлень, характер інцидентів, про які повідомлено, а також заходи, вжиті відповідно до статті 14(3) та (5) і статті 16(3) та (6).

ГЛАВА III
СПІВПРАЦЯ

Стаття 11

Група співпраці

1. Для підтримки та сприяння стратегічній співпраці та обміну інформацією між державами- членами та зміцнення повної довіри між ними, з огляду на досягнення високого спільного рівня безпеки мережевих та інформаційних систем у Союзі, цей документ засновує Групу співпраці.

Група співпраці виконує свої завдання на основі дворічних робочих програм, як вказано в другому підпараграфі параграфа 3.

2. Група співпраці складається з представників держав- членів, Комісії та ENISA.

Якщо доцільно, Група співпраці може запрошувати представників відповідних стейкхолдерів для участі в її роботі.

Комісія повинна надати секретаріат.

3. Завдання групи співпраці повинні бути такі:

(a) надання стратегічного керівництва діяльністю мережі CSIRT, створеною відповідно до статті 12;

(b) обмін кращими практиками щодо обміну інформацією, пов'язаною з повідомленням про інциденти, як вказано в статті 14(3) та (5) і статті 16(3) та (6);

(c) обмін кращими практиками між державами- членами та, у співпраці з ENISA, допомога державам- членам у нарощуванні потенціалу для забезпечення безпеки мережевих та інформаційних систем;

(d) обговорення спроможностей та підготованості держав -членів, а також добровільне оцінювання національних стратегій щодо безпеки мережевих та інформаційних систем та дієвості CSIRT і визначення кращої практики;

(e) обмін інформацією та кращою практикою щодо підвищення поінформованості й навчання;

(f) обмін інформацією та кращою практикою щодо досліджень і розробок, що стосуються безпеки мережевих та інформаційних систем;

(g) якщо доречно, обмін досвідом з відповідними установами, органами, офісами та агентствами Союзу у питаннях, що стосуються безпеки мережевих та інформаційних систем;

(h) обговорення стандартів та специфікацій, вказаних у статті 19, з представниками відповідних європейських організацій стандартизації;

(i) збір інформації про кращу практику щодо ризиків та інцидентів;

(j) щорічне перевіряння підсумкових звітів, вказаних у другому підпараграфі статті 10(3);

(k) обговорення роботи, що проводиться відносно навчань, що стосуються безпеки мережевих та інформаційних систем, освітніх програм та навчання, у тому числі роботи, яку виконує ENISA;

(l) за допомоги ENISA, обмін кращими практиками щодо визначення операторів основних послуг державами- членами, у тому числі, стосовно транскордонних залежностей, відносно ризиків та інцидентів;

(m) обговорення принципів передачі повідомлень про інциденти, як вказано в статтях 14 та 16.

До 9 лютого 2018 року та кожні два роки після цього, Група співпраці створює робочу програму стосовно дій, які необхідно вжити для досягнення її цілей та виконання завдань, які повинні узгоджуватися з цілям цієї Директиви.

4. З метою перегляду, вказаного в статті 23, та до 9 серпня 2018 року і кожні півтора роки після цього, Група співпраці готує звіт, що оцінює досвід, отриманий зі стратегічної співпраці відповідно до цієї статті.

5. Комісія повинна ухвалювати імплементаційні акти, що встановлюють процедурні порядок та умови, необхідні для функціонування Групи співпраці. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, вказаної в статті 22(2).

Для цілей першого підпараграфа, Комісія подає перший варіант імплементаційного акта комітету, вказаному в статті 22(1) до 9 лютого 2017 року.

Стаття 12

Мережа CSIRT

1. З метою зміцнення повної довіри між державами- членами та сприяння швидкій та дієвій оперативній взаємодії, цей документ створює мережу національних CSIRT.

2. Мережа CSIRT складається з представників CSIRT держав- членів та CERT-ЄС. Комісія повинна брати участь у мережі CSIRT як спостерігач. ENISA повинна надавати секретаріат та активно підтримувати співпрацю між CSIRT.

3. Завдання мережі CSIRT повинні бути такі:

(a) обмін інформацією щодо послуг CSIRT, операцій та спроможностей щодо співпраці;

(b) на запит представника CSIRT від держави- члена, яка потенційно піддається негативній дії інциденту — обмін некомерційною чутливою інформацією, пов'язаною з таким інцидентом та пов'язаних ризиків та її обговорення; однак, CSIRT будь-якої держави- члена може відмовитися від участі у такому обговоренні якщо існує ризик упередженості при розслідуванні такого інциденту;

(c) обмін неконфіденційною інформацією, що стосується окремих інцидентів, та добровільне забезпечення її доступності;

(d) на запит представника CSIRT держави- члена, обговорення та, якщо можливо, визначення координованого реагування на інцидент, визначений у межах юрисдикції тієї самої держави- члена;

(e) надання державам- членам підтримки у врегулюванні транскордонних інцидентів на основі їхньої добровільної взаємної допомоги;

(f) обговорення, дослідження та визначення додаткових форм оперативної взаємодії, у тому числі стосовно:

  (i) категорій ризиків та інцидентів;

  (ii) своєчасних попереджень;

  (iii) взаємної допомоги;

  (iv) принципів та умов координації, коли держави- члени реагують на транскордонні ризики та інциденти;

(g) інформування Групи співпраці про свою діяльність та подальші форми оперативної взаємодії, обговорені відповідно до пункту (f), та подання запитів на керівництво в цьому відношенні;

(h) обговорення уроків, здобутих з навчань стосовно безпеки мережевих та інформаційних систем, у тому числі організованих ENISA;

(i) на запит окремої CSIRT, обговорення спроможностей та підготованості такої CSIRT;

(j) видання настанов для сприяння конвергенції операційних практик щодо застосування положень цієї статті, які стосуються оперативної взаємодії.

4. З метою перегляду, вказаного в статті 23, та до 9 серпня 2018 року і кожні півтора роки після цього, мережа CSIRT готує звіт, що оцінює досвід, отриманий із оперативної взаємодії, у тому числі висновки та рекомендації, відповідно до цієї статті. Такий звіт також подають Групі співпраці.

5. Мережа CSIRT встановлює свій власний регламент роботи.

Стаття 13

Міжнародна співпраця

Союз може укладати міжнародні угоди, відповідно до статті 218 TFEU, з третіми країнами або міжнародними організаціями, що дозволяють та організовують їхню участь у певній діяльності Групи співпраці. Такі угоди повинні враховувати потребу у забезпеченні належної охорони даних.

ГЛАВА IV

БЕЗПЕКА МЕРЕЖЕВИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ОПЕРАТОРІВ ОСНОВНИХ ПОСЛУГ

Стаття 14

Вимоги до безпеки й повідомлення про інциденти

1. Держави- члени повинні забезпечувати, щоб оператори основних послуг вживали відповідних та пропорційних технічних та організаційних заходів для управління ризиками, пов‘язаним з безпекою мережевих та інформаційних систем, які вони використовують у своїх операціях. З огляду на новітні знання, такі заходи повинні забезпечувати рівень безпеки мережевих та інформаційних систем, що відповідає ризику, який виник.

2. Держави- члени забезпечують, щоб оператори основних послуг вживали відповідних заходів для запобігання та мінімізації впливу інцидентів, що впливають на безпеку мережевих та інформаційних систем, що використовуються для надання таких основних послуг з метою забезпечення безперервності таких послуг.

3. Держави- члени забезпечують, щоб оператори основних послуг без неналежної затримки повідомляли компетентний орган або CSIRT про інциденти, що мають значний вплив на безперервність основних послуг, які вони надають. Повідомлення повинні включати інформацію, що надає змогу компетентному органу або CSIRT визначати будь-який транскордонний вплив інциденту. Повідомлення повинне не призводити до збільшення відповідальності сторони, яка його надсилає.

4. Для визначення ступеня значності впливу інциденту, необхідно враховувати, зокрема, такі параметри:

(a) число користувачів, які піддаються негативній дії перебоїв основної послуги;

(b) тривалість інциденту;

(c) географічне поширення стосовно місцевості, яка піддається негативній дії інциденту.

5. На основі інформації, яку надав у повідомленні оператор основних послуг, компетентний орган або CSIRT інформує іншу державу- член (держави-члени), яка піддається негативній дії, про те, чи має інцидент значний вплив на безперервність основних послуг у такій державі- члені. При цьому компетентний орган або CSIRT згідно із законодавством Союзу або національним законодавством, що відповідає законодавству Союзу, повинна зберігати безпеку та комерційні інтереси оператора основних послуг, а також конфіденційність інформації, наданої в його повідомленні.

Якщо дозволяють обставини, компетентний орган або CSIRT надає оператору основних послуг, що надсилає повідомлення, відповідну інформацію про подальші заходи щодо його повідомлення, таку як інформація, що може допомогти результативному врегулюванню інциденту.

На запит компетентного органу або CSIRT єдиний контактний пункт пересилає повідомлення, вказані в першому підпараграфі, єдиним контактним пунктам інших держав- членів, які піддаються негативній дії.

6. Проконсультувавшись із оператором основних послуг, який надсилає повідомлення, компетентний орган або CSIRT можуть повідомити населення про окремі інциденти, якщо поінформованість громадськості необхідна для запобігання інциденту або врегулювання поточного інциденту.

7. Компетентні органи, які діють спільно в межах Групи співпраці, можуть розробляти та ухвалювати настанови щодо обставин, за яких від операторів основних послуг вимагається повідомляти про інциденти, у тому числі про параметри для визначення значності впливу інциденту, як вказано в параграфі 4.

Стаття 15

Реалізація й забезпечення виконання

1. Держави- члени забезпечують наявність в компетентних органів необхідних повноважень та засобів для оцінювання дотримання операторами основних послуг своїх зобов’язань відповідно до статті 14 та його впливу на безпеку мережевих та інформаційних систем.

2. Держави- члени забезпечують наявність в компетентних органів повноважень та засобів для того, щоби вимагати від операторів основних послуг надання:

(a) інформації, необхідної для оцінювання безпеки їхніх мережевих та інформаційних систем, у тому числі документально встановлених політик безпеки;

(b) доказів результативної реалізації політик безпеки, таких як результати аудиту безпеки, проведеного компетентним органом або кваліфікованим аудитором, і, в другому випадку, надати компетентному органу його результати, у тому числі підтверджуючі докази.

Запитуючи таку інформацію або доказ, компетентний орган повинен зазначити мету такого запиту та уточнити, яка інформація вимагається.

3. Оцінивши інформацію або результати аудитів безпеки, вказаних у параграфі 2, компетентний орган може видати операторам основних послуг зобов'язальні інструкції щодо усунення виявлених недоліків.

4. Компетентний орган повинен тісно співпрацювати з органами з питань захисту даних під час врегулювання інцидентів, які є наслідком витоків персональних даних.

ГЛАВА V
БЕЗПЕКА МЕРЕЖЕВИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ НАДАВАЧІВ ЦИФРОВИХ ПОСЛУГ

Стаття 16

Вимоги до безпеки й повідомлення про інциденти

1. Держави- члени забезпечують визначення надавачами цифрових послуг відповідних та пропорційних технічних та організаційних заходів для управління ризиками, що виникають для безпеки мережевих та інформаційних систем, які вони використовують у контексті пропонування послуг, вказаних у додатку III, в межах Союзу та вжиття таких заходів. З огляду на новітні знання, такі заходи повинні забезпечувати рівень безпеки мережевих та інформаційних систем, що відповідає ризику, який виник, та враховувати такі елементи:

(a) безпеку систем та устаткування;

(b) врегулювання інцидентів;

(c) управління безперервністю бізнесу;

(d) моніторинг, аудит та випробовування;

(e) відповідність міжнародним стандартам.

2. Держави- члени забезпечують вжиття надавачами цифрових послуг заходів для запобігання інцидентам, які впливають на безпеку їхніх мережевих та інформаційних систем, та мінімізації їх негативного впливу на послуги, вказані в додатку III, які пропонуються в межах Союзу, з метою забезпечення безперервності таких послуг.

3. Держави-члени забезпечують повідомлення надавачами цифрових послуг без неналежної затримки компетентного органу або CSIRT про будь-який інцидент, котрий має значний негативний вплив на надання послуги, вказаної в додатку III, яку вони пропонують в межах Союзу. Повідомлення повинні містити інформацію, що дає змогу компетентному органу або CSIRT визначати значність будь-якого негативного транскордонного впливу. Повідомлення повинне не призводити до збільшення відповідальності сторони, яка його надсилає.

4. Щоби визначити чи є негативний вплив інциденту значним, необхідно враховувати, зокрема, такі параметри:

(a) число користувачів, які піддаються негативній дії інциденту, зокрема користувачів, які залежать від послуги у наданні своїх власних послуг;

(b) тривалість інциденту;

(c) географічне поширення стосовно місцевості, яка піддається негативній дії інциденту;

(d) обсяг перебоїв у функціонуванні послуги;

(e) обсяг впливу на економічну та соціальну діяльність.

Зобов'язання повідомляти про інцидент застосовують лише, якщо надавач цифрових послуг має доступ до інформації, необхідної для оцінювання негативного впливу інциденту з урахуванням параметрів, вказаних у першому підпараграфі.

5. Якщо оператор основних послуг розраховує на стороннього надавача цифрових послуг для надання послуги, яка є основною для підтримки критичної соціальної та економічної діяльності, то такий оператор повідомляє про будь-який значний негативний вплив на безперервність основних послуг через інцидент, що піддає надавача цифрових послуг негативній дії.

6. За доцільності і, зокрема, якщо інцидент, вказаний у параграфі 3, стосується двох або більше держав- членів, компетентний орган або CSIRT повідомляє інші держави- члени, які піддаються негативній дії. При цьому, компетентні органи, CSIRT та єдині контактні пункти згідно із законодавством Союзу або національним законодавством, що відповідає законодавству ЄС, повинні зберігати безпеку надавача цифрових послуг та комерційні інтереси, а також конфіденційність наданої інформації.

7. Проконсультувавшись із відповідним надавачем цифрових послуг, компетентний орган або CSIRT і, за доцільності, органи або CSIRT інших держав- членів можуть повідомити населення про окремі інциденти або вимагати цього від надавача цифрових послуг, якщо поінформованість громадські необхідна для запобігання інциденту або врегулювання поточного інциденту, або якщо розкриття інциденту іншим чином відповідає інтересам громадськості.

8. Комісія повинна ухвалити імплементаційні акти для додаткового уточнення елементів, вказаних в параграфі 1, та параметрів, перелічених в параграфі 4 цієї статті. Такі імплементаційні акти необхідно ухвалити згідно з експертною процедурою, вказаною в статті 22(2), до 9 серпня 2017 року.

9. Комісія може ухвалювати імплементаційні акти, що встановлюють формати та процедури, застосовні до вимог до повідомлення. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, вказаної в статті 22(2).

10. Без обмеження статті 1(6), держави- члени не повинні накладати на надавачів цифрових послуг будь-яких додаткових вимог до безпеки або повідомлення.

11. Глава V не застосовується до мікро- та малих підприємств, як визначено в Рекомендації Комісії 2003/361/ЄС [(19)].

Стаття 17

Реалізація й забезпечення виконання

1. Держави- члени забезпечують вжиття компетентними органами заходів, якщо необхідно, за допомогою наглядових заходів *ex post*, за умови отримання доказів невідповідності надавача цифрових послуг вимогам, встановленим у статті 16. Такі докази може подати компетентний орган іншої держави- члена, в якій надається послуга.

2. Для цілей параграфа 1, компетентні органи повинні мати необхідні повноваження та засоби для того, щоби вимагати від надавачів цифрових послуг:

(a) надання інформації, необхідної для оцінювання безпеки їхніх мережевих та інформаційних систем, у тому числі документально встановлених політик безпеки;

(b) усунення будь-якої невідповідності вимогам, встановленим у статті 16.

3. Якщо надавач цифрових послуг має основний осідок або представника у державі- члені, але його мережеві та інформаційні системи розташовані в одній або декількох державах- членах, компетентний орган держави- члена головного осідка або представника та компетентні органи таких інших держав- членів повинні співпрацювати та допомагати один одному мірою необхідності. Така допомога та співпраця може охоплювати обмін інформацією між відповідними компетентними органами та запити на вжиття наглядових заходів, вказаних в параграфі 2.

Стаття 18

Юрисдикція та територіальність

1. Для цілей цієї Директиви, надавач цифрових послуг вважається таким, що знаходиться під юрисдикцією держави- члена, в якій він має головний осідок. Надавач цифрових послуг вважається таким, в якого є головний осідок у державі- члені, якщо у такій державі- члені він має головний осідок.

2. Надавач цифрових послуг, заснований не в Союзі, але пропонує послуги, вказані в додатку III в межах Союзу, повинен призначити представника в Союзі. Представник повинен бути заснований в одній з тих держав- членів, в яких пропонують такі послуги. Надавач цифрових послуг вважається таким, що знаходиться під юрисдикцією держави- члена, в якій засновано його представника.

3. Призначення надавачем цифрових послуг свого представника не повинно обмежувати судові позови, які можуть бути подані проти самого надавача цифрових послуг.

ГЛАВА VI
СТАНДАРТИЗАЦІЯ ТА ДОБРОВІЛЬНА НОТИФІКАЦІЯ

Стаття 19

Стандартизація

1. Для сприяння конвергентної імплементації статті 14(1) та (2) і статті 16(1) та (2), держави- члени, без нав’язування або дискримінації на користь використання певного типу технології, повинні заохочувати використання європейських або міжнародно визнаних стандартів та специфікацій, які стосуються безпеки мережевих та інформаційних систем.

2. ENISA, у співпраці з державами- членами повинно розробляти поради та настанови відносно технічних сфер, які необхідно враховувати стосовно параграфа 1, а також відносно вже існуючих стандартів, у тому числі національних стандартів держав- членів, що дозволяють охопити такі сфери.

Стаття 20

Добровільне повідомлення

1. Без обмеження статті 3, суб’єкти, що їх не були визначено як операторів основних послуг та що не є надавачами цифрових послуг, можуть добровільно повідомляти про інциденти, що мають значний негативний вплив на безперервність послуг, які вони надають.

2. Опрацьовуючи повідомлення, держави- члени повинні діяти згідно із процедурою, встановленою в статті 14. Держави- члени можуть надати опрацюванню обов’язкових повідомлень вищий пріоритет, ніж опрацюванню добровільних повідомлень. Добровільні повідомлення опрацьовують лише якщо така опрацювання не складає непропорційного або неналежного тягаря для відповідних держав-членів.

Добровільне повідомлення не повинно спричиняти накладання на суб’єкта, який його надсилає, будь-яких зобов’язань, які б не розповсюджувались на нього у випадку його ненадсилання.

ГЛАВА VII
ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 21

Санкції

Держави- члени повинні встановити правила щодо санкцій, застосовних до порушень національних положень, ухвалених відповідно до цієї Директиви, та вживати всі необхідні заходи для забезпечення їх виконання. Передбачені санкції повинні бути дієвими,

пропорційними і стримувальними. Держави- члени повинні повідомити Комісію про такі правила та такі заходи до 9 травня 2018 року, а також без затримки повідомляти її про будь-які подальші зміни, які на них впливають.

Стаття 22

Процедура комітету

1. Комісії повинен надавати допомогу Комітет з безпеки мережевих та інформаційних систем. Такий комітет є комітетом у розумінні Регламенту (ЄС) № 182/2011.

2. У разі покликання на цей параграф, застосовується стаття 5 Регламенту (ЄС) № 182/2011

Стаття 23

Перегляд

1. До 9 травня 2019 року Комісія повинна подати звіт Європейському Парламенту і Раді, з оцінкою послідовності підходу, який держави- члени застосовували у визначенні операторів основних послуг.

2. Комісія повинна періодично переглядати функціонування цієї Директиви та звітувати Європейському Парламентові й Раді. З цією метою та з огляду на подальше просування стратегічної та операційної співпраці, Комісія повинна брати до уваги звіти Групи співпраці та мережі CSIRT про досвід, отриманий на стратегічно-операційному рівні. У своєму перегляді Комісія також повинна оцінити списки, що містяться в додатках II та III, а також послідовність у визначенні операторів основних послуг та послуг у секторах, вказаних у додатку II. Перший звіт необхідно подати до 9 травня 2021 року.

Стаття 24

Перехідні положення

1. Без обмеження статті 25 та з метою надання державам- членам додаткових можливостей для належної співпраці протягом періоду транспозиції, Група співпраці та мережа CSIRT повинна почати виконання завдань, поставлених у статтях 11(3) та 12(3) відповідно, до 9 лютого 2017 року.

2. На період з 9 лютого 2017 року до 9 листопада 2018 року та в цілях допомоги державам- членам у застосуванні послідовного підходу у визначенні операторів основних послуг, Група співпраці повинна обговорити цей процес, суть та тип національних інструментів, що дозволяють визначення операторів основних послуг у межах конкретного сектора за критеріями, встановленими в статтях 5 та 6. Група співпраці також повинна обговорювати, на запит держави- члена, конкретні проекти національних актів такої держави- члена, що дозволяють визначення операторів основних послуг у межах конкретного сектора за критеріями, встановленими в статтях 5 та 6.

3. До 9 лютого 2017 року та в цілях цієї статті, держави- члени повинні забезпечувати належне представництво у Групі співпраці та мережі CSIRT.

Стаття 25

Транспозиція

1. Держави- члени повинні до 9 травня 2018 року ухвалити й опублікувати закони, підзаконні нормативно-правові акти та адміністративні положення, необхідні для виконання вимог цієї Директиви. Вони повинні негайно проінформувати про це Комісію.

Вони повинні застосовувати такі інструменти з 10 травня 2018 року.

Коли держави- члени ухвалюють такі інструменти, вони повинні містити покликання на цю Директиву або супроводжуватися таким покликаннями у разі їх офіційної публікації. Методи здійснення такого покликання визначають держави- члени.

2. Держави- члени повинні передати Комісії тексти основних положень національного законодавства, які вони ухвалюють у сфері, що її регулює ця Директива.

Стаття 26

Набуття чинності

Ця Директива набуває чинності на двадцятий день після її публікації в *Офіційному віснику Європейського Союзу*.

Стаття 27

Адресати

Цю Директиву адресовано державам-членам.

Вчинено у Страсбурзі, 6 липня 2016 року.

За Європейський Парламент
Президент
M. SCHULZ
За Раду
Президент
I. KORČOK

---

(1) OB C 271, 19.09.2013, с. 133.

(2) Позиція Європейського Парламенту від 13 березня 2014 року (ще не опубліковано в Офіційному віснику) та позиція Ради у першому читанні від 17 травня 2016 року (ще не опубліковано в Офіційному віснику). Позиція Європейського Парламенту від 6 липня 2016 року (ще не опубліковано в Офіційному віснику).

(3) Директива Європейського Парламенту і Ради 2002/21/ЄС від 7 березня 2002 року про спільні регулятивні рамки для мереж та послуг електронного зв'язку (Рамкова Директива) (OB L 108, 24.04.2002, с. 33).

(4) Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних трансакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС (OB L 257, 28.08.2014, с. 73).

(5) Рішення Ради 2013/488/ЄС від 23 вересня 2013 року про правила безпеки для захисту інформації ЄС, що не підлягає розголошенню (OB L 274, 15.10.2013, с. 1).

(6) OB C 352, 07.10.2014, с. 4.

(7) Регламент Європейського Парламенту і Ради (ЄС) № 526/2013 від 21 травня 2013 року про Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) та про скасування Регламенту (ЄС) № 460/2004 (OB L 165, 18.06.2013, с. 41).

(8) Регламент Європейського Парламенту і Ради (ЄС) № 1025/2012 від 25 жовтня 2012 року про європейську стандартизацію, про зміни і доповнення до Директив Ради 89/686/ЄЕС та 93/15/ЄЕС та Директив Європейського Парламенту і Ради 94/9/ЄС, 94/25/ЄС, 95/16/ЄС, 97/23/ЄС, 98/34/ЄС, 2004/22/ЄС, 2007/23/ЄС, 2009/23/ЄС та 2009/105/ЄС та про скасування Рішення Ради 87/95/ЄЕС та Рішення Європейського Парламенту і Ради № 1673/2006/ЄС (OB L 316, 14.11.2012, с. 12).

(9) Регламент Європейського Парламенту і Ради (ЄС) № 182/2011 від 16 лютого 2011 року про встановлення правил та загальних принципів відносно механізмів контролю з боку держав-членів за реалізацією Комісією своїх виконавчих повноважень (OB L 55, 28.02.2011, с. 13).

(10) Директива Європейського Парламенту і Ради 95/46/ЄС від 24 жовтня 1995 року про захист осіб стосовно опрацювання персональних даних та про вільний рух таких даних (OB L 281, 23.11.1995, с. 31).

(11) Регламент Європейського Парламенту і Ради (ЄС) № 45/2001 від 18 грудня 2000 року про захист осіб стосовно опрацювання персональних даних інституціями та органами Співтовариства та про вільний рух таких даних (OB L 8, 12.01.2001, с. 1).

(12) Регламент Європейського Парламенту і Ради (ЄС) № 1049/2001 від 30 травня 2001 року про загальний доступ до документів Європейського Парламенту, Ради та Комісії (OB L 145, 31.05.2001, с. 43).

(13) OB C 32, 04.02.2014, с. 19.

(14) Директива Ради 2008/114/ЄС від 8 грудня 2008 року про визначення та призначення критичних європейських інфраструктур та про оцінювання потреби у покращенні їх захисту (OB L 345, 23.12.2008, с. 75).

(15) Директива Європейського Парламенту і Ради 2011/93/ЄС від 13 грудня 2011 року про боротьбу з сексуальним насильством та сексуальною експлуатацією дітей та дитячою порнографією та про заміну Рамкового рішення Ради 2004/68/ЮВС (ОВ L 335, 17.12.2011, с. 1).

(16) Директива Європейського Парламенту і Ради 2013/40/ЄС від 12 серпня 2013 року про напади на інформаційні системи та про заміну Рамкового рішення Ради 2005/222/ЮВС (ОВ L 218, 14.08.2013, с. 8).

(17) Директива Європейського Парламенту і Ради (ЄС) 2015/1535 від 9 вересня 2015 року про встановлення порядку надання інформації в сфері технічних регламентів та правил стосовно послуг інформаційного суспільства (ОВ L 241, 17.09.2015, с. 1).

(18) Директива Європейського Парламенту і Ради (ЄС) № 2013/11/ЄС від 21 травня 2013 року про альтернативне вирішення спорів стосовно споживчих спорів та про зміни і доповнення до Регламенту (ЄС) № 2006/2004 та Директиви 2009/22/ЄС (Директива про альтернативне вирішення спорів зі споживачами) (ОВ L 165, 18.06.2013, с. 63).

(19) Рекомендація Комісії 2003/361/ЄС від 6 травня 2003 року про визначення мікро-, малих та середніх підприємств (ОВ L 124, 20.05.2003, с. 36).

ДОДАТОК I

ВИМОГИ ТА ЗАВДАННЯ ГРУП РЕАГУВАННЯ НА ІНЦИДЕНТИ, ПОВ'ЯЗАНІ З КОМП'ЮТЕРНОЮ БЕЗПЕКОЮ (CSIRT)

Вимоги та завдання CSIRT повинну бути належним чином та чітко визначеними, їх необхідно підтримувати національною політикою та/або нормативно-правовими актами. Вони повинні містити таке:

(1) Вимоги до CSIRT:

(a) CSIRT повинні забезпечувати високий рівень доступності своїх послуг зв'язку, уникаючи елементів, відмова яких спричиняє відмову всієї системи (SPOF), та мати декілька засобів зв'язку з ними та зв'язку з іншими у будь-який час. Крім того, канали комунікації повинні бути чітко визначені та добре відомі клієнтурі та співпрацюючим партнерам.

(b) Приміщення та допоміжні інформаційні системи CSIRT повинні бути розташовані у безпечних місцях.

(c) Безперервність бізнесу:

(i) CSIRT повинні бути оснащені належною системою управління запитами та їх скеровування, для полегшення їх передачі.

(ii) Необхідно належним чином забезпечувати CSIRT персоналом, щоб гарантувати доступність у будь-який час.

(iii) CSIRT повинна спиратися на інфраструктуру, безперервність якої забезпечена. Для цього повинні бути доступні запасні системи та резервний робочий простір.

(d) CSIRT повинні мати можливість за бажанням брати участь у мережах міжнародної співпраці.

(2) Завдання CSIRT:

(a) Завдання CSIRT повинні включати щонайменше:

(i) моніторинг інцидентів на національному рівні;

(ii) забезпечення своєчасного попередження, сигналів тривоги, оголошень та розповсюдження інформації про ризики та інциденти серед відповідних стейкхолдерів;

(iii) реагування на інциденти;

(iv) забезпечення динамічного аналізу ризиків та інцидентів й інформації про поточну ситуацію;

(v) участь у мережі CSIRT.

(b) CSIRT повинна встановити відносини співпраці з приватним сектором.

(c) Для сприяння співпраці, CSIRT повинні сприяти ухваленню та використанню спільних

або стандартизованих практик для:

(i) порядку врегулювання ризиків та інцидентів;

(ii) схем класифікації інцидентів, ризиків та інформації.

ДОДАТОК II

ТИПИ СУБ'ЄКТІВ ДЛЯ ЦІЛЕЙ ПУНКТУ (4) СТАТТІ 4

Сектор	Підсектор	Тип суб'єкта
1.Енергетика	(a)Електроенергія	—Електроенергетичні підприємства, як визначено в пункті (35) статті 2 Директиви Європейського Парламенту і Ради 2009/72/ЄС (1), що виконують функцію «постачання», як визначено в пункті (19) статті 2 зазначеної Директиви.
		—Оператори розподільчих систем, як визначено в пункті (6) статті 2 Директиви 2009/72/ЄС
		—Оператори систем передачі, як визначено в пункті (4) статті 2 Директиви 2009/72/ЄС
	(b)Нафта	—Оператори нафтопроводів
		—Оператори нафтовидобувного, -переробного устаткування, установок підготовки нафти, нафтозберігальних та -передавальних потужностей
	(c)Газ	—Постачальні підприємства, як визначено в пункті (8) статті 2 Директиви Європейського Парламенту і Ради 2009/73/ЄС (2)
		—Оператори розподільчих систем, як визначено в пункті (6) статті 2 Директиви 2009/73/ЄС
		—Оператори систем передачі, як визначено в пункті (4) статті 2 Директиви 2009/73/ЄС
		—Оператори систем зберігання, як визначено в пункті (10) статті 2 Директиви 2009/73/ЄС
		—Оператори систем скрапленого природного газу, як визначено в пункті (12) статті 2 Директиви 2009/73/ЄС
		—Суб'єкти ринку природного газу, як визначено в пункті (1) статті 2 Директиви 2009/73/ЄС
		—Оператори устаткування для перероблення та підготовки природного газу.

2.Транспорт	(a)Повітряний транспорт	—Авіаперевізники, як визначено в пункті (4) статті 3 Регламенту Європейського Парламенту і Ради 300/2008 [3]
		—Органи управління аеропортами, як визначено в пункті (2) статті 2 Директиви Європейського Парламенту і Ради 2009/12/ЄС [4], аеропорти, як визначено в пункті (1) статті 2 вказаної Директиви, у тому числі основні аеропорти, перелічені в секції 2 додатка II до Регламенту Європейського Парламенту і Ради (ЄС) № 1315/2013 [5], та суб'єкти, що експлуатують допоміжне обладнання, розташоване в аеропортах
		—Оператори управління рухом, що надають послуги керування повітряним рухом, як визначено в пункті (1) статті 2 Регламенту Європейського Парламенту і Ради (ЗС) № 549/2004 [6]
	(b)Залізничний транспорт	—Керівники інфраструктур, як визначено в пункті (2) статті 3 Директиви Європейського Парламенту і Ради 2012/34/ЄС [7]
		—Залізничні підприємства, як визначено в пункті (1) статті 3 Директиви 2012/34/ЄС, у тому числі оператори об'єктів обслуговування інфраструктури, як визначено в пункті (12) статті 3 Директиви 2012/34/ЄС
	(c)Водний транспорт	—Компанії-оператори внутрішнього, морського, каботажного пасажирського та вантажного водного транспорту, як визначено для морських перевезень в додатку I до Регламенту Європейського Парламенту і Ради (ЄС) № 725/2004 [8], за винятком індивідуальних суден, якими оперують такі компанії
		—Керівні органи портів, як визначено в пункті (1) статті 3 Директиви Європейського Парламенту і Ради 2005/65/ЄС [9], у тому числі їхні портові споруди, як визначено в пункті (11) статті 2 Регламенту (ЄС) № 725/2004, та суб'єкти, які експлуатують установки та обладнання, розташовані в портах
		—Оператори служб руху суден, як визначено в пункті (o) статті 3 Директиви

		Європейського Парламенту і Ради 2002/59/ЄС [(10)]
	(d)Дорожній транспорт	—Дорожні органи, як визначено в пункті (12) статті 2 Делегованого Регламенту Комісії (ЄС) 2015/962 [(11)], відповідальні за управління рухом
		—Оператори інтелектуальних транспортних систем, як визначено в пункті (1) статті 4 Директиви Європейського Парламенту і Ради 2010/40/ЄС [(12)]
3.Банківська діяльність		Кредитні установи, як визначено в пункті (1) статті 4 Регламенту Європейського Парламенту і Ради (ЄС) № 575/2013 [(13)]
4.Інфраструктури фінансових ринків		—Оператори торгових майданчиків, як визначено в пункті (24) статті 4 Директиви Європейського Парламенту і Ради 2014/65/ЄС [(14)]
		—Центральні контрагенти (ССР), як визначено в пункті (1) статті 2 Регламенту Європейського Парламенту і Ради (ЄС) № 648/2012 [(15)]
5.Сектор охорони здоров’я	Заклади охорони здоров’я (у тому числі лікарні та приватні клініки)	Постачальники послуг охорони здоров’я, як визначено в пункті (g) статті 3 Директиви Європейського Парламенту і Ради 2011/24/ЄС [(16)]
6.Постачання та розповсюдження питної води		Постачальники та розповсюджувачі води для споживання людиною, як визначено в пункті (1) (a) статті 2 Директиви Ради 98/83/ЄС [(17)], але за винятком розповсюджувачів, для яких розповсюдження води для споживання людиною є лише частиною їхньої загальної діяльності з розповсюдження інших виробів широкого споживання та товарів, які не вважаються основними послугами.
7.Цифрова інфраструктура		—IXP
		—Надавачі послуг DNS
		—Реєстри імен у доменах верхнього рівня

[(1)] Директива Європейського Парламенту і Ради № 2009/72/ЄС від 13 липня 2009 року про спільні правила для внутрішнього ринку електроенергії та про скасування Директиви 2003/54/ЄС (OB L 211, 14.08.2009, с. 55).

[(2)] Директива Європейського Парламенту і Ради № 2009/73/ЄС від 13 липня 2009 року про спільні правила для внутрішнього ринку природного газу та про скасування Директиви 2003/55/ЄС (OB L 211, 14.08.2009, с. 94).

[(3)] Регламент Європейського Парламенту і Ради (ЄС) № 300/2008 від 11 березня 2008 року про спільні правила у сфері безпеки цивільної авіації та про скасування Регламенту (ЄС) № 2320/2002 (OB L 97, 09.04.2008, с. 72).

[(4)] Директива Європейського Парламенту і Ради 2009/21/ЄС від 11 березня 2009 року про аеропортові збори (OB L 70, 14.03.2009, с. 11).

[(5)] Регламент Європейського Парламенту і Ради (ЄС) № 1315/2013 від 11 грудня 2013 року про настанови Союзу для розвитку транс’європейської транспортної мережі та про скасування Рішення № 661/2010/ЄС (OB L 348, 20.12.2013, с. 1).

[(6)] Регламент Європейського Парламенту і Ради 549/2004 від 10 березня 2004 року про рамки створення єдиного повітряного простору Європи (рамковий Регламент) (OB L 96, 31.03.2004, с. 1).

(7) Директива Європейського Парламенту і Ради 2012/34/ЄС від 21 листопада 2012 року про заснування єдиної європейської залізничної зони (ОВ L 343, 14.12.2012, с. 32).

(8) Регламент Європейського Парламенту і Ради № 725/2004 від 31 березня 2004 року про посилення безпеки суден і портових споруд (ОВ L 129, 29.04.2004, с. 6).

(9) Директива Європейського Парламенту і Ради 2005/65/ЄС від 26 жовтня 2005 року про посилення безпеки портів (ОВ L 310, 25.11.2005, с. 28).

(10) Директива Європейського Парламенту і Ради 2002/59/ЄС від 27 червня 2002 року про заснування системи моніторингу руху суден та інформування в Співтоваристві та про скасування Директиви Ради 93/75/ЄЕС (ОВ L 208, 05.08.2002, с. 10).

(11) Делегований Регламент Комісії (ЄС) 2015/962 від 18 грудня 2014 року про доповнення Директиви Європейського Парламенту і Ради 2010/40/ЄС стосовно надання інформаційних послуг щодо руху у всьому ЄС у реальному часі (ОВ L 157, 23.06.2015, с. 21).

(12) Директива Європейського Парламенту і Ради 2010/40/ЄС від 7 липня 2010 року про рамки розгортання розумних транспортних систем у секторі дорожнього транспорту та взаємодію з іншими видами транспорту (ОВ L 207, 06.08.2010, с. 1).

(13) Регламент Європейського Парламенту і Ради (ЄС) № 575/2013 від 26 червня 2013 року про пруденційні вимоги для кредитних установ та інвестиційних фірм та про зміни і доповнення до Регламенту (ЄС) № 648/2012 (ОВ L 176, 27.06.2013, с. 1).

(14) Директива Європейського Парламенту і Ради (ЄС) № 2014/65/ЄС від 15 травня 2014 року про ринки фінансових інструментів та про зміни і доповнення до Директиви 2002/92/ЄС та Директиви 2011/61/ЄСОВ L 173, 12.06.2014, с. 349).

(15) Регламент Європейського Парламенту і Ради (ЄС) № 648/2012 від 4 липня 2012 року про позабіржові похідні фінансові інструменти, центральних контрагентів та реєстри трансакцій (ОВ L 201, 27.07.2012, с. 1).

(16) Директива Європейського Парламенту і Ради 2011/24/ЄС від 9 березня 2011 року про застосування прав пацієнтів у транскордонній системі охорони здоров'я (ОВ L 88, 04.04.2011, с. 45).

(17) Директива Ради 98/83/ЄС від 3 листопада 1998 року про якість води, призначеної для споживання людиною (ОВ L 330, 05.12.1998, с. 32).

ДОДАТОК III

ТИПИ ЦИФРОВИХ ПОСЛУГ ДЛЯ ЦІЛЕЙ ПУНКТУ (5) СТАТТІ 4

1. Електронний торговий майданчик.
2. Електронна пошукова система.
3. Послуга хмарних обчислень.