Урядовий офіс координації європейської та євроатлантичної інтеграції
Секретаріату Кабінету Міністрів України

Переклад затверджений

Заступник генерального директора Урядового офісу
координації європейської та
євроатлантичної інтеграції
Секретаріату Кабінету Міністрів України — О.В. Генчев
(найменування посади) (підпис) (ініціали та прізвище)

01 липня 2021 р.

РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2019/881

від 17 квітня 2019 року

про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку)

(Текст стосується ЄЕП)

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 проєкту законодавчого акта національним парламентам,

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

Беручи до уваги висновок Комітету регіонів ([2]),

Діючи згідно зі звичайною законодавчою процедурою ([3]),

Оскільки:

(1) Мережеві та інформаційні системи й електронні комунікаційні мережі та послуги відіграють важливу роль у суспільстві та стали опорою економічного зростання. Інформаційно-комунікаційні технології (ІКТ) лежать в основі комплексних систем, які підтримують щоденну життєдіяльність суспільства, забезпечують функціонування економік у ключових сферах, серед яких охорона здоров'я, енергетика, фінанси та транспорт, і зокрема підтримують функціонування внутрішнього ринку.

(2) Використання мережевих та інформаційних систем громадянами, організаціями та підприємствами по всьому Союзу сягнуло наскрізного характеру. Діджитизація та конективність стали основними характеристиками дедалі більшої кількості продуктів і послуг, а з настанням ери інтернету речей протягом наступного десятиліття по всьому Союзу очікується подальша поява надзвичайно великої кількості цифрових пристроїв, здатних під'єднуватися до всесвітньої мережі Інтернет. Попри зростання кількості пристроїв, що під'єднуються до мережі Інтернет, недостатність вбудованих засобів забезпечення безпеки і стійкості призводить до послаблення кібербезпеки. У цьому

РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2019/881

від 17 квітня 2019 року

про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку)

(Текст стосується ЄЕП)

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 проєкту законодавчого акта національним парламентам,

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

Беручи до уваги висновок Комітету регіонів ([2]),

Діючи згідно зі звичайною законодавчою процедурою ([3]),

Оскільки:

(1) Мережеві та інформаційні системи й електронні комунікаційні мережі та послуги відіграють важливу роль у суспільстві та стали опорою економічного зростання. Інформаційно-комунікаційні технології (ІКТ) лежать в основі комплексних систем, які підтримують щоденну життєдіяльність суспільства, забезпечують функціонування економік у ключових сферах, серед яких охорона здоров'я, енергетика, фінанси та транспорт, і зокрема підтримують функціонування внутрішнього ринку.

(2) Використання мережевих та інформаційних систем громадянами, організаціями та підприємствами по всьому Союзу сягнуло наскрізного характеру. Діджитизація та конективність стали основними характеристиками дедалі більшої кількості продуктів і послуг, а з настанням ери інтернету речей протягом наступного десятиліття по всьому Союзу очікується подальша поява надзвичайно великої кількості цифрових пристроїв, здатних під'єднуватися до всесвітньої мережі Інтернет. Попри зростання кількості пристроїв, що під'єднуються до мережі Інтернет, недостатність вбудованих засобів забезпечення безпеки і стійкості призводить до послаблення кібербезпеки. У цьому контексті обмежене використання сертифікації призводить до того, що фізичні особи, організації та підприємства як користувачі не мають достатньої інформації про характеристики кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ, що підриває їхню довіру до цифрових інструментів. Мережеві та інформаційні системи здатні забезпечувати підтримку всіх аспектів нашого життя та сприяти зростанню економіки Союзу. Вони є наріжним каменем на шляху до створення єдиного цифрового ринку.

(3) Зростання діджитизації та конективності підвищує ризики кібербезпеки, і таким чином робить суспільство в цілому більш вразливим до кіберзагроз та підвищує небезпеки, з якими можуть стикатися фізичні особи, у тому числі вразливі групи фізичних осіб, серед яких діти. Для пом'якшення згаданих ризиків потрібно вживати всіх необхідних заходів для підвищення кібербезпеки у Союзі, щоб забезпечити кращий захист від кіберзагроз мережевих та інформаційних систем, комунікаційних мереж, цифрових продуктів, послуг та пристроїв, якими користуються громадяни, організації та підприємства — від малих і середніх підприємств (МСП), як визначено в Рекомендації Комісії 2003/361/ЄС ([4]), до операторів критичної інфраструктури.

(4) Шляхом надання доступу до відповідної інформації громадськості Європейське агентство з питань

мережевої та інформаційної безпеки (ENISA), створене Регламентом Європейського Парламенту і Ради (ЄС) № 526/2013 ([5]), сприятиме розвитку сфери кібербезпеки в Союзі, зокрема, МСП та стартапів. ENISA повинне прагнути до тіснішої співпраці з університетами та дослідними установами для сприяння зменшенню залежності від продуктів і послуг у сфері кібербезпеки, що походять з-поза меж Союзу, та для посилення ланцюгів постачання у межах Союзу.

(5) Кібератаки як явище стаються дедалі частіше, і зв'язана економіка й суспільство як найбільш вразливі до кіберзагроз та кібератак вимагають надійнішого захисту. І хоча кібератаки часто носять транскордонний характер, компетенції відповідних органів у сфері кібербезпеки та правозастосування та вживані ними заходи з реагування в рамках їхніх політик переважно обмежені національними рамками. Широкомасштабні інциденти можуть призводити до порушень у наданні основних послуг по всьому Союзу. Це виносить необхідність ефективного та скоординованого реагування й управління кризами на рівень Союзу на основі спеціальних політик та ширших інструментів європейської солідарності та взаємної допомоги. Крім того, для виробників політики, промисловості та користувачів важливими є регулярні оцінювання стану кібербезпеки та стійкості у Союзі на основі надійних даних Союзу, а також систематичні прогнози майбутнього розвитку, проблем та загроз як на рівні Союзу, так і в глобальному масштабі.

(6) У світлі зростання викликів кібербезпеки, що постають перед Союзом, існує потреба в комплексному наборі заходів, створених на основі минулих дій і заходів Союзу для сприяння досягненню цілей, що взаємно посилюють одна одну. Такі цілі включають подальше підвищення спроможності та готовності держав-членів і підприємств, а також покращення співпраці, обміну інформацією та координації між усіма державами-членами та установами, органами, офісами й агентствами Союзу. Крім того, зважаючи на позакордонний характер кіберзагроз, існує потреба в нарощуванні потенціалу на рівні Союзу для доповнення заходів держав-членів, зокрема, у випадках великомасштабних транскордонних інцидентів та криз, враховуючи при цьому важливість збереження та подальшого посилення національної спроможності реагувати на кіберзагрози будь-якого масштабу.

(7) Також існує потреба в додаткових зусиллях, спрямованих на підвищення обізнаності громадян, організацій та підприємств про питання, пов'язані з кібербезпекою. Крім того, оскільки інциденти підривають довіру до надавачів цифрових послуг та до єдиного цифрового ринку як такого, особливо серед споживачів, існує потреба в подальшому посиленні довіри шляхом розповсюдження у прозорий спосіб інформації про рівні безпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ з акцентом на тому, що навіть сертифікація кібербезпеки високого рівня не може гарантувати, що продукт ІКТ, послуга ІКТ або процес ІКТ є повністю безпечними. Зростання довіри може бути досягнуто завдяки сертифікації Союзу, що визнаватиметься у всіх державах-членах та передбачатиме спільні вимоги до кібербезпеки і критерії оцінювання для всіх національних ринків і секторів.

(8) Кібербезпека є питанням не суто технологічним. Для неї має велике значення людська поведінка. Відповідно, необхідно всіляко просувати «кібергігієну», а саме: прості та планові заходи, які у разі їх впровадження та здійснення на регулярній основі громадянами, організаціями та підприємствами мінімізують вплив ризиків від кіберзагроз.

(9) Для цілей посилення структур кібербезпеки Союзу важливо підтримувати й розвивати потенціал держав-членів з комплексного реагування на кіберзагрози, включно з транскордонними інцидентами.

(10) Користувачі бізнесового та приватного секторів повинні володіти точною інформацією стосовно рівня надійності, стосовно якого було сертифіковано їхні продукти ІКТ, послуги ІКТ та процеси ІКТ. У той же час жоден продукт ІКТ чи послуга ІКТ не є цілком кібербезпечними, тому потрібно просувати та пріоритизувати базові правила кібергігієни. Зважаючи на дедалі більшу доступність пристроїв Інтернету речей, може бути виділено низку добровільних заходів, за допомогою яких приватний сектор може посилювати довіру до безпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ.

(11) Сучасні продукти ІКТ та системи часто містять інтегровані одну чи більше сторонніх технологій та компонентів або покладаються на них; серед них модулі програмного забезпечення, бібліотеки або інтерфейси прикладних застосунків. Їх використання, яке часто називають «залежністю», може становити додаткові ризики для кібербезпеки, оскільки потенційні вразливості сторонніх компонентів можуть мати негативний вплив на безпеку продуктів ІКТ, послуг ІКТ та процесів ІКТ. У багатьох випадках виявлення та документування таких залежностей дає змогу кінцевим користувачам товарів ІКТ, послуг ІКТ та процесів ІКТ вдосконалювати власні дії з управління ризиками, пов'язаними з кібербезпекою, шляхом покращення, наприклад, управління вразливостями та процедур відновлення кібербезпеки користувачів.

(12) Організації, виробників або надавачів, що здійснюють проєктування та розробку продуктів ІКТ, послуг ІКТ або процесів ІКТ, необхідно заохочувати до впровадження на якомога раніших стадіях проєктування та розробки заходів, спрямованих на якомога вищий рівень захисту безпеки таких продуктів, послуг та процесів, щоб імовірність виникнення кібератак та потенційного впливу від них була мінімальною (концепція вбудованої безпеки). Необхідно забезпечити безпеку продукту ІКТ, послуги ІКТ або процесу ІКТ протягом строку служби через процеси проєктування та розробки, які повинні постійно розвиватися для скорочення ризику завдання шкоди внаслідок зловмисного використання.

(13) Підприємства, організації та публічний сектор повинні налаштовувати конфігурацію продуктів ІКТ, послуг ІКТ або процесів ІКТ, які вони розробили, у спосіб, який дасть змогу забезпечити високий рівень безпеки шляхом надання першому користувачу типової конфігурації з найбільш безпечними налаштуваннями з можливих (концепція типових параметрів безпеки), таким чином зменшивши для користувачів тягар, пов'язаний із належним налаштуванням конфігурації продукту ІКТ, послуги ІКТ або процесу ІКТ. Типові параметри безпеки не повинні вимагати з боку користувача тривалого налаштування конфігурації або специфічних технічних знань чи неінтуїтивної поведінки, та після запровадження повинні працювати без ускладнень та надійно. Якщо на індивідуальній основі аналіз ризиків та практичності засвідчить, що таке типове налаштування не є реалістичним, користувачу необхідно пропонувати можливість вибору найбільш безпечного налаштування.

(14) Регламентом Європейського Парламенту і Ради (ЄС) № 460/2004 ([6]) було створено ENISA для цілей сприяння досягненню цілей із забезпечення високого та результативного рівня мережевої та інформаційної безпеки в межах Союзу, та з розвитку культури мережевої та інформаційної безпеки на користь громадян, споживачів, підприємств та публічних адміністрацій. Регламентом Європейського Парламенту і Ради (ЄС) № 1007/2008 ([7]) було розширено мандат ENISA до березня 2012 року. Регламентом Європейського Парламенту і Ради (ЄС) № 580/2011 ([8]) було додатково розширено мандат ENISA до 13 вересня 2013 року. Регламентом (ЄС) № 526/2013 було розширено мандат ENISA до 19 червня 2020 року.

(15) Союзом уже було вжито важливих кроків для забезпечення кібербезпеки та для підвищення довіри до цифрових технологій. У 2013 році було ухвалено Стратегію Європейського Союзу з кібербезпеки, яка мала на меті скерувати політику Союзу з реагування на загрози і ризики для кібербезпеки. З наміром забезпечити кращий захист для громадян в онлайновому середовищі у 2016 році було ухвалено перший правовий акт Союзу у сфері кібербезпеки у формі Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 ([9]). Директивою (ЄС) 2016/1148 було запроваджено вимоги щодо національної спроможності у сфері кібербезпеки, встановлено перші механізми для посилення стратегічної та операційної співпраці між державами-членами, та визначено обов'язки стосовно заходів безпеки та повідомлень про інциденти по всіх секторах, які є життєво важливими для економіки й суспільства, серед яких енергетика, транспорт, постачання та розподіл питної води, інфраструктури банківського та фінансового ринків, сфера громадського здоров'я, цифрова інфраструктура та ключові надавачі цифрових послуг (пошукові системи, послуги хмарних обчислень та електронні торгові майданчики).

Ключову роль у забезпеченні виконання зазначеної Директиви було покладено на ENISA. Крім того, Порядок денний Європейського Союзу з безпеки визначає важливим пріоритетом ефективну

боротьбу з кіберзлочинністю, що в цілому має сприяти досягненню вищого рівня кібербезпеки. Також досягненню вищого рівня кібербезпеки на єдиному цифровому ринку сприяють і інші правові акти, серед яких Регламент Європейського Парламенту і Ради (ЄС) 2016/679 ([10]) та директиви Європейського Парламенту і Ради 2002/58/ЄС ([11]) та (ЄС) 2018/1972 ([12]).

(16) З моменту ухвалення Стратегії Європейського Союзу з кібербезпеки у 2013 році та останнього перегляду мандату ENISA загальний політичний контекст суттєво змінився, оскільки глобальне середовище стало більш невизначеним та менш безпечним. На цьому тлі та в контексті позитивного розвитку ролі ENISA як довідкового пункту для консультацій та експертних знань, як фасилітатора співпраці та нарощування потенціалу, а також у рамках нової політики Союзу з кібербезпеки, необхідно переглянути мандат ENISA, визначити його роль у зміненій екосистемі кібербезпеки та забезпечити, щоб воно дієво сприяло реагуванню Союзу на проблеми з кібербезпекою, що виникли внаслідок радикальних трансформацій масштабу кіберзагроз, для яких поточний мандат не є достатнім, як було визнано під час оцінювання діяльності ENISA.

(17) ENISA, створене відповідно до цього Регламенту, повинне бути наступником ENISA, створеного відповідно до Регламенту (ЄС) № 526/2013. ENISA повинне виконувати завдання, покладені на нього цим Регламентом та іншими правовими актами Союзу у сфері кібербезпеки та, серед іншого, надавати консультацію й ділитися експертними знаннями, а також діяти як центр інформації та знань Союзу. Воно повинне сприяти обміну найкращими практиками між державами-членами та приватними заінтересованими сторонами, подавати пропозиції стосовно політики Комісії та державам-членам, діяти як довідковий центр для ініціатив секторальної політики Союзу стосовно кібербезпеки та сприяти операційній співпраці як між державами-членами, так і між державами-членами й установами, органами, офісами та агентствами Союзу.

(18) У рамках Рішення 2004/97/ЄС, Євратом, ухваленого за спільною згодою представників держав-членів на засіданні на рівні голів держав або урядів ([13]), представники держав-членів ухвалили рішення про те, що головний офіс ENISA повинен бути розташований у Греції в місті, визначеному урядом Греції. Держава-член ведення діяльності ENISA повинна забезпечити найкращі можливі умови для безперешкодного та ефективного функціонування ENISA. Для належного та ефективного виконання своїх завдань, для добору та утримання персоналу та для посилення ефективності роботи з побудови зв’язків украй важливо, щоб ENISA базувалося в належному місці розташування, яке поміж іншого має добре транспортне сполучення та засоби для розміщення членів подружжя та дітей, що супроводжують членів персоналу ENISA. Тому в угоді між ENISA та державою-членом ведення діяльності, після отримання згоди Правління ENISA, повинно бути визначено відповідні домовленості.

(19) Зважаючи на подальше зростання ризиків і проблем, пов’язаних із кібербезпекою, з якими стикається Союз, існує потреба у збільшенні фінансових та людських ресурсів, виділених ENISA, у відповідь на посилення його ролі та розширення його завдання, та з огляду на його критичне становище в екосистемі організацій, що захищають цифрову екосистему Союзу, та для надання ENISA змоги ефективно виконувати завдання, покладені на нього цим Регламентом.

(20) ENISA повинне нарощувати експертні знання та підтримувати їх рівень, а також функціонувати як довідковий центр, і тим самим утверджувати довіру і впевненість у єдиному ринку завдяки своїй незалежності, якості пропонованих консультацій, якості розповсюджуваної інформації, прозорості своїх процедур, прозорості своїх методів ведення діяльності та ретельності у виконанні своїх завдань. ENISA повинне активно підтримувати національні зусилля та проактивно долучатися до зусиль Союзу з одночасним виконанням своїх завдань у повній співпраці з установами, органами, офісами та агентствами Союзу та з державами-членами, з уникненням дублювання роботи та з просуванням синергії зусиль. На додаток, ENISA повинне будувати свою роботу на основі взаємодії і співпраці з приватним сектором та іншими відповідними заінтересованими сторонами. Для ENISA повинно бути визначено низку завдань, виконанням яких воно повинне досягати своїх цілей, проте з наданням достатньої гнучкості у веденні його діяльності.

(21) Щоб мати змогу надавати адекватну підтримку для операційної співпраці між державами-членами, ENISA повинне додатково посилювати свій технічний та людський потенціал, а також навички персоналу. ENISA повинне нарощувати свої ноу-хау та інші спроможності. ENISA та держави-члени на добровільній основі можуть розробляти програми відкомандирування національних експертів до ENISA, створення пулів експертів та здійснення обмінів персоналу.

(22) ENISA повинне допомагати Комісії шляхом надання консультацій, висновків та аналізів стосовно всіх питань Союзу, що стосуються розробки, оновлення та перегляду політики й законодавства у сфері кібербезпеки та з окремих її секторальних питань для посилення актуальності політик і законів Союзу в розрізі виміру кібербезпеки та для забезпечення послідовності у застосуванні таких політик і законів на національному рівні. ENISA повинне діяти як довідковий центр для консультацій та надання експертних знань для ініціатив щодо секторальної політики та законодавства, пов'язаних із питаннями кібербезпеки. ENISA повинне регулярно інформувати Європейський Парламент про свою діяльність.

(23) Публічне ядро відкритого Інтернету, зокрема його основні протоколи та інфраструктура, які є глобальним публічним благом, забезпечує основні функціональні можливості Інтернету в цілому та підтримує його нормальне функціонування. ENISA повинне підтримувати безпеку публічного ядра відкритого Інтернету та стабільність його функціонування, що включає, зокрема, ключові протоколи (серед яких DNS, BGP, та IPv6), функціонування системи доменних імен (серед іншого і функціонування всіх доменів вищого рівня) та функціонування кореневої зони.

(24) Засадничим завданням ENISA є просування послідовного застосування актуальної нормативно-правової бази, зокрема через дієву імплементацію Директиви (ЄС) 2016/1148 та інших відповідних правових інструментів, які стосуються аспектів кібербезпеки, що є важливими для підвищення кіберстійкості. У світлі швидкоплинної зміни ландшафту кіберзагроз чітко зрозуміло, що держави-члени потребують більш комплексної та крос-політичної підтримки у розбудові кіберстійкості.

(25) ENISA повинне допомагати державам-членам та установам, органам, офісам та агентствам Союзу в їхніх зусиллях із побудови та посилення спроможностей і готовності попереджати, виявляти й відбивати кіберзагрози та інциденти, пов'язані з безпекою мережевих та інформаційних систем. Зокрема, ENISA повинне підтримувати формування та посилення груп для реагування на інциденти у сфері комп'ютерної безпеки (CSIRT), передбачених у Директиві (ЄС) 2016/1148, як на національному рівні, так і на рівні Союзу, щоб сприяти досягненню вищого загального рівня їхньої професійної компетенції в Союзі. Діяльність, яку ENISA провадить стосовно операційної спроможності держав-членів, повинна бути спрямована на активну підтримку заходів, яких держави-члени вживають на виконання ними своїх обов'язків за Директивою (ЄС) 2016/1148, а тому така діяльність не повинна стати заміною таких заходів.

(26) ENISA повинне також допомагати в розробці й оновленні стратегій з безпеки мережевих та інформаційних систем на рівні Союзу та, за запитом, на рівні держави-члена, зокрема, з питань кібербезпеки, та повинне сприяти розповсюдженню таких стратегій, а також відстежувати прогрес у їх виконанні. ENISA повинне також сприяти покриттю потреб у підготовці та в навчальних матеріалах, включно з потребами публічних органів, та у відповідних випадках також і стосовно навчання тренерів, на основі Рамки цифрових компетенцій для громадян, щоб допомагати державам-членам та установам, органам, офісам та агентствам Союзу в нарощуванні їхніх власних спроможностей з підготовки.

(27) ENISA повинне надавати підтримку державам-членам у підвищенні рівня обізнаності та освіти з питань кібербезпеки шляхом сприяння тіснішій координації та обміну найкращими практиками між державами-членами. Така підтримка може полягати в розвитку мережі національних освітніх контактних пунктів та розробці навчальної платформи з кібербезпеки. Мережа національних освітніх контактних пунктів може працювати в рамках Мережі національних зв'язкових офіцерів та може стати відправною точкою для майбутньої співпраці між державами-членами.

(28) ENISA повинне допомагати Групі співпраці, створеній згідно з Директивою (ЄС) 2016/1148, на

виконання її завдань, зокрема, шляхом надання експертних знань, консультацій та шляхом сприяння обміну найкращими практиками, між іншим, стосовно ідентифікації операторів основних послуг державами-членами, а також стосовно транскордонних залежностей у зв'язку з ризиками та інцидентами.

(29) Для стимулювання співпраці між публічним і приватним секторами та в межах приватного сектора, зокрема для підтримки захисту критичних інфраструктур, ENISA повинне підтримувати обмін інформацією між секторами, зокрема між секторами, наведеними у додатку II до Директиви (ЄС) 2016/1148, шляхом надання найкращих практик та настанов щодо наявних інструментів та процедур, а також шляхом надання вказівок щодо того, як вирішувати регулятивні питання стосовно обміну інформацією, наприклад, через сприяння у створенні секторальних аналітично-інформаційних центрів.

(30) Через постійне зростання потенційного негативного впливу від вразливостей у продуктах ІКТ, послугах ІКТ та процесах ІКТ, пошук та реагування на такі вразливості відіграє важливу роль у загальному зменшенні ризиків кібербезпеки. Співпраця між організаціями, виробниками або надавачами вразливих продуктів ІКТ, послуг ІКТ та процесів ІКТ та членами співтовариства досліджень у сфері кібербезпеки та урядовими органами, які знаходять вразливості, показала позитивний приклад значного зростання як випадків виявлення вразливостей, так і належного реагування на вразливості у продуктах ІКТ, послугах ІКТ та процесах ІКТ. Скоординоване виявлення вразливостей повинно бути структурованим процесом співпраці, під час якого про вразливості повідомляють власнику інформаційної системи, що дає змогу організації проводити діагностику та усувати вразливості до розкриття докладної інформації про вразливості третім сторонам або громадськості. Такий процес також повинен передбачати координацію між особою, яка ідентифікувала вразливості, та організацією, якій вона про них повідомляє, стосовно публікації таких вразливостей. Скоординовані політики розкриття інформації про загрози можуть відігравати важливу роль у комплексі зусиль держав-членів з посилення кібербезпеки.

(31) ENISA повинне збирати та аналізувати інформацію з національних звітів, які надають CSIRT та міжінституційні групи з реагування на надзвичайні ситуації в комп'ютерній сфері для установ, органів та агентств Союзу, створені згідно з Угодою між Європейським Парламентом, Європейською Радою, Радою Європейського Союзу, Європейською Комісією, Судом Європейського Союзу, Європейським Центральним Банком, Європейською Рахунковою Палатою, Європейською службою зовнішніх справ, Європейським економічно-соціальним комітетом, Європейським комітетом регіонів та Європейським інвестиційним банком стосовно організації та функціонування групи з реагування на надзвичайні ситуації в комп'ютерній сфері для установ, органів та агентств Союзу (CERT-EU) ([14]), з метою сприяння запровадженню спільних процедур, мови та термінології для обміну інформацією. У цьому контексті ENISA повинне включати приватний сектор у розумінні Директиви (ЄС) 2016/1148, якою закладено основи для добровільного обміну технічною інформацією на операційному рівні у мережі груп для реагування на інциденти в сфері комп'ютерної безпеки (CSIRT), створеної зазначеною Директивою.

(32) ENISA повинне сприяти реагуванню на рівні Союзу на випадки широкомасштабних транскордонних інцидентів та криз, пов'язаних із кібербезпекою. Зазначене завдання належить виконувати в рамках мандата ENISA згідно з цим Регламентом, і загальний підхід повинен узгоджуватися з державами-членами у контексті Рекомендації Комісії (ЄС) 2017/1584 ([15]) та висновків Ради від 26 червня 2018 року про скоординоване реагування з боку ЄС на широкомасштабні інциденти та кризи, пов'язані з кібербезпекою. Зазначене завдання може включати збір потрібної інформації та дії в ролі фасилітатора між мережею CSIRT та технічною спільнотою, а також між виробниками рішень, відповідальними за управління кризами. Крім того, ENISA повинне підтримувати операційну співпрацю між державами-членами на запит однієї чи більше держав-членів щодо технічного опрацювання інцидентів шляхом сприяння обміну технічними рішеннями між державами-членами та шляхом проведення публічних комунікаційних

кампаній. ENISA повинне підтримувати операційну співпрацю шляхом відпрацювання механізмів для такої співпраці через регулярні навчально-тренувальні заходи у сфері кібербезпеки.

(33) При підтримці операційної співпраці ENISA повинне користуватися доступними технічними та операційними експертними знаннями CERT-EU шляхом застосування структурованої співпраці. Така структурована співпраця може ґрунтуватися на експертних знаннях ENISA. У відповідних випадках, між двома організаціями повинно бути укладено спеціальні угоди з визначенням практичних інструментів для такої співпраці та для уникнення дублювання роботи.

(34) При виконанні свого завдання щодо підтримки операційної співпраці у межах мережі CSIRT у ENISA повинна бути змога надавати підтримку державам-членам, за їхнім запитом, зокрема щодо надання консультацій стосовно вдосконалення їхньої спроможності запобігати інцидентам, виявляти їх та реагувати на них, шляхом сприяння у технічному опрацюванні інцидентів, що мають значний або суттєвий негативний вплив, або шляхом забезпечення аналізу кіберзагроз та інцидентів. ENISA повинне сприяти технічному опрацюванню інцидентів, що мають значний або суттєвий негативний вплив, зокрема шляхом підтримки добровільного обміну технічними рішеннями між державами-членами або шляхом підготовки зведеної технічної інформації, як-от щодо технічних рішень, обмін якими здійснили держави-члени на добровільних засадах. У Рекомендації (ЄС) 2017/1584 державам-членам рекомендовано співпрацювати добросовісно та без невиправданої затримки обмінюватися між собою та ENISA інформацією стосовно широкомасштабних інцидентів та криз, пов'язаних із кібербезпекою. Така інформація також допоможе ENISA при виконанні ним свого завдання з підтримки операційної співпраці.

(35) Як частину звичайної співпраці на технічному рівні на підтримку ситуаційної обізнаності в Союзі у тісній співпраці з державами-членами, ENISA повинне регулярно готувати детальний технічний звіт ЄС про стан кібербезпеки стосовно інцидентів та кібератак на основі доступної для громадськості інформації, власного аналізу та звітів, наданих йому командами CSIRT держав-членів або єдиними контактними пунктами з безпеки мережевих та інформаційних систем («єдині контактні пункти»), створеними відповідно до Директиви (ЄС) 2016/1148, в обох випадках на добровільній основі, Європейським центром кіберзлочинності (ЕС3) у Європолі, CERT-EU та, у відповідних випадках, Розвідувально-ситуаційним центром Європейського Союзу (EU INTCEN) при Європейській службі зовнішніх справ. Такий звіт повинен надаватися Раді, Комісії, Високому представнику Союзу з питань закордонних справ і політики безпеки та мережі CSIRT.

(36) Підтримку ENISA щодо технічних запитів *ex-post*, поданих заінтересованими державами-членами стосовно інцидентів, які мають значний вплив або суттєвий негативний вплив, повинно бути зосереджено на запобіганні майбутнім інцидентам. Заінтересовані держави-члени повинні надавати необхідну інформацію та допомогу, щоб ENISA мало змогу забезпечити ефективну підтримку щодо технічних запитів *ex-post*.

(37) Держави-члени можуть запрошувати підприємства, яких торкнувся інцидент, до співпраці шляхом надання необхідної інформації та допомоги ENISA без обмеження їхнього права захищати комерційно чутливу інформацію, а також надання інформації, що є важливою для громадської безпеки.

(38) Щоб краще розуміти проблеми у сфері кібербезпеки, та з наміром надання державам-членам та установам, органам, офісам та агентствам Союзу стратегічних консультацій з урахуванням майбутніх перспектив, ENISA потрібно здійснювати аналіз наявних та новітніх ризиків кібербезпеки. З цією метою ENISA повинне у співпраці з державами-членами та, у відповідних випадках, із органами статистики та іншими органами збирати відповідні доступні публічно та надані добровільно дані й інформацію та здійснювати аналіз новітніх технологій та проводити тематичні оцінювання очікуваного соціального, правового, економічного та регуляторного впливу технологічних інновацій на мережеву та інформаційну безпеку та, зокрема, на кібербезпеку. Крім того, ENISA повинне підтримувати держави-члени та установи, органи, офіси та агентства Союзу у виявленні новітніх ризиків кібербезпеки та попередженні інцидентів шляхом проведення аналізу кіберзагроз, вразливостей та інцидентів.

(39) Для підвищення стійкості Союзу, ENISA необхідно накопичити експертні знання у сфері кібербезпеки інфраструктур, зокрема, для підтримки секторів, перелічених у додатку II до Директиви (ЄС) 2016/1148, та секторів, що використовуються надавачами цифрових послуг, переліченими в додатку III до зазначеної Директиви, шляхом надання консультацій, підготовки настанов та обміну найкращими практиками. З метою забезпечення легшого доступу до краще структурованої інформації про ризики кібербезпеки та можливі засоби їх подолання ENISA необхідно розробити та підтримувати актуальність «інформаційного хабу» Союзу, єдиного порталу, що надаватиме громадськості інформацію про питання кібербезпеки, яка надходитиме від Союзу та національних установ, органів, офісів та агентств. Сприяння доступності краще структурованої інформації про ризики кібербезпеки та можливі засоби їх подолання може також допомогти державам-членам у посиленні їхньої спроможності та узгодженні їхніх практик, і в такий спосіб сприятиме підвищенню їхньої загальної стійкості до кібератак.

(40) ENISA необхідно сприяти підвищенню обізнаності громадськості про ризики кібербезпеки, у тому числі через кампанії з підвищення обізнаності по всьому ЄС шляхом просування освіти, та забезпечити надання настанов щодо належних практик для окремих користувачів, орієнтованих на громадян, організації та підприємства. ENISA потрібно також сприяти просуванню найкращих практик та рішень, у тому числі щодо кібергігієни та кіберграмотності на рівні громадян, організацій та підприємств, шляхом збору та аналізу публічно доступної інформації про значні інциденти, та шляхом складання й публікації звітів і настанов для громадян, організацій та підприємств, щоб підвищити їхній і загальний рівень готовності та стійкості. ENISA потрібно також намагатися надавати споживачам актуальну інформацію про застосовні схеми сертифікації, наприклад, шляхом підготовки настанов та рекомендацій. Крім того, ENISA потрібно організовувати згідно з Планом заходів із цифрової просвіти, схваленим Повідомленням Комісії від 17 січня 2018 року, у співпраці з державами-членами та установами, органами, офісами та агентствами Союзу регулярні кампанії з популяризації та просвіти, спрямовані на кінцевих користувачів, з метою просування більш безпечної онлайнової поведінки фізичних осіб та їхньої цифрової грамотності, для підвищення обізнаності про потенційні кіберзагрози, у тому числі про онлайнову кримінальну діяльність, як от фішингові атаки, мережі ботів, фінансове та банківське шахрайство, інциденти шахрайства з даними, а також рекламувати важливість базової багатофакторної автентифікації, встановлення оновлень та латок, шифрування, анонімізації та порад із захисту даних.

(41) ENISA необхідно відігравати центральну роль в активізації зусиль з підвищення обізнаності кінцевих користувачів щодо питань безпеки пристроїв та безпечного використання послуг; також ENISA повинне просувати ширше застосування концепцій вбудованої безпеки та вбудованої конфіденційності на рівні Союзу. У переслідуванні цієї цілі ENISA необхідно використовувати доступні найкращі практики та досвід, особливо найкращі практики та досвід академічних установ та дослідників сфери безпеки ІТ.

(42) Для підтримки підприємств, що здійснюють діяльність у секторі кібербезпеки, а також користувачів кібербезпекових рішень, ENISA необхідно розробити та підтримувати актуальність «ринкової обсерваторії» шляхом регулярного аналізу та розповсюдження інформації про основні тенденції на ринку кібербезпеки, як з боку попиту, так і з боку пропозиції.

(43) ENISA необхідно допомагати в зусиллях Союзу щодо співпраці з міжнародними організаціями, а також у рамках відповідної міжнародної співпраці у сфері кібербезпеки. Зокрема, ENISA необхідно сприяти, у відповідних випадках, співпраці з такими організаціями, як ОЕСР, ОБСЄ та НАТО. Така співпраця може включати спільні навчально-тренувальні заходи з кібербезпеки та спільну координацію реагування на інциденти. Такі заходи повинні здійснюватися в повній відповідності з принципами інклюзивності, взаємності та автономності Союзу у виробленні й ухваленні рішень, без обмеження специфічного характеру безпекової та оборонної політики будь-якої держави-члена.

(44) Для забезпечення повного досягнення своїх цілей ENISA необхідно встановити та підтримувати зв’язок із відповідними наглядовими органами Союзу та з іншими компетентними органами в

Союзі, установами, органами, офісами та агентствами Союзу, серед яких CERT-EU, EC3, Європейське оборонне агентство (EDA), Європейське агентство з питань глобальних навігаційних супутникових систем (Європейське агентство GNSS), Орган європейських регуляторів електронних комунікацій (BEREC), Європейське агентство з оперативного управління великомасштабними IT-системами у просторі свободи, безпеки та правосуддя (eu-LISA), Європейський Центральний Банк (ЄЦБ), Європейський орган банківського нагляду, Агентство з питань співпраці регуляторних органів у сфері енергетики (ACER), Агентство з безпеки польотів Європейського Союзу (EASA), а також із будь-якими іншими агентствами Союзу, пов'язаними з кібербезпекою. ENISA необхідно також встановити та підтримувати зв'язок з органами, які займаються захистом даних, для обміну ноу-хау та найкращими практиками, а також необхідно надавати консультації з питань кібербезпеки, що можуть мати вплив на їхню роботу. Представники органів правозастосування та захисту даних Союзу та держав-членів повинні мати змогу бути представленими в Консультативній групі ENISA. Співпрацюючи з правозастосовчими органами стосовно питань безпеки мережевих та інформаційних систем, що можуть впливати на їхню роботу, ENISA потрібно враховувати наявні канали інформації та створені мережі.

(45) Можуть встановлюватися партнерства з академічними установами, що мають дослідний потенціал у відповідних сферах, та повинні бути створені відповідні канали для отримання думок від організацій споживачів та інших організацій, які потрібно брати до уваги.

(46) ENISA, виконуючи роль секретаріату мережі CSIRT, повинне підтримувати CSIRT держав-членів та CERT-EU у здійсненні операційної співпраці стосовно відповідних завдань мережі CSIRT, як зазначено в Директиві (ЄС) 2016/1148. Крім того, ENISA повинне просувати та підтримувати співпрацю між відповідними CSIRT у разі інцидентів, атак або порушень у мережах чи інфраструктурі, управління та захист яких здійснюється CSIRT, та залучати або бути здатним залучати принаймні два CSIRT із належним урахування стандартних операційних процедур мережі CSIRT.

(47) Для підвищення готовності Союзу реагувати на інциденти, ENISA потрібно регулярно організовувати кібербезпекові навчально-тренувальні заходи на рівні Союзу та, за запитом держав членів, надавати державам-членам та установам, органам, офісам та агентствам Союзу допомогу в організації таких навчально-тренувальних заходів. Широкомасштабні комплексні навчально-тренувальні заходи, що включають технічні, операційні або стратегічні елементи, необхідно організовувати кожні два роки. Крім того, ENISA потрібно мати змогу регулярно організовувати менш комплексні навчально-тренувальні заходи з тією самою ціллю для підвищення готовності Союзу реагувати на інциденти.

(48) ENISA необхідно продовжувати нарощувати та підтримувати рівень власних експертних знань щодо сертифікації кібербезпеки з метою підтримки політики Союзу в зазначеній сфері. ENISA повинне ґрунтувати свою діяльність на наявних найкращих практиках та повинне просувати розвиток сертифікації кібербезпеки у межах Союзу, у тому числі шляхом сприяння запровадженню та використанню рамок сертифікації кібербезпеки на рівні Союзу (європейських рамок сертифікації кібербезпеки) з метою підвищення прозорості кібербезпеки продуктів ІКТ, послуг ІКТ, процесів ІКТ, внаслідок чого відбуватиметься посилення рівня впевненості в цифровому внутрішньому ринку та його конкурентоспроможності.

(49) Необхідно, щоб дієві політики у сфері кібербезпеки ґрунтувалися на добре розроблених методах оцінювання ризиків як у публічному, так і в приватному секторах. Методи оцінювання ризиків використовуються на різних рівнях, і щодо їх ефективного застосування не існує загальної практики. Підтримка та розробка найкращих практик для оцінювання ризиків та рішень щодо взаємодійного управління ризиками в організаціях публічного та приватного секторів підвищить рівень кібербезпеки у Союзі. З цією метою ENISA необхідно підтримувати співпрацю між заінтересованими сторонами на рівні Союзу та сприяти їх зусиллям щодо запровадження та розвитку європейських та міжнародних стандартів управління ризиками та вимірюваної безпеки

електронних продуктів, систем, мереж та послуг, які в сукупності з програмним забезпечення становлять собою мережеві та інформаційні системи.

(50) ENISA необхідно заохочувати держави-члени, виробників або надавачів продуктів ІКТ, послуг ІКТ або процесів ІКТ з метою підвищення їхніх загальних стандартів безпеки у такий спосіб, щоб усі користувачі інтернету могли вжити необхідних заходів для забезпечення їхньої особистої кібербезпеки, та необхідно передбачити для них відповідні стимули це робити. Зокрема, виробники та надавачі продуктів ІКТ, послуг ІКТ або процесів ІКТ повинні передбачити будь-які необхідні оновлення та повинні відкликати, вилучати або утилізовувати продукти ІКТ, послуги ІКТ або процеси ІКТ, які не відповідають стандартам кібербезпеки, тоді як імпортери та розповсюджувачі повинні забезпечити, щоб продукти ІКТ, послуги ІКТ та процеси ІКТ, які вони вводять в обіг на ринку Союзу, відповідали застосовним вимогам та не становили ризику для споживачів Союзу.

(51) У співпраці з компетентними органами ENISA повинне бути здатним розповсюджувати інформацію стосовно рівня кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ, що пропонуються на внутрішньому ринку, та повинне видавати попередження виробникам або надавачам продуктів ІКТ, послуг ІКТ або процесів ІКТ та вимагати від них їх підвищувати безпеку їхніх продуктів ІКТ, послуг ІКТ та процесів ІКТ, включно з кібербезпекою.

(52) ENISA необхідно брати до уваги поточні дослідження, розробки й технологічні оцінки, зокрема стосовно тих видів діяльності, що здійснюються в рамках різних дослідних ініціатив Союзу, з метою консультування установ, органів, офісів та агентств Союзу та держав-членів, у відповідних випадках на їхній запит, стосовно потреб і пріоритетів для досліджень у сфері кібербезпеки. З питань ідентифікації потреб і пріоритетів для досліджень, ENISA потрібно також консультуватися з відповідними групами користувачів. Більш конкретно, може бути встановлена співпраця з Європейською дослідницькою радою, Європейським інститутом інновацій та технологій та Інститутом досліджень з питань безпеки Європейського Союзу.

(53) Під час підготовки європейських схем сертифікації кібербезпеки ENISA необхідно регулярно консультувати організації стандартизації, зокрема європейські організації стандартизації.

(54) Кіберзагрози є проблемним питанням глобального виміру. Існує потреба у тіснішій співпраці для вдосконалення стандартів кібербезпеки, у тому числі потреба у визначенні спільних норм поведінки, ухваленні кодексів поведінки, використанні міжнародних стандартів, а також в обміні інформацією, сприянні активнішій міжнародній співпраці у відповідь на проблеми з безпеки мережевих та інформаційних систем та сприянні спільному глобальному підходу до таких питань. З цією метою ENISA необхідно підтримувати дедалі активніше залучення Союзу та співпрацю з третіми країнами та міжнародними організаціями шляхом надання необхідних експертних знань і аналізу відповідним установам, органам, офісам та агентствам Союзу, у відповідних випадках.

(55) ENISA повинне бути здатним реагувати на спеціальні запити щодо надання консультацій та підтримки державам-членам та установам, органам, офісам та агентствам Союзу з питань, що належать до сфери повноважень ENISA.

(56) Чутливим і рекомендованим питанням є впровадження певних принципів врядування ENISA, спрямованих на виконання Спільної заяви та Спільного підходу, погодженого в липні 2012 року Міжінституційною робочою групою з питань децентралізованих агентств ЄС, метою яких є активізація діяльності децентралізованих агентств та вдосконалення їхньої продуктивності. Рекомендації, наведені у Спільній заяві та у Спільному підході, повинні бути відображені, якщо доцільно, у робочих програмах ENISA, оцінках ENISA та звітності й адміністративній співпраці ENISA.

(57) Правління у складі представників держав-членів та Комісії повинне визначати загальні напрямки роботи ENISA та виконувати свої завдання відповідно до положень цього Регламенту. На Правління необхідно покласти повноваження, необхідні для визначення і схвалення бюджету, перевірки виконання бюджету, ухвалення належних фінансових правил, визначення прозорих робочих процедур для вироблення та ухвалення рішень ENISA, ухвалювати єдиний програмний документ

ENISA, ухвалювати власний внутрішній регламент, призначати виконавчого директора та ухвалювати рішення про продовження або припинення строку перебування на посаді виконавчого директора.

(58) Для забезпечення належного і дієвого функціонування ENISA, Комісія та держави члени повинні призначати у Правління лише осіб із професійними експертними знаннями та досвідом. Комісія та держави-члени повинні докладати зусиль для забезпечення того, щоб їхні відповідні представники у Правлінні змінювалися якомога рідше, для забезпечення безперервності його роботи.

(59) Безперебійне функціонування ENISA вимагає призначення його виконавчого директора, виходячи з його заслуг та документально підтверджених адміністративних та управлінських навичок, а також компетенції та досвіду, пов'язаних із кібербезпекою. Виконавчий директор повинен виконувати свої обов'язки повністю незалежно. Виконавчий директор повинен готувати проєкт річної робочої програми ENISA після проведення консультацій із Комісією, та повинен вживати усіх заходів, необхідних для забезпечення належного виконання згаданої робочої програми. Виконавчий директор повинен готувати щорічний звіт для подання Правлінню, і такий звіт повинен стосуватися виконання річної робочої програми ENISA, містити проєкт кошторису доходів і видатків ENISA, а також містити інформацію про виконання бюджету. Крім того, у виконавчого директора повинна бути можливість створювати спеціалізовані експертні робочі групи для розв'язання специфічних питань, зокрема наукового, правового або соціоекономічного характеру. Серед іншого необхідно, щоб він міг створити спеціалізовану експертну робочу групу для підготовки проєкту європейської схеми сертифікації кібербезпеки («проєкт схеми»). Виконавчий директор повинен забезпечувати, щоб членів спеціалізованих експертних робочих груп добирали відповідно до найвищих стандартів щодо рівня експертних знань, із забезпеченням гендерного балансу та належного представництва публічних адміністрацій держав-членів, установ, органів, офісів та агентств Союзу та приватного сектора, включно з промисловістю, користувачами та академічними експертами з питань безпеки мереж та інформації, щодо спеціалізованих питань до розгляду.

(60) Виконавча рада повинна сприяти ефективному функціонуванню Правління. У рамках роботи з підготовки рішень Правління Виконавча рада повинна детально досліджувати відповідну інформацію, вивчати доступні варіанти та надавати поради і пропозиції з підготовки рішень Правління.

(61) ENISA повинне використовувати Консультативну групу ENISA як дорадчий орган, щоб забезпечити підтримку постійного діалогу з приватним сектором, організаціями споживачів та іншими відповідними заінтересованими сторонами. Консультативну групу ENISA створює Правління за пропозицією виконавчого директора, і вона повинна зосередити свою увагу на питаннях, піднятих заінтересованими сторонами, та повинна доносити їх до уваги ENISA. Консультативна група ENISA повинна надавати консультації, зокрема, у рамках підготовки проєкту робочої програми ENISA. Склад Консультативної групи ENISA та покладені на неї завдання повинні бути достатніми для забезпечення представництва заінтересованих сторін у роботі ENISA.

(62) Для допомоги ENISA та Комісії у сприянні проведенню консультацій з відповідними заінтересованими сторонами повинна бути створена Група стейкхолдерів з питань сертифікації кібербезпеки. Група стейкхолдерів з питань сертифікації кібербезпеки повинна складатися з членів, що збалансовано представляють галузь з боку і попиту, і пропозиції продуктів ІКТ та послуг ІКТ, та повинна включати, зокрема, МСП, надавачів цифрових послуг, європейські та міжнародні органи стандартизації, національні органи з акредитації, наглядові органи з питань захисту даних та органи з оцінювання відповідності відповідно до Регламенту Європейського Парламенту і Ради (ЄС) № 765/2008 ([16]), а також представників академічної спільноти та організацій споживачів.

(63) В ENISA повинно бути запроваджено правила щодо управління конфліктами інтересів та запобігання таким конфліктам інтересів. ENISA також необхідно застосовувати відповідні положення Союзу стосовно публічного доступу до документів, як визначено у Регламенті Європейського Парламенту і Ради (ЄС) № 1049/2001 ([17]). Опрацювання персональних даних в

ENISA необхідно здійснювати відповідно до положень Регламенту Європейського Парламенту і Ради (ЄС) 2018/1725 ([18]). ENISA необхідно забезпечити дотримання положень, що застосовуються до установ, органів, офісів та агентств Союзу, а також положень національного законодавства стосовно опрацювання інформації, зокрема чутливої незасекреченої інформації та секретної інформації Європейського Союзу (EUCI).

(64) Щоб гарантувати повну автономію та незалежність ENISA, та щоб дати змогу ENISA виконувати додаткові завдання, включно з непередбаченими невідкладними завданнями, ENISA необхідно надати достатній та автономний бюджет, надходження до якого повинні формуватися з внесків Союзу та внесків третіх країн, які беруть участь у роботі ENISA. Для забезпечення достатньої спроможності виконувати всі покладені на нього завдання та для досягнення поставлених перед ним цілей, ENISA повинне мати належний бюджет. Більшість персоналу ENISA повинна бути прямо задіяна в операційній реалізації мандату ENISA. Державі-члену ведення діяльності та будь-якій іншій державі-члену повинно бути дозволено здійснювати добровільні внески до бюджету ENISA. Необхідно застосовувати бюджетну процедуру Союзу, якщо йдеться про дотації, які надаються за рахунок загального бюджету Союзу. Крім того, для забезпечення прозорості та підзвітності звітність ENISA повинна проходити аудит з боку Рахункової палати.

(65) Сертифікація кібербезпеки відіграє важливу роль у підвищенні довіри до продуктів ІКТ, послуг ІКТ та процесів ІКТ, а також їхньої безпеки. Єдиний цифровий ринок та, зокрема, економіка даних та інтернет речей можуть процвітати лише за умови, що існуватиме довіра з боку загальної громадськості до таких продуктів, послуг та процесів, і що вони здатні забезпечити певний рівень кібербезпеки. Автомобілі, електронні медичні вироби, системи контролю промислової автоматизації та розумні електросистеми з постійним під’єднанням до мережі інтернет та з функціями автоматизованого функціонування — лише деякі з прикладів секторів, у яких сертифікація вже набула широкого використання або набуде в найближчій перспективі. Сектори, що регулюються положеннями Директиви (ЄС) 2016/1148, також належать до секторів, у яких сертифікація кібербезпеки є критичною.

(66) У Повідомленні «Посилення кіберстійкості систем Європи та сприяння побудові конкурентної та інноваційної галузі кібербезпеки» від 2016 року Комісія відзначила потребу у високоякісних, доступних та взаємодійних продуктах і рішеннях у сфері кібербезпеки. У наданні продуктів ІКТ, послуг ІКТ та процесів ІКТ у межах єдиного ринку спостерігається значна географічна фрагментованість. Причина цього полягає в тому, що галузь кібербезпеки переважно розвивалася на основі попиту з боку національних урядів. На додаток, відсутність взаємодійних рішень (технічних стандартів), практик та загальноєвропейських механізмів сертифікації формує прогалини на єдиному ринку у сфері кібербезпеки. Це ускладнює конкурентоспроможність європейських підприємств на національному, загальноєвропейському та світовому рівнях. Це також скорочує вибір доступних для фізичних осіб та підприємств технологій кібербезпеки. Аналогічним чином, у Повідомленні 2017 року про середньостроковий огляд впровадження Стратегії розбудови Єдиного цифрового ринку «Конективний Єдиний цифровий ринок для всіх» Комісія відзначала потребу в безпечних конективних продуктах і системах, та зазначала, що створення європейських рамок безпеки ІКТ дасть змогу визначити правила організації процесу сертифікації безпеки ІКТ в Союзі, що своєю чергою посилить довіру до інтернету та подолає поточну фрагментарність внутрішнього ринку.

(67) На поточний момент, сертифікація кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ носить обмежений характер. Вона існує переважно на рівні держав-членів або у рамках схем, створених самою галуззю. За такого контексту, як правило, сертифікат, виданий національним органом сертифікації кібербезпеки, не визнається в іншій державі-члені. Як наслідок, компанії мусять сертифікувати свої продукти ІКТ, послуги ІКТ та процеси ІКТ в кількох державах-членах, у яких вони здійснюють діяльність, наприклад, у рамках національних закупівельних процедур, що призводить до підвищення їхніх витрат. Крім того, з появою нових схем дедалі більше спостерігається відсутність узгодженого та комплексного підходу до горизонтальних аспектів

кібербезпеки, наприклад, у сфері інтернету речей. Наявні схеми мають значні недоліки та відмінності в частині охопленні продуктів, рівнів надійності, сутнісних критеріїв та фактичного використання, що унеможливлює застосування механізмів взаємного визнання в рамках Союзу.

(68) Було докладено зусиль для забезпечення взаємного визнання сертифікатів у межах Союзу. Однак ці зусилля виявилися успішними тільки частково. Найважливішим прикладом у цьому зв'язку є Угода про взаємне визнання (MRA) Групи вищих посадових осіб з безпеки інформаційних систем (SOG-IS). Незважаючи на те, що цей документ є найважливішим зразком співпраці та взаємного визнання у сфері сертифікації безпеки, SOG-IS охоплює тільки деякі держави-члени. З цієї причини MRA SOG-IS має обмежену дієвість з точки зору внутрішнього ринку.

(69) Таким чином, необхідно утвердити спільний підхід та запровадити європейську схему сертифікації кібербезпеки, що закладе основні горизонтальні вимоги для майбутніх європейських схем сертифікації кібербезпеки та забезпечить визнання і використання в усіх державах-членах європейських сертифікатів з кібербезпеки та декларацій ЄС про відповідність для продуктів ІКТ, послуг ІКТ або процесів ІКТ. На цьому шляху важливо спиратися на наявні національні та міжнародні схеми, а також на системи взаємного визнання, серед яких SOG-IS; крім того, необхідно забезпечити плавний перехід від наявних схем у рамках таких систем до схем відповідно до нових європейських рамок сертифікації кібербезпеки. Європейські рамки сертифікації кібербезпеки повинні слугувати подвійній меті. По-перше, вони повинні сприяти підвищенню довіри до продуктів ІКТ, послуг ІКТ та процесів ІКТ, які були сертифіковані за європейськими схемами сертифікації кібербезпеки. По-друге, вони повинні сприяти зникненню численних суперечливих або дубльованих національних схем сертифікації кібербезпеки, що дасть змогу скоротити витрати підприємств, які ведуть діяльність на єдиному цифровому ринку. Європейські схеми сертифікації кібербезпеки повинні носити недискримінаційний характер та ґрунтуватися на європейських або міжнародних стандартах, крім випадків, коли такі стандарти довели свою неефективність або невідповідність у досягненні законних цілей Союзу стосовно питань сертифікації кібербезпеки.

(70) Європейські рамки сертифікації кібербезпеки повинні бути створені як єдиний інструмент для всіх держав-членів, щоб запобігти появі «торгівлі сертифікацією» внаслідок різних рівнів суворості у рівних державах-членах.

(71) Європейські схеми сертифікації кібербезпеки повинні ґрунтуватися на тому, що вже існує на міжнародному та національному рівні, та за необхідності й на технічних специфікаціях від форумів та консорціумів, шляхом вивчення поточних сильних сторін та оцінки й усунення слабин.

(72) Галузі потрібні гнучкі рішення щодо кібербезпеки, щоб випереджати кіберзагрози, тому будь-яка схема сертифікації повинна бути розроблена в такий спосіб, що дає змогу уникнути ризику її швидкого застарівання.

(73) Комісію необхідно наділити повноваженнями ухвалювати європейські схеми сертифікації кібербезпеки для конкретних груп продуктів ІКТ, послуг ІКТ та процесів ІКТ. Національні органи сертифікації кібербезпеки повинні забезпечувати впровадження таких схем та нагляд за ними, і видані згідно з такими схемами сертифікати повинні бути дійсними й визнаватися по всьому Союзу. Схеми сертифікації, які використовуються галуззю або іншими приватними організаціями, не повинні підпадати під сферу дії цього Регламенту. Однак, якщо органи використовують такі схеми, вони повинні мати змогу пропонувати, щоб Комісія брала такі схеми до уваги за основу для схвалення як європейську схему сертифікації кібербезпеки.

(74) Положення цього Регламенту не повинні обмежувати право Союзу стосовно специфічних правил для сертифікації продуктів ІКТ, послуг ІКТ та процесів ІКТ. Зокрема, Регламентом (ЄС) 2016/679 встановлено положення про запровадження механізмів сертифікації захисту даних та штампів і знаків захисту даних з метою підтвердження відповідності операцій опрацювання, які здійснюють контролери і оператори, положенням згаданого Регламенту. Такий механізм сертифікації та штампів і знаків захисту даних повинен давати змогу суб'єктам даних швидко оцінювати рівень захисту даних відповідних продуктів ІКТ, послуг ІКТ та процесів ІКТ. Цей Регламент не обмежує

сертифікації операцій з опрацювання даних згідно з Регламентом (ЄС) 2016/679, у тому числі якщо такі операції вбудовані у продукти ІКТ, послуги ІКТ та процеси ІКТ.

(75) Завданням європейських схем сертифікації кібербезпеки повинно бути забезпечення того, що продукти ІКТ, послуги ІКТ та процеси ІКТ, які сертифіковано за такими схемами, відповідають визначеним вимогам, метою яких є захист доступності, автентичності, цілісності та конфіденційності даних, які зберігають, передають або опрацьовують, або пов'язаних функцій чи послуг, пропонованих такими продуктами, послугами або процесами або доступних із їхньою допомогою протягом їх життєвого циклу. У цьому Регламенті неможливо визначити детальні вимоги до кібербезпеки усіх продуктів ІКТ, послуг ІКТ та процесів ІКТ. Продукти ІКТ, послуги ІКТ та процеси ІКТ та потреби кібербезпеки, пов'язані з такими продуктами, послугами та процесами, настільки різноманітні, що дуже складно розробити загальні вимоги до кібербезпеки, які можливо застосувати за всіх обставин. Тому необхідно ухвалити широке та загальне визначення поняття «кібербезпека» для цілей сертифікації, яке згодом може бути доповнене набором специфічних цілей кібербезпеки, що їх потрібно буде брати до уваги при розробці європейських схем сертифікації кібербезпеки. Відповідні механізми, за допомогою яких буде досягнуто таких цілей у конкретних продуктах ІКТ, послугах ІКТ та процесах ІКТ, в подальшому будуть уточнюватися на рівні окремих схем сертифікації, ухвалених Комісією, наприклад, шляхом покликання на стандарти або технічні специфікації, якщо відповідні стандарти відсутні.

(76) Технічні специфікації, що будуть використовуватися у європейських схемах сертифікації кібербезпеки, повинні враховувати вимоги, визначені в додатку II до Регламенту Європейського Парламенту і Ради (ЄС) № 1025/2012 ([19]). Однак можуть бути необхідними певні відхилення від згаданих вимог у належним чином обґрунтованих випадках, коли такі технічні специфікації будуть використовуватися у європейській схемі сертифікації кібербезпеки стосовно рівня надійності «високий». Причини застосування таких відхилень повинні бути оприлюднені перед громадськістю.

(77) Оцінювання відповідності — це процедура для оцінювання міри відповідності спеціальним вимогам щодо продуктів ІКТ, послуг ІКТ або процесів ІКТ. Така процедура здійснюється незалежною третьою особою, яка не є ані виробником, ані надавачем продуктів ІКТ, послуг ІКТ або процесів ІКТ, які є предметом оцінювання. Після успішного проходження оцінювання продуктів ІКТ, послуг ІКТ або процесів ІКТ повинен видаватися європейський сертифікат з безпеки. Європейський сертифікат з кібербезпеки повинен вважатися підтвердженням того, що оцінювання було проведено належним чином. Залежно від рівня надійності, європейська схема сертифікації кібербезпеки повинна визначати, який орган повинен видати європейський сертифікат з кібербезпеки — приватний чи публічний. Оцінювання відповідності та сертифікація як такі не можуть гарантувати, що продукти ІКТ, послуги ІКТ та процеси ІКТ є кібербезпечними. Вони радше слугують як процедури та технічні методології для підтвердження того, що продукти ІКТ, послуги ІКТ та процеси ІКТ пройшли тестування та що вони відповідають певним вимогам до кібербезпеки, які викладено в інших документах, як, наприклад, у технічних стандартах.

(78) Вибір належної сертифікації та пов'язаних із нею вимог до безпеки з боку користувачів європейських сертифікатів з кібербезпеки повинен ґрунтуватися на аналізі ризиків, пов'язаних з використанням продуктів ІКТ, послуг ІКТ або процесів ІКТ. Відповідно, рівень надійності повинен відповідати рівню ризику, пов'язаному з використанням за призначенням продукту ІКТ, послуги ІКТ або процесу ІКТ.

(79) Європейська схема сертифікації кібербезпеки може передбачати проведення оцінювання відповідності під одноосібну відповідальність виробника або надавача продуктів ІКТ, послуг ІКТ або процесів ІКТ («самооцінювання відповідності»). У таких випадках повинно бути достатньо, щоб виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ самостійно проводив усі перевірки, спрямовані на забезпечення відповідності продуктів ІКТ, послуг ІКТ або процесів ІКТ вимогам європейської схеми сертифікації кібербезпеки. Самооцінювання відповідності повинно вважатися належним для продуктів ІКТ, послуг ІКТ або процесів ІКТ низької складності, що

становлять низький ризик для громадськості, як-от із простим проєктом та технологією виробництва. Крім того, самооцінювання відповідності повинно дозволятися лише у разі, якщо продукти ІКТ, послуги ІКТ та процеси ІКТ відповідають рівню надійності «базовий».

(80) Європейські схеми сертифікації кібербезпеки можуть передбачати існування як самооцінювання відповідності, так і сертифікації продуктів ІКТ, послуг ІКТ або процесів ІКТ. У такому разі схема повинна передбачати чіткі та зрозумілі засоби для споживачів або інших користувачів, які б дозволяли відрізнити продукти ІКТ, послуги ІКТ та процеси ІКТ, за оцінювання яких відповідає виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ, від продуктів ІКТ, послуг ІКТ або процесів ІКТ, які сертифіковані третьою особою.

(81) Виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ, який здійснює самооцінювання відповідності, повинен бути здатним видавати та підписувати декларацію ЄС про відповідність як частину процедури оцінювання відповідності. Декларація ЄС про відповідність — це документ, у якому зазначається, що конкретний продукт ІКТ, послуга ІКТ або процес ІКТ відповідає вимогам європейської схеми сертифікації кібербезпеки. У разі оформлення та підписання декларації ЄС про відповідність виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ повинен брати на себе відповідальність за відповідність продуктів ІКТ, послуг ІКТ або процесів ІКТ правовим вимогам європейської схеми сертифікації кібербезпеки. Копію декларації ЄС про відповідність вимогам необхідно надавати національним органам із сертифікації кібербезпеки та ENISA.

(82) Виробники або надавачі продуктів ІКТ, послуг ІКТ або процесів ІКТ повинні надавати доступ до декларації ЄС про відповідність, технічної документації та іншої відповідної інформації, що стосується відповідності продуктів ІКТ, послуг ІКТ або процесів ІКТ європейській схемі сертифікації кібербезпеки, компетентному національному органу з сертифікації кібербезпеки на період, визначений у відповідній європейській схемі сертифікації кібербезпеки. Технічна документація повинна визначати умови, що застосовуються згідно зі схемою, та повинна охоплювати проєктування, виробництво та експлуатацію продукту ІКТ, послуги ІКТ або процесу ІКТ мірою, якою це необхідно для самооцінювання відповідності. Технічна документація повинна бути складена в такий спосіб, щоб можливо було виконати оцінювання відповідності продукту ІКТ або послуги ІКТ вимогам, що застосовуються згідно з відповідною схемою.

(83) Управління європейськими рамками сертифікації кібербезпеки повинне передбачати залучення держав-членів та належне залучення заінтересованих сторін, а також визначати роль Комісії під час підготовки планів, пропозицій, запитів, проєктів та ухвалення чи перегляду європейських схем сертифікації кібербезпеки.

(84) За підтримки Європейської групи з сертифікації кібербезпеки (ECCG) та Групи стейкхолдерів з питань сертифікації кібербезпеки, а також після відкритих та широких консультацій Комісія повинна підготувати послідовну робочу програму Союзу щодо європейських схем сертифікації кібербезпеки, і опублікувати її у формі необов’язкового інструмента. Послідовна робоча програма Союзу повинна стати стратегічним документом, що дає змогу галузі, національним органам та органам зі стандартизації, зокрема, здійснювати підготовку майбутніх європейських схем сертифікації кібербезпеки заздалегідь. Послідовна робоча програма Союзу повинна включати багаторічний огляд запитів щодо проєктів схем, які комісія має намір подати до ENISA для підготовки на основі конкретних підстав. Комісія повинна враховувати послідовну робочу програму Союзу при підготовці свого Послідовного плану щодо стандартизації ІКТ та запитів на стандартизацію до європейських організацій стандартизації. У світлі швидкого запровадження та розгортання нових технологій, виникнення раніше невідомих ризиків кібербезпеки та законодавчого й ринкового розвитку Комісія або ECCG повинні мати повноваження звертатися до ENISA із запитами про підготовку проєктів схем, які не були включені до послідовної робочої програми Союзу. У таких випадках Комісія та ECCG повинні також оцінювати необхідність таких запитів, враховувати загальні цілі й мету цього Регламенту та потребу в забезпеченні безперервності планування та використання ресурсів ENISA.

Після отримання таких запитів ENISA повинне без невиправданої затримки готувати проєкти схем для конкретних продуктів ІКТ, послуг ІКТ та процесів ІКТ. Комісія повинна оцінювати позитивний та негативний вплив своїх запитів на відповідний сегмент ринку, особливо на МСП, у розрізі інновацій, перешкод для виходу на такий ринок та витрат для кінцевих користувачів. Комісію необхідно уповноважити на ухвалення європейських схем сертифікації кібербезпеки на основі проєктів схем, підготовлених ENISA, шляхом імплементаційних актів. Беручи до уваги загальну мету та безпекові цілі, передбачені в цьому Регламенті, ухвалена Комісією європейська схема сертифікації кібербезпеки повинна визначати мінімальний набір елементів, що стосуються предмету, сфери застосування та функціонування індивідуальної схеми. Серед іншого, такі елементи повинні включати сферу застосування та цілі сертифікації кібербезпеки, включно з категоріями охоплених продуктів ІКТ, послуг ІКТ та процесів ІКТ, детальну специфікацію вимог до кібербезпеки, наприклад, шляхом покликання на стандарти або технічні специфікації, специфічні критерії оцінювання та методи оцінювання, а також очікуваний рівень надійності («базовий», «істотний» або «високий») та оцінювання рівнів, якщо доцільно. У ENISA повинна бути змога відхиляти запити від ECCG. Такі рішення ухвалює Правління; такі рішення повинні бути належним чином обґрунтовані.

(85) ENISA повинне вести вебсайт для надання інформації про європейські схеми сертифікації кібербезпеки та їх публікування, що серед іншого повинен містити запити на підготовку проєктів схем та відгуки, отримані в рамках консультацій, проведених ENISA на підготовчій фазі. Вебсайт повинен також містити інформацію про європейські сертифікати з кібербезпеки та декларації ЄС про відповідність, видані згідно з цим Регламентом, включно з інформацією стосовно відкликання й завершення дії європейських сертифікатів з кібербезпеки та декларацій ЄС про відповідність. На вебсайті повинні також вказуватися національні схеми сертифікації кібербезпеки, які замінено європейською схемою сертифікації кібербезпеки.

(86) Рівень надійності європейської схеми сертифікації кібербезпеки — це основа впевненості в тому, що продукт ІКТ, послуга ІКТ або процес ІКТ відповідає вимогам безпеки конкретної європейської схеми сертифікації кібербезпеки. Для забезпечення узгодженості європейських рамок сертифікації кібербезпеки, європейська схема сертифікації кібербезпеки повинна визначати рівні надійності європейських сертифікатів з кібербезпеки та декларацій ЄС про відповідність, виданих згідно за такою схемою. Кожен європейський сертифікат з кібербезпеки має стосуватися одного з рівнів надійності: «базового», «істотного» або «високого», а декларація ЄС про відповідність має стосуватися лише рівня надійності «базовий». Рівень надійності має бути відображенням суворості та глибини оцінювання продукту ІКТ, послуги ІКТ або процесу ІКТ, та повинен характеризуватися покликанням на технічні специфікації, стандарти та процедури стосовно нього, включно з процедурами технічного контролю, метою яких є пом’якшення або попередження інцидентів. У різних галузевих сферах, у яких застосовується сертифікація, кожен рівень надійності повинен бути послідовним.

(87) У європейській схемі сертифікації кібербезпеки може бути визначено декілька рівнів оцінювання, залежно від суворості та глибини використовуваних методів оцінювання. Рівні оцінювання повинні відповідати одному з рівнів надійності та повинні бути пов’язані з відповідною комбінацією компонентів надійності. Для всіх рівнів надійності продукти ІКТ, послуги ІКТ або процеси ІКТ повинні передбачати низку функцій безпеки, визначених конкретною схемою, що можуть включати: готову конфігурацію безпеки, підписаний код, безпечні оновлення, запобігання зловмисному використанню та захист вбудованого програмного забезпечення й динамічної пам’яті. Такі функції повинно бути розроблено, та їх повинні підтримувати з використанням орієнтованих на безпеку підходів до розробки та пов’язаних інструментів, щоб забезпечити надійне вбудування дієвих програмних та апаратних механізмів.

(88) Для рівня надійності «базовий» оцінювання повинне враховувати принаймні такі компоненти надійності: оцінювання повинне принаймні включати аналіз технічної документації продукту ІКТ, послуги ІКТ або процесу ІКТ органом з оцінювання відповідності. Якщо сертифікація охоплює

процеси ІКТ, предметом технічного огляду також повинен бути процес, використаний для проєктування, розробки та обслуговування продукту ІКТ або послуги ІКТ. Якщо європейська схема сертифікації кібербезпеки передбачає самооцінювання відповідності, виробнику або надавачу продуктів ІКТ, послуг ІКТ або процесів ІКТ повинно бути достатньо виконати самостійне оцінювання продукту ІКТ, послуги ІКТ або процесу ІКТ на відповідність схемі сертифікації.

(89) Для рівня надійності «істотний» оцінювання, на додаток до вимог для рівня надійності «базовий», повинне враховувати принаймні перевірку безпеки функціональних компонентів продукту ІКТ, послуги ІКТ або процесу ІКТ на відповідність технічній документації.

(90) Для рівня надійності «високий» оцінювання, на додаток до вимог для рівня надійності «істотний», повинне враховувати принаймні випробування ефективності, яке оцінює функціональні компоненти продукту ІКТ, послуги ІКТ або процесу ІКТ з точки зору опірності передовим кібератакам, які виконують суб'єкти зі значними вміннями та ресурсами.

(91) Використання європейської сертифікації кібербезпеки та декларацій ЄС про відповідність повинне залишатися добровільним, крім як у випадках, коли це передбачено актами права Союзу або актами права держав-членів, ухваленими на виконання актів права ЄС. За відсутності гармонізованого законодавства Союзу, держави-члени повинні мати змогу ухвалювати національні технічні регламенти з визначенням обов'язковості сертифікації згідно з європейською схемою сертифікації кібербезпеки відповідно до Директиви Європейського Парламенту і Ради (ЄС) 2015/1535 ([20]). Держави-члени також можуть використовувати європейську сертифікацію кібербезпеки в контексті публічних закупівель та Директиви Європейського Парламенту і Ради 2014/24/ЄС ([21]).

(92) У певних сферах може бути необхідним у майбутньому встановлювати специфічні вимоги до кібербезпеки та запроваджувати їх обов'язкову сертифікацію певних продуктів ІКТ, послуг ІКТ або процесів ІКТ, щоб підвищувати рівень кібербезпеки в Союзі. Комісія повинна здійснювати постійний моніторинг впливу ухвалених європейських схем сертифікації кібербезпеки у розрізі доступності безпечних продуктів ІКТ, послуг ІКТ та процесів ІКТ на внутрішньому ринку, та повинна здійснювати регулярне оцінювання рівня використання схем сертифікації виробниками або надавачами продуктів ІКТ, послуг ІКТ або процесів ІКТ. Повинна бути надана оцінка дієвості європейських схем сертифікації кібербезпеки та потреби в обов'язковості специфічних схем у світлі законодавства Союзу з кібербезпеки, зокрема Директиви (ЄС) 2016/1148, беручи до уваги питання безпеки мережевих та інформаційних систем, що використовуються операторами основних послуг.

(93) Європейські сертифікати з кібербезпеки та декларації ЄС про відповідність повинні допомагати кінцевим користувачам робити поінформований вибір. Тому продукти ІКТ, послуги ІКТ та процеси ІКТ, які було сертифіковано чи на які було видано декларацію ЄС про відповідність, повинні супроводжуватися структурованою інформацією, адаптованою під очікуваний рівень технічних знань потенційного кінцевого користувача. Уся така інформація повинна бути доступна онлайн та у фізичній формі, якщо доцільно. Кінцевий користувач повинен мати доступ до інформації щодо реєстраційного номера схеми сертифікації, рівня надійності, опису ризиків кібербезпеки, пов'язаних з продуктом ІКТ, послугою ІКТ або процесом ІКТ, та органу чи організації, ким видано сертифікат, або мати змогу отримати копію європейського сертифіката з кібербезпеки. Крім того, кінцевого користувача повинно бути поінформовано про політику підтримки кібербезпеки, а точніше про те, як довго кінцевий користувач може розраховувати на отримання оновлень або латок кібербезпеки, від виробника або надавача продуктів ІКТ, послуг ІКТ або процесів ІКТ. За необхідності повинні бути надані вказівки про дії чи налаштування, з допомогою яких кінцевий користувач може встановити або підвищити рівень кібербезпеки продукту ІКТ або послуги ІКТ, та вказано контактну інформацію місця, за яким можна звернутися або отримати підтримку в разі кібератак (на додаток до автоматичного надсилання звітів). Така інформація повинна підлягати регулярному оновленню та публікуватися на вебсайті разом з наданням інформації про європейські схеми сертифікації кібербезпеки.

(94) У світлі досягнення цілей цього Регламенту та уникнення фрагментації внутрішнього ринку,

національні схеми або процедури сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ або процесів ІКТ, охоплених європейською схемою сертифікації кібербезпеки, повинні втратити дію з дати, встановленої Комісією за допомогою імплементаційних актів. Крім того, держави-члени не повинні вводити нових національних схем сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ, які вже охоплені чинною європейською схемою сертифікації кібербезпеки. Однак, не потрібно обмежувати держави-члени в ухваленні або збереженні національних схем сертифікації кібербезпеки для потреб національної безпеки. Держави-члени повинні інформувати Комісію та ECCG про будь-які наміри створити нові національні схеми сертифікації кібербезпеки. Комісія та ECCG повинні оцінювати вплив нових національних схем сертифікації кібербезпеки на належне функціонування внутрішнього ринку та у світлі будь-яких стратегічних інтересів при запиті на ухвалення замість них європейської схеми сертифікації кібербезпеки.

(95) Європейські схеми сертифікації кібербезпеки покликані допомогти гармонізувати практики кібербезпеки у Союзі. Вони повинні сприяти підвищенню рівня кібербезпеки по всьому Союзу. При розробці європейських схем сертифікації кібербезпеки необхідно враховувати та передбачати розвиток інновацій у сфері кібербезпеки.

(96) Європейські схеми сертифікації кібербезпеки повинні враховувати поточні методи розробки програмного та апаратного забезпечення та, зокрема, вплив частого оновлення програмного забезпечення та оновлення мікропрограм на окремі європейські сертифікати з кібербезпеки. Європейські схеми сертифікації кібербезпеки повинні визначати умови, на яких у разі оновлення може вимагатися повторна сертифікація продукту ІКТ, послуги ІКТ чи процесу ІКТ або звуження сфери дії конкретного європейського сертифіката з кібербезпеки, беручи до уваги будь-який можливий негативний вплив оновлення на відповідність вимогам безпеки такого сертифіката.

(97) Після ухвалення європейської схеми сертифікації кібербезпеки виробники або надавачі продуктів ІКТ, послуг ІКТ або процесів ІКТ повинні мати змогу подавати заяви на сертифікацію своїх продуктів ІКТ, послуг ІКТ або процесів ІКТ до органу з оцінювання відповідності за їхнім вибором будь-де в Союзі. Органи з оцінювання відповідності повинні бути акредитовані національним органом з акредитації, якщо вони відповідають вимогам, визначеним у цьому Регламенті. Акредитацію необхідно надавати на максимальний строк у п’ять років, і повинна бути змога продовжити її на тих самих умовах, якщо орган з оцінювання відповідності продовжує відповідати вимогам. Національні органи з акредитації повинні обмежувати або призупиняти дію або відкликати акредитацію органу з оцінювання відповідності за умови недотримання умов акредитації або порушення органом з оцінювання відповідності положень цього Регламенту.

(98) Покликання у національному законодавстві на національні стандарти, які втратили чинність унаслідок набуття чинності європейською схемою сертифікації кібербезпеки, можуть бути джерелом плутанини. Тому держави-члени повинні відображати ухвалення європейської схеми сертифікації кібербезпеки у своєму національному законодавстві.

(99) Для досягнення еквівалентності стандартів по всьому Союзу, для сприяння взаємному визнанню та для просування загального прийняття європейських сертифікатів з кібербезпеки та декларацій ЄС про відповідність, необхідно запровадити систему партнерських перевірок між національними органами з сертифікації кібербезпеки. Партнерська перевірка повинна охоплювати процедури для нагляду за відповідністю продуктів ІКТ, послуг ІКТ та процесів ІКТ умовам видачі європейських сертифікатів з кібербезпеки, для моніторингу обов’язків виробників або надавачів продуктів ІКТ, послуг ІКТ чи процесів ІКТ, які здійснюють самооцінювання відповідності, для моніторингу органів з оцінювання відповідності та відповідності експертних знань персоналу органів, що видають сертифікати рівня надійності «високий». У Комісії повинна бути змога шляхом ухвалення імплементаційних актів визначати принаймні п’ятирічний план партнерських перевірок та визначати критерії й методології для функціонування системи партнерських перевірок.

(100) Без обмеження системи партнерських перевірок у цілому, що повинна бути запроваджена серед усіх національних органів сертифікації кібербезпеки в європейських рамках сертифікації кібербезпеки, певні європейські схеми сертифікації кібербезпеки можуть включати механізм

партнерського оцінювання для органів, що видають європейські сертифікати з кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ з рівнем надійності «високий» у рамках таких схем. ECCG має підтримувати впровадження таких механізмів партнерського оцінювання. Партнерські оцінювання повинні передбачати оцінювання ступеня гармонізації виконання своїх завдань відповідними органами, і вони можуть включати механізми оскарження. Результати партнерського оцінювання повинні оприлюднюватися. Відповідні органи можуть ухвалювати потрібні інструменти для адаптації своєї практики та експертних знань відповідним чином.

(101) Держави-члени повинні призначити один чи більше національних органів із сертифікації кібербезпеки для здійснення нагляду за дотриманням обов'язків, виниклих на підставі цього Регламенту. Національним органом із сертифікації кібербезпеки може бути як новостворений орган, так і вже наявний. Держава-член також повинна мати змогу призначати, після погодження з іншою державою-членом, один чи більше національних органів із сертифікації кібербезпеки на території такої іншої держави-члена.

(102) Національні органи з сертифікації кібербезпеки повинні, серед іншого, здійснювати моніторинг та забезпечувати дотримання обов'язків виробників чи надавачів продуктів ІКТ, послуг ІКТ або процесів ІКТ, створених на їхній території, у розрізі декларації ЄС про відповідність, повинні надавати підтримку національним органам з акредитації у здійсненні моніторингу та нагляду за діяльністю органів з оцінювання відповідності шляхом надання їм експертних знань та відповідної інформації, повинні уповноважувати органи з оцінювання відповідності здійснювати свої завдання, якщо такі органи відповідають додатковим вимогам, визначеним у європейській схемі сертифікації кібербезпеки, та повинні здійснювати моніторинг відповідних змін у сфері сертифікації кібербезпеки. Національні органи з сертифікації кібербезпеки повинні також розглядати скарги, подані фізичними або юридичними особами, пов'язані з європейськими сертифікатами з кібербезпеки, виданими такими органами, або пов'язані з європейськими сертифікатами з кібербезпеки, виданими органами з оцінювання відповідності, якщо такі сертифікати підтверджують рівень надійності «високий», та повинні розслідувати предмет таких скарг у належній мірі й інформувати скаржника про хід і результат розслідування протягом розумного строку. Крім того, національні органи з сертифікації кібербезпеки повинні співпрацювати з іншими національними органами сертифікації кібербезпеки або іншими органами публічної влади, у тому числі шляхом поширення інформації щодо можливої невідповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ вимогам цього Регламенту або вимогам конкретних європейських схем сертифікації кібербезпеки. Комісія повинна сприяти обміну інформацією шляхом запровадження загальної системи електронного обміну інформацією, наприклад, через Інформаційно-комунікаційну систему ринкового нагляду (ICSMS) та Систему швидкого сповіщення для небезпечних нехарчових продуктів (RAPEX), які вже використовуються органами ринкового нагляду відповідно до Регламенту (ЄС) № 765/2008.

(103) З метою забезпечення узгодженого використання європейських рамок сертифікації кібербезпеки, необхідно створити ECCG у складі з представників національних органів із сертифікації кібербезпеки. Основним завданням ECCG буде консультування та допомога Комісії у її роботи із забезпечення послідовного впровадження та використання європейських рамок сертифікації кібербезпеки, допомагати та тісно співпрацювати з ENISA у підготовці проєктів схем сертифікації кібербезпеки, у належним чином обґрунтованих випадках звертатися до ENISA із запитом про підготовку проєкту схеми, видавати висновки для ENISA щодо проєктів схем та видавати висновки для Комісії щодо підтвердження або перегляду наявних європейських схем сертифікації кібербезпеки. ECCG має сприяти обміну належними практиками та експертними знаннями між різними національними органами сертифікації кібербезпеки, відповідальними за авторизацію органів з оцінювання відповідності та видачу європейських сертифікатів з кібербезпеки.

(104) Для підвищення обізнаності та сприяння прийняттю майбутніх європейських схем сертифікації кібербезпеки, Комісія може видавати загальні або специфічні галузеві настанови з кібербезпеки, наприклад, щодо належних практик кібербезпеки або відповідальної поведінки у сфері

кібербезпеки, з акцентом на позитивному впливі від використання сертифікованих продуктів ІКТ, послуг ІКТ та процесів ІКТ.

(105) Для подальшого сприяння торгівлі та визнання того, що ланцюги постачання ІКТ мають глобальну природу, на підставі статті 218 Договору про функціонування Європейського Союзу (ДФЄС) Союз може укладати угоди про взаємне визнання європейських сертифікатів з кібербезпеки. Беручи до уваги консультації з ENISA та Європейською групою з сертифікації кібербезпеки, Комісія може рекомендувати започаткування відповідних переговорів. Стосовно кожної європейської схеми сертифікації кібербезпеки повинно бути розроблено спеціальні умови стосовно угод про взаємне визнання з третіми країнами.

(106) Для забезпечення однакових умов імплементації цього Регламенту необхідно надати Комісії виконавчі повноваження. Такі повноваження мають здійснюватися відповідно до Регламенту Європейського Парламенту і Ради (ЄС) № 182/2011 ([22]).

(107) Для ухвалення імплементаційних актів щодо європейських схем сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ або процесів ІКТ, для ухвалення імплементаційних актів щодо механізмів стосовно запитів до ENISA, для ухвалення імплементаційних актів стосовно плану партнерських перевірок національних органів з сертифікації кібербезпеки та для ухвалення імплементаційних актів стосовно обставин, форматів та процедур для нотифікації Комісії національними органами з сертифікації кібербезпеки акредитованих органів з оцінювання відповідності повинна використовуватися експертна процедура.

(108) Діяльність ENISA повинна бути предметом регулярного та незалежного оцінювання. Таке оцінювання повинне стосуватися цілей, робочих практик та відповідності завдань ENISA, зокрема, завдань щодо операційної співпраці на рівні Союзу. Таке оцінювання повинне охоплювати також вплив, дієвість і ефективність європейських рамок сертифікації кібербезпеки. У разі перегляду, Комісія повинна оцінювати, наскільки роль ENISA як довідкового центру для консультацій та обміну експертними знаннями може бути посилена, а також Комісія повинна оцінювати потенціал розширення ролі ENISA стосовно оцінювання продуктів ІКТ, послуг ІКТ та процесів ІКТ третіх країн, які не відповідають правилам Союзу, при ввезенні таких продуктів, послуг та процесів до Союзу.

(109) Оскільки цілі цього Регламенту не можуть достатньою мірою бути досягнуті державами-членами, але їх можна, з огляду на його масштаб і наслідки, краще досягти на рівні Союзу, Союз може ухвалити інструменти згідно з принципом субсидіарності, як встановлено у статті 5 Договору про Європейський Союз (ДЄС). Згідно з принципом пропорційності, як визначено у зазначеній статті, цей Регламент не виходить за межі необхідного для досягнення таких цілей.

(110) Регламент (ЄС) № 526/2013 необхідно скасувати,

УХВАЛИЛИ ЦЕЙ РЕГЛАМЕНТ:

РОЗДІЛ І
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1

Предмет та сфера застосування

1. З метою забезпечення належного функціонування внутрішнього ринку з одночасним прагненням досягнути високого рівня кібербезпеки, кіберстійкості та довіри в межах Союзу, цей Регламент встановлює:

(a) цілі, завдання та організаційні питання, що стосуються ENISA (Агентства Європейського Союзу з питань мережевої та інформаційної безпеки); та

(b) рамки для створення європейських схем сертифікації кібербезпеки з метою забезпечення належного

рівня кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ в Союзі, а також з метою уникнення фрагментації внутрішнього ринку стосовно схем сертифікації кібербезпеки в Союзі.

Рамки, зазначені в пункті (b) першого підпараграфа, застосовують без обмежень до спеціальних положень в інших правових актах Союзу, що стосуються добровільної або обов'язкової сертифікації.

2. Цей Регламент не обмежує компетенцій держав-членів щодо діяльності, пов'язаної з громадською безпекою, обороною, національної безпекою, та діяльності держави у сферах кримінального права.

Стаття 2

Терміни та означення

Для цілей цього Регламенту застосовують такі терміни та означення:

(1) «кібербезпека» означає діяльність, необхідну для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, які зазнають впливу кіберзагроз;

(2) «мережева та інформаційна система» означає мережеву та інформаційну систему, як означено в пункті (1) статті 4 Директиви (ЄС) 2016/1148;

(3) «національна стратегія безпеки мережевих та інформаційних систем» означає національну стратегію безпеки мережевих та інформаційних систем, як означено в пункті (3) статті 4 Директиви (ЄС) 2016/1148;

(4) «оператор основних послуг» означає оператора основних послуг, як означено в пункті (4) статті 4 Директиви (ЄС) 2016/1148;

(5) «надавач цифрових послуг» означає надавача цифрових послуг, як означено в пункті (6) статті 4 Директиви (ЄС) 2016/1148;

(6) «інцидент» означає інцидент, як означено в пункті (7) статті 4 Директиви (ЄС) 2016/1148;

(7) «врегулювання інцидентів» означає врегулювання інцидентів, як означено в пункті (8) статті 4 Директиви (ЄС) 2016/1148;

(8) «кіберзагроза» означає будь-яку потенційну обставину, подію або дію, яка може пошкодити, порушити або інакше негативно вплинути на мережеві та інформаційні системи, користувачів таких систем та інших осіб;

(9) «європейська схема сертифікації кібербезпеки» означає комплексний набір правил, технічні вимоги, стандарти та процедури, які встановлені на рівні Союзу та які застосовують до сертифікації або оцінювання відповідності конкретних продуктів ІКТ, послуг ІКТ або процесів ІКТ;

(10) «національна схема сертифікації кібербезпеки» означає комплексний набір правил, технічні вимоги, стандарти та процедури, які розроблені та ухвалені національним органом публічної влади та які застосовують до сертифікації або оцінювання відповідності продуктів ІКТ, послуг ІКТ або процесів ІКТ в рамках конкретної схеми;

(11) «європейський сертифікат з кібербезпеки» означає документ, виданий відповідним органом, який підтверджує, що було проведено оцінювання певного продукту ІКТ, послуги ІКТ або процесу ІКТ на відповідність конкретним вимогам, встановленим у європейській схемі сертифікації кібербезпеки;

(12) «продукт ІКТ» означає елемент або групу елементів мережі або інформаційної системи;

(13) «послуга ІКТ» означає послугу, що головним або переважним чином полягає в передачі, зберіганні, отриманні або опрацюванні інформації за допомогою мережевих та інформаційних систем;

(14) «процес ІКТ» означає комплекс заходів, спрямованих на проєктування, розробку, надання або технічне обслуговування продукту ІКТ або послуги ІКТ;

(15) «акредитація» означає акредитацію, як означено в пункті (10) статті 2 Регламенту (ЄС) № 765/2008;

(16) «національний орган з акредитації» означає національний орган з акредитації, як означено в пункті (11) статті 2 Регламенту (ЄС) № 765/2008;

(17) «оцінювання відповідності» означає оцінювання відповідності, як означено в пункті (12) статті 2 Регламенту (ЄС) № 765/2008;

(18) «орган з оцінювання відповідності» означає орган з оцінювання відповідності, як означено в пункті (13) статті 2 Регламенту (ЄС) № 765/2008;

(19) «стандарт» означає стандарт, як означено в пункті (1) статті 2 Регламенту (ЄС) № 1025/2012;

(20) «технічні специфікації» означають документ, що встановлює технічні вимоги, яким повинні відповідати продукт ІКТ, послуга ІКТ або процес ІКТ, або процедури оцінювання відповідності стосовно продукту ІКТ, послуги ІКТ або процесу ІКТ;

(21) «рівень надійності» означає основу впевненості в тому, що продукт ІКТ, послуга ІКТ або процес ІКТ відповідає вимогам безпеки конкретної європейської схеми сертифікації кібербезпеки, вказує, на якому рівні відбулося оцінювання продукту ІКТ, послуги ІКТ або процесу ІКТ, але як такий не визначає рівень безпеки відповідного продукту ІКТ, послуги ІКТ або процесу ІКТ;

(22) «самооцінювання відповідності» означає дію, виконувану виробником або надавачем продуктів ІКТ, послуг ІКТ або процесів ІКТ, яка надає оцінку стосовно того, чи такі продукти ІКТ, послуги ІКТ або процеси ІКТ відповідають вимогам конкретної європейської схеми сертифікації кібербезпеки.

РОЗДІЛ II
(АГЕНТСТВО ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ)

ГЛАВА I
Мандат та цілі

Стаття 3

Мандат

1. ENISA виконує завдання, покладені на нього відповідно до цього Регламенту, з метою досягнення високого загального рівня кібербезпеки на території Союзу, у тому числі шляхом надання активної підтримки державам-членам, установам, органам, офісам та агентствам Союзу в покращенні рівня кібербезпеки. ENISA слугує довідковим пунктом, що надає консультації та експертні знання стосовно кібербезпеки установам, органам, офісам та агентствам Союзу, а також іншим відповідних стейкхолдерам у Союзі.

ENISA сприяє зниженню рівня фрагментації внутрішнього ринку, виконуючи завдання, покладені на нього відповідно до цього Регламенту.

2. ENISA виконує завдання, покладені на нього відповідно до правових актів Союзу, які визначають заходи для наближення законів, підзаконних нормативно-правових актів та адміністративних положень держави-члена, пов’язаних із кібербезпекою.

3. Виконуючи ці завдання, ENISA діє незалежно, уникаючи дублювання діяльності держав-членів та враховуючи наявні експертні знання держав-членів.

4. ENISA розробляє власні ресурси, зокрема технічні та людські здібності та вміння, необхідні для виконання завдань, покладених на нього відповідно до цього Регламенту.

Стаття 4

Цілі

1. ENISA є центром експертних знань з кібербезпеки завдяки своїй незалежності, науковій та технічній якості наданих консультацій, допомоги та інформації, прозорості своїх оперативних процедур, методів роботи та сумлінного виконання своїх завдань.

2. ENISA надає допомогу установам, органам, офісам та агентствам Союзу, а також державам-членам у розробленні та імплементації політики Союзу з питань кібербезпеки, у тому числі галузевої політики з кібербезпеки.

3. ENISA підтримує розбудову потенціалу та готовність на території Союзу шляхом надання допомоги установам, органам, офісам та агентствам Союзу, а також державам-членам та публічним і приватним стейкхолдерам для посилення захисту їхніх мережевих та інформаційних систем, розробки та посилення кіберстійкості та можливості реагування, а також для розвитку вмінь і навичок у сфері кібербезпеки.

4. ENISA сприяє співпраці, у тому числі обміну інформацією та координації на рівні Союзу, серед держав-членів, установ, органів, офісів та агентств Союзу та відповідних приватних і публічних стейкхолдерів у питаннях кібербезпеки.

5. ENISA сприяє розширенню можливостей у сфері кібербезпеки на рівні Союзу, щоб підтримати заходи держав-членів для запобігання кіберзагрозам та реагування на них, зокрема у випадку транскордонних інцидентів.

6. ENISA сприяє використанню європейської схеми сертифікації кібербезпеки з метою уникнення фрагментації внутрішнього ринку. ENISA сприяє впровадженню та технічному обслуговуванню європейських рамок сертифікації кібербезпеки відповідно до розділу III цього Регламенту з метою посилення прозорості кібербезпеки продуктів ІКТ, послуг ІКТ, процесів ІКТ, внаслідок чого відбуватиметься посилення рівня впевненості в цифровому внутрішньому ринку та його конкурентоспроможності.

7. ENISA сприяє досягненню високого рівня обізнаності в питаннях кібербезпеки, у тому числі кібергігієни та кіберграмотності, серед громадян, організацій та підприємств.

ГЛАВА II

Завдання

Стаття 5

Розробка та імплементація політики та законодавства Союзу

ENISA сприяє розробці та імплементації політики та законодавства Союзу шляхом:

(1) надання допомоги та консультацій стосовно розробки й перегляду політики та законодавства Союзу у сфері кібербезпеки та галузевої політики й законодавчих ініціатив, якщо це пов’язано з питанням кібербезпеки, зокрема шляхом надання незалежного висновку та аналізу, а також проведення підготовчої роботи;

(2) надання допомоги державам-членам у послідовній імплементації політики та законодавства Союзу з питань кібербезпеки, зокрема стосовно Директиви (ЄС) 2016/1148, у тому числі шляхом надання висновків, настанов та найкращих практик з таких питань як управління ризиками, звітування про інциденти та обмін інформацією, а також шляхом сприяння обміну найкращими практиками в цьому питанні між компетентними органами;

(3) надання допомоги державам-членам, а також установам, органам, офісам та агентствам Союзу в розробленні та сприянні впровадженню політик у сфері кібербезпеки, що стосуються підтримання загальної доступності або цілісності публічного ядра відкритого інтернету;

(4) сприяння роботі групи співпраці відповідно до статті 11 Директиви (ЄС) 2016/1148, із наданням своїх експертних знань та допомоги;

(5) підтримки:

(a) у розробленні та імплементації політики Союзу у сфері електронної ідентифікації та довірчих послуг, зокрема шляхом надання консультацій та видання технічних настанов, а також сприяння обміну найкращими практиками між компетентними органами;

(b) у сприянні підвищенню рівня безпеки електронних комунікацій, у тому числі шляхом надання консультацій та експертних знань, а також сприяння обміну найкращими практиками між компетентними органами;

(c) держав-членів в імплементації конкретних аспектів політики та законодавства Союзу про захист даних і приватності, що стосуються кібербезпеки, у тому числі шляхом надання консультацій Європейській раді із захисту даних за її запитом;

(6) підтримання регулярного перегляду діяльності в рамках політики Союзу, шляхом підготовки щорічного звіту щодо стану імплементації відповідних правових рамок стосовно:

(a) інформації щодо оповіщення про інциденти в державах-членах, надані єдиними контактними пунктами групі співпраці відповідно до статті 10(3) Директиви (ЄС) 2016/1148;

(b) резюме оповіщень про порушення безпеки або втрату цілісності, отриманих від надавачів довірчих послуг та наданих ENISA наглядовими органами відповідно до статті 19(3) Регламенту (ЄС) № 910/2014 Європейського Парламенту і Ради ([23]);

(c) оповіщень про інциденти безпеки, переданих провайдерами громадських електронних комунікаційних мереж, або про доступні для громадськості електронні комунікаційні послуги, надані ENISA компетентними органами відповідно до статті 40 Директиви (ЄС) 2018/1972.

Стаття 6

Розбудова потенціалу

1. ENISA надає допомогу:

(a) державам-членам у їхніх зусиллях щодо покращення рівня запобігання кібератакам та інцидентам, їх виявлення, аналізу та спроможності реагувати на них, шляхом забезпечення їх досвідом та експертними знаннями;

(b) державам-членам та установам, органам, офісам та агентствам Союзу в створенні та імплементації політики розкриття вразливостей на добровільній основі;

(c) установам, органам, офісам та агентствам Союзу у їхніх зусиллях щодо покращення рівня запобігання кібератакам та інцидентам, їх виявлення та аналізу, а також щодо покращення їх спроможності реагувати на них, зокрема шляхом надання належної підтримки CERT-EU;

(d) державам-членам у розробленні національних CSIRT на запит відповідно до статті 9(5) Директиви (ЄС) 2016/1148;

(e) державам-членам у розробленні національних стратегій щодо безпеки мережевих та інформаційних систем на запит відповідно до статті 7(2) Директиви (ЄС) 2016/1148, сприяє поширенню таких стратегій та відзначає прогрес у їх імплементації на території Союзу для просування найкращих практик;

(f) установам Союзу в розробленні та перегляді стратегій Союзу з питань кібербезпеки, сприянні їх поширенню та відстеженні прогресу в їх імплементації;

(g) національним CSIRT та CSIRT Союзу в підвищенні рівня їх спроможностей, у тому числі шляхом сприяння діалогу та обміну інформацією, щоб гарантувати, що з урахуванням сучасного рівня науково-технічного розвитку кожна CSIRT має загальний набір спроможностей та діє відповідно до найкращих практик;

(h) державам-членам шляхом організації регулярних навчань з кібербезпеки на рівні Союзу, зазначених

у статті 7(5), принаймні двічі на рік, та надання рекомендацій стосовно політики на основі процесу оцінювання навчань та вивченого під час них матеріалу;

(i) відповідним органам публічної влади, запропонувавши їм навчання з кібербезпеки, у відповідних випадках у співпраці зі стейкхолдерами;

(j) групі співпраці в процесі обміну найкращими практиками, зокрема стосовно ідентифікації державами-членами операторів основних послуг, відповідно до пункту (l) статті 11(3) Директиви (ЄС) 2016/1148, у тому числі стосовно транскордонних залежностей, що стосуються ризиків та інцидентів.

2. ENISA сприяє обміну інформацією всередині галузей та між ними, зокрема в галузях, перерахованих у додатку II до Директиви (ЄС) 2016/1148, із наданням найкращих практик та настанов щодо наявних інструментів, процедур, а також щодо того, як вирішувати регулятивні питання стосовно обміну інформацією.

Стаття 7

Оперативна співпраця на рівні Союзу

1. ENISA сприяє оперативній співпраці серед держав-членів, установ, органів, офісів та агентств Союзу та між стейкхолдерами.

2. ENISA співпрацює на оперативному рівні та створює синергії з установами, органами, офісами та агентствами Союзу, у тому числі CERT-EU, зі службами, які займаються кіберзлочинами, та з наглядовими органами, які займаються захистом приватності та персональних даних, з метою вирішення питань спільного інтересу, у тому числі шляхом:

(a) обміну ноу-хау та найкращими практиками;

(b) надання консультацій та настанов щодо відповідних питань з кібербезпеки;

(c) вжиття практичних заходів для виконання конкретних завдань після консультацій з Комісією.

3. ENISA створює секретаріат мережі CSIRT відповідно до статті 12(2) Директиви (ЄС) 2016/1148 та в такій ролі активно сприяє обміну інформацією та співпраці між його членами.

4. ENISA надає допомогу державам-членам щодо оперативної співпраці в рамках мережі CSIRT шляхом:

(a) консультування щодо посилення спроможностей із запобігання інцидентам, їх виявлення та реагування на них, консультацій щодо окремих кіберзагроз за запитом однієї або більше держав-членів;

(b) надання допомоги на запит однієї або більше держав-членів в оцінюванні інцидентів, які мають значний вплив, із забезпеченням експертними знаннями та зі сприянням технічному врегулюванню таких інцидентів, зокрема зі сприянням добровільному обміну відповідною інформацією та технічними рішеннями між державами-членами;

(c) аналізування вразливості та інцидентів на основі доступної для громадськості інформації або інформації, наданої добровільно державою-членом з цією метою; та

(d) надання підтримки з питань технічних запитів *ex-post* на запит однієї або більше держав-членів стосовно інцидентів, які мають значний вплив у розумінні Директиви (ЄС) 2016/1148.

При виконанні цих завдань ENISA та CERT-EU структуровано співпрацюють, щоб отримати користь від синергій та уникнути дублювання заходів.

5. ENISA регулярно організовує навчання з кібербезпеки на рівні Союзу та надає підтримку державам-членам, установам, органам, офісам та агентствам Союзу в організації навчань з кібербезпеки на їхні запити. Такі навчання з кібербезпеки на рівні Союзу можуть містити технічні, оперативні або стратегічні елементи. Двічі на рік ENISA організовує великомасштабні комплексні навчання.

У відповідних випадках ENISA також сприяє та допомагає в організації галузевих навчань з кібербезпеки разом із відповідними організаціями, які також беруть участь у навчаннях з кібербезпеки на рівні Союзу.

6. У тісній співпраці з державами-членами ENISA регулярно готує детальний технічний звіт ЄС про стан кібербезпеки стосовно інцидентів та кібератак на основі доступної для громадськості інформації, власного аналізу та звітів, наданих, серед іншого, командами CSIRT держав-членів або єдиними контактними пунктами, створеними відповідно до Директиви (ЄС) 2016/1148, в обох випадках на добровільній основі, EC3 та CERT-EU.

7. ENISA сприяє розробленню спільного реагування на великомасштабні транскордонні інциденти або кризи, пов'язані з кібербезпекою, на рівні Союзу та на рівні держав-членів переважно шляхом:

(a) збирання та аналізування звітів від національних джерел, які доступні громадськості або поширення яких відбувається на добровільній основі, щоб посприяти досягненню загальної ситуаційної обізнаності;

(b) забезпечення ефективного потоку інформації та надання механізмів передачі вирішення проблем на вищий рівень між мережею CSIRT та технічними й політичними суб'єктами, відповідальними за вироблення й ухвалення рішень, на рівні Союзу;

(c) сприяння технічному врегулюванню таких інцидентів або криз на запит, зокрема сприяючи добровільному обміну технічними рішеннями між державами-членами;

(d) надання підтримки установам, органам, офісам та агентствам Союзу та державам-членам у комунікації з громадськістю стосовно таких інцидентів або криз на їхній запит;

(e) тестування планів співпраці в реагуванні на такі інциденти або кризи на рівні Союзу та шляхом надання допомоги державам-членам у тестуванні таких планів на національному рівні на їхній запит.

Стаття 8

Ринок, сертифікація кібербезпеки та стандартизація

1. ENISA сприяє та надає допомогу в розробленні та імплементації політики Союзу з сертифікації кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ, як визначено в розділі III цього Регламенту, шляхом:

(a) постійного моніторингу розвитку у відповідних сферах стандартизації та рекомендування відповідних технічних специфікацій для використання в розробці європейських схем сертифікації кібербезпеки відповідно до пункту (c) статті 54(1) у разі відсутності стандартів;

(b) підготовки проєктів європейських схем сертифікації кібербезпеки («проєкти схем») для продуктів ІКТ, послуг ІКТ та процесів ІКТ відповідно до статті 49;

(c) оцінювання ухвалених європейських схем сертифікації кібербезпеки відповідно до статті 49(8);

(d) участі в партнерських перевірках відповідно до статті 59(4);

(e) надання допомоги Комісії в створенні секретаріату ECCG відповідно до статті 62(5).

2. ENISA створює секретаріат Групи стейкхолдерів із питань сертифікації кібербезпеки відповідно до статті 22(4).

3. ENISA складає та оприлюднює настанови та розробляє належні практики з питань вимог з кібербезпеки до продуктів ІКТ, послуг ІКТ та процесів ІКТ у співпраці з національними органами з сертифікації кібербезпеки та галуззю в офіційному, структурованому та прозорому порядку.

4. ENISA сприяє розбудові потенціалу відносно процесів оцінювання та сертифікації шляхом складання та оприлюднення настанов, а також шляхом надання підтримки державам-членам за їхнім запитом.

5. ENISA сприяє створенню та широкому використанню європейських та міжнародних стандартів управління ризиками та безпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ.

6. У співпраці з державами-членами та галуззю ENISA складає рекомендації та настанови стосовно технічних сфер, пов'язаних із вимогами безпеки до операторів основних послуг та надавачів цифрових послуг, а також стосовно вже наявних стандартів, у тому числі національних стандартів держав-членів, відповідно до статті 19(2) Директиви (ЄС) 2016/1148.

7. ENISA аналізує та поширює висновки стосовно головних тенденцій на ринку кібербезпеки як щодо попиту, так і щодо пропозиції, для сприяння розвитку ринку кібербезпеки в Союзі.

Стаття 9

Знання та інформація

ENISA:

(a) аналізує новітні технології та проводить тематичні оцінювання очікуваного соціального, правового, економічного та регуляторного впливу технологічних інновацій на кібербезпеку;

(b) виконує довгостроковий стратегічний аналіз кіберзагроз та інцидентів, щоб виявляти новітні тенденції та сприяти запобіганню інцидентів;

(c) у співпраці з експертами органів держав-членів та відповідними стейкхолдерами надає рекомендації, настанови та найкращі практики для безпеки мережевих та інформаційних систем, зокрема для безпеки інфраструктур, що підтримують сектори, перелічені в додатку II до Директиви (ЄС) 2016/1148, та тих, які використовують надавачі цифрових послуг, перелічені в додатку III до зазначеної Директиви;

(d) за допомогою спеціального порталу збирає, організовує та оприлюднює інформацію щодо кібербезпеки, надану установами, органами, офісами та агентствами Союзу, та інформацію щодо кібербезпеки, надану на добровільній основі державами-членами та приватними й публічними стейкхолдерами;

(e) збирає та аналізує доступну для громадськості інформацію стосовно значних інцидентів та складає звіти з метою надання настанов громадянам, організаціям та підприємствам на території Союзу.

Стаття 10

Підвищення рівня обізнаності та освіта

ENISA:

(a) підвищує рівень обізнаності громадськості про ризики, пов'язані з кібербезпекою, та дає настанови щодо належних практик для окремих користувачів, орієнтовані на громадян, організації та підприємства, у тому числі стосовно кібергігієни та кіберграмотності;

(b) у співпраці з державами-членами, установами, органами, офісами та агентствами Союзу й галузевими структурами регулярно організовує кампанії з підвищення обізнаності для покращення рівня кібербезпеки та всебічного висвітлення цього питання в Союзі, а також заохочує широке громадське обговорення;

(c) надає допомогу державам-членам у підвищенні рівня обізнаності щодо кібербезпеки та сприяє освіті в галузі кібербезпеки;

(d) підтримує тісну координацію та обмін найкращими практиками з питань обізнаності щодо кібербезпеки та освіти серед держав-членів.

Стаття 11

Дослідження та інновації

Стосовно досліджень та інновацій ENISA:

(a) консультує установи, органи, офіси та агентства Союзу та держави-члени щодо потреб і пріоритетів досліджень у сфері, що дозаолить ефективно реагувати на поточні та нові ризики й кіберзагрози, у тому числі з урахуванням нових та новітніх інформаційно-комунікаційних технологій, та з метою ефективного застосування технологій запобігання ризикам;

(b) бере участь в імплементації програм фінансування досліджень та інновацій або як бенефіціар, якщо Комісія надала йому відповідні повноваження;

(c) сприяє проведенню стратегічних досліджень та реалізації інноваційних програм на рівні Союзу в сфері кібербезпеки.

Стаття 12

Міжнародна співпраця

ENISA допомагає в зусиллях Союзу щодо співпраці з третіми країнами та міжнародними організаціями, а також у рамках відповідної міжнародної співпраці, щоб посприяти співпраці в питаннях, пов'язаних із кібербезпекою, шляхом:

(a) участі у відповідних випадках у ролі спостерігача в організації, що проводить міжнародні навчання, та підготовки аналізу і надання звітів про результати таких навчань Правлінню;

(b) сприяння обміну найкращими практиками на запит Комісії;

(c) надання експертних знань на запит Комісії;

(d) консультування та підтримання Комісії в питаннях, що стосуються угод про взаємне визнання сертифікатів про рівень кібербезпеки з третіми країнами, у співпраці з ECCG, створеною відповідно до статті 62.

ГЛАВА III

Організація ENISA

Стаття 13

Структура ENISA

До адміністративно-управлінської структури ENISA належать:

(a) Правління;

(b) Виконавча рада;

(c) виконавчий директор;

(d) Консультативна група ENISA;

(e) Мережа національних зв'язкових офіцерів.

Секція 1

Правління

Стаття 14

Склад Правління

1. До складу Правління входять по одному члену, призначеному кожною державою-членом, та два члени, призначені Комісією. Усі члени мають право голосу.

2. Кожен член Правління має свого заступника. Такий заступник представляє члена в разі його або її відсутності.

3. Членів Правління та їхніх заступників призначають на основі їхніх знань у сфері кібербезпеки з урахуванням їхніх відповідних управлінських, адміністративних та бюджетних навичок. Комісія та держави-члени докладають зусиль для забезпечення того, щоб їхні представники у Правлінні змінювалися якомога рідше, для забезпечення безперервності роботи Правління. Комісія та держави-члени прагнуть досягти гендерного балансу в Правлінні.

4. Строк дії повноважень членів Правління та їхніх заступників становить чотири роки. Такий строк є поновлюваним.

Стаття 15

Функції Правління

1. Правління:

(a) встановлює основний напрям діяльності ENISA та забезпечує діяльність ENISA відповідно до правил та принципів, встановлених у цьому Регламенті; також забезпечує узгодження роботи ENISA та діяльності держав-членів, у тому числі й на рівні Союзу;

(b) ухвалює проєкт єдиного програмного документа ENISA, зазначеного у статті 24, перед поданням його на розгляд Комісії для отримання висновку;

(c) ухвалює єдиний програмний документ ENISA з урахуванням висновку Комісії;

(d) здійснює контроль за імплементацією багаторічних та річних програм, включених до єдиного програмного документа;

(e) ухвалює річний бюджет ENISA та виконує інші функції стосовно бюджету ENISA відповідно до глави IV;

(f) оцінює та ухвалює зведений річний звіт про діяльність ENISA, який містить фінансову звітність та опис того, як ENISA досягнуло своїх показників ефективності, подає річний звіт та його оцінку Європейському Парламенту, Раді, Комісії та Рахунковій палаті до 1 липня поточного року та оприлюднює річний звіт;

(g) ухвалює фінансові правила, які застосовують до ENISA відповідно до статті 32;

(h) ухвалює стратегію боротьби з шахрайством, пропорційну ризикам шахрайства, беручи до уваги аналіз витрат і вигід від заходів, які підлягають імплементації;

(i) увалює правила щодо запобігання та управління конфліктами інтересів між своїми членами;

(j) забезпечує належні подальші заходи на основі висновків та рекомендацій, отриманих у результаті розслідувань Європейського бюро боротьби із шахрайством (OLAF), а також із різних звітів про проведення внутрішнього або зовнішнього аудиту та оцінок;

(k) ухвалює свій внутрішній регламент, включно з правилами ухвалення попередніх рішень стосовно делегування специфічних завдань відповідно до статті 19(7);

(l) стосовно питань, пов’язаних із персоналом ENISA, виконує повноваження, які відповідно до Положення про персонал («Положення про персонал») та Умов працевлаштування інших службовців Європейського Союзу («Умови працевлаштування інших службовців»), встановлених у Регламенті Ради (ЄЕС, Євратом, ЄСВС) № 259/68 ([24]) покладено на орган, уповноважений призначати персонал, та на орган, уповноважений укладати трудові договори, («повноваження органу, що уповноважений призначати персонал»), відповідно до параграфа 2 цієї статті;

(m) ухвалює правила імплементації Положень про персонал та Умов працевлаштування інших службовців відповідно до процедури, встановленої в статті 110 Положення про персонал;

(n) призначає виконавчого директора та, у відповідних випадках, подовжує строк його повноважень або

звільняє його або її з посади відповідно до статті 36;

(o) призначає бухгалтера, який може бути бухгалтером Комісії та який є повністю незалежним у виконанні своїх обов'язків;

(p) ухвалює всі рішення щодо створення внутрішніх структур ENISA та, за необхідності, щодо зміни таких структур, беручи до уваги потреби діяльності ENISA та враховуючи розсудливе управління бюджетом;

(q) дає дозвіл на створення робочих механізмів відповідно до статті 7;

(r) дає дозвіл на створення та укладання робочих угод відповідно до статті 42.

2. Відповідно до статті 110 Положення про персонал Правління ухвалює рішення на основі статті 2(1) Положення про персонал та статті 6 Умов працевлаштування інших службовців із делегуванням відповідних повноважень органу, уповноваженому призначати персонал, виконавчому директорові та з визначенням умов, за яких таке делегування повноважень може бути призупинено. Виконавчий директор може субделегувати такі повноваження.

3. Якщо цього вимагають виняткові обставини, Правління може ухвалювати рішення призупинити делегування повноважень органу, уповноваженого призначати персонал, виконавчому директору, а також повноважень органу, уповноваженого призначати персонал, субделегованих виконавчим директором, та натомість виконувати їх самостійно або делегувати їх одному зі своїх членів або члену персоналу, іншому ніж виконавчий директор.

Стаття 16

Голова Правління

Правління обирає голову та заступника голови серед своїх членів більшістю у дві третини голосів членів. Строк перебування на посаді становить чотири роки і є поновлюваним один раз. Однак якщо їхнє членство у Правлінні закінчується у будь-який час протягом строку перебування на посаді, строк їх перебування на посаді закінчується автоматично у такий день. Заступник голови замінює на посаді голову *ex officio*, якщо голова не здатний виконувати свої обов'язки.

Стаття 17

Засідання Правління

1. Засідання Правління скликає його голова.

2. Правління проводить щонайменше два чергові засідання на рік. Правління також проводить позачергові засідання на запит голови, на запит Комісії або на запит принаймні однієї третини його членів.

3. Виконавчий директор бере участь у засіданнях Правління, але без права голосу.

4. Члени Консультативної групи ENISA можуть брати участь у засіданнях Правління на запрошення голови, проте без права голосу.

5. Члени Правління та їхні заступники можуть отримувати допомогу консультантів або експертів під час засідань Правління відповідно до внутрішнього регламенту Правління.

6. ENISA створює секретаріат Правління.

Стаття 18

Правила голосування Правління

1. Правління ухвалює рішення більшістю голосів своїх членів.

2. Більшість у дві третини голосів членів Правління вимагається для ухвалення єдиного програмного документа та річного бюджету, а також для призначення на посаду, подовження строку перебування на

посаді або звільнення з посади виконавчого директора.

3. Кожний член має один голос. У разі відсутності одного з членів, його заступник уповноважений користуватися правом голосу такого члена.

4. Голова Правління бере участь у голосуванні.

5. Виконавчий директор не бере участі в голосуванні.

6. Внутрішній регламент Правління встановлює більш детальні процедури голосування, зокрема обставини, за яких певний член може діяти від імені іншого члена.

Секція 2

Виконавча рада

Стаття 19

Виконавча рада

1. Виконавча рада надає допомогу Правлінню.

2. Виконавча рада:

(a) готує рішення, які ухвалює Правління;

(b) разом із Правлінням забезпечує належні подальші заходи на основі висновків та рекомендацій, отриманих у результаті розслідувань OLAF, а також з різних звітів про проведення внутрішнього або зовнішнього аудиту та оцінок;

(c) без обмеження обов'язків виконавчого директора, визначених у статті 20, надає допомогу та консультації виконавчому директору стосовно імплементації рішень Правління з адміністративних та бюджетних питань відповідно до статті 20.

3. До складу Виконавчої ради входять п'ять членів. Членів Виконавчої ради призначають з числа членів Правління. Одним із членів повинен бути голова Правління, який також може виконувати роль голови Виконавчої ради, та ще одним членом повинен бути один із представників Комісії. Під час призначення членів Виконавчої ради необхідно дотримуватися принципів забезпечення гендерного балансу у Виконавчій раді. Виконавчий директор бере участь у засіданнях Виконавчої ради, але без права голосу.

4. Строк дії повноважень членів Виконавчої ради становить чотири роки. Такий строк є поновлюваним.

5. Виконавча рада проводить засідання принаймні раз на три місяці. Голова Виконавчої ради скликає додаткові засідання на запит її членів.

6. Правління визначає внутрішній регламент Виконавчої ради.

7. За необхідності в надзвичайних ситуаціях Виконавча рада може ухвалювати певні попередні рішення від імені Правління, зокрема з адміністративно-управлінських питань, включаючи призупинення делегування повноважень органу, уповноваженого призначати персонал, та бюджетні питання. Правління повинне без невиправданої затримки отримувати повідомлення про будь-які такі тимчасові рішення. Правління потім вирішує, схвалити чи відхилити тимчасове рішення, не пізніше ніж через три місяці після ухвалення рішення. Виконавча рада не ухвалює рішень від імені Правління, які вимагають схвалення більшістю у дві третіх голосів членів Правління.

Секція 3

Виконавчий директор

Стаття 20

Обов’язки виконавчого директора

1. Агентством ENISA керує його виконавчий директор, який є незалежним у виконанні своїх обов’язків. Виконавчий директор є підзвітним перед Правлінням.

2. Виконавчий директор на запрошення звітує перед Європейським Парламентом про виконання своїх обов’язків. Рада може вимагати від виконавчого директора звітування про виконання його або її завдань.

3. Виконавчий директор відповідає за:

(a) щоденне управління ENISA;

(b) виконання рішень, ухвалених Правлінням;

(c) підготовку проєкту єдиного програмного документа і подання його Правлінню для схвалення перед поданням його Комісії;

(d) виконання єдиного програмного документа та звітування перед Правлінням про його виконання;

(e) підготовку зведеного річного звіту про діяльність ENISA, включно з виконанням річної робочої програми ENISA, та його подання Правлінню для оцінювання та затвердження;

(f) підготовку плану дій за результатами висновків ретроспективного оцінювання та звітування перед Комісією про прогрес двічі на рік;

(g) підготовку плану дій за результатами висновків звітів про проведення внутрішнього або зовнішнього аудиту, а також розслідувань OLAF, та звітування про прогрес двічі на рік перед Комісією та регулярно перед Правлінням;

(h) підготовку проєкту фінансових правил, застосовних до ENISA, як зазначено в статті 32;

(i) підготовку проєкту кошторису доходів і витрат ENISA та за виконання його бюджету;

(j) захист фінансових інтересів Союзу шляхом застосування запобіжних заходів проти шахрайства, корупції та будь-яких інших незаконних дій шляхом проведення дієвих перевірок та, у разі виявлення порушень, стягнення неправильно сплачених сум і, у відповідних випадках, накладення дієвих, пропорційних і стримувальних адміністративних і фінансових санкцій;

(k) підготовку стратегії боротьби з шахрайством для ENISA і представлення її Правлінню для затвердження;

(l) встановлення та підтримання контакту з бізнес-спільнотами та споживчими організаціями для забезпечення регулярного діалогу з відповідними стейкхолдерами;

(m) регулярний обмін ідеями та інформацією з установами, органами, офісами та агентствами Союзу щодо їхньої діяльності з питань кібербезпеки для забезпечення узгодженості в розробленні та імплементації політики Союзу;

(n) виконання інших завдань, покладених на виконавчого директора цим Регламентом.

4. У разі необхідності та в рамках цілей та завдань ENISA виконавчий директор може створювати спеціалізовані експертні робочі групи, включно із залученням експертів з компетентних органів держав-членів. Виконавчий директор заздалегідь інформує про них Правління. Процедури, зокрема щодо формування складу робочих груп, призначення експертів робочих груп виконавчим директором та діяльності робочих груп, повинні бути визначені у внутрішньому регламенті ENISA.

5. У разі необхідності, для ефективного та дієвого виконання завдань ENISA та на основі відповідного аналізу витрат і вигід виконавчий директор може ухвалити рішення про створення одного чи більше місцевих офісів в одній чи більше державах-членах. Перед ухваленням рішення про створення місцевого офісу виконавчий директор звертається за висновком до відповідних держав-членів, у тому числі до держави-члена, у якій розташований офіс ENISA, та отримує попередню згоду Комісії та Правління. У разі незгоди, що виникає в процесі консультування виконавчого директора та відповідних держав-членів, це питання виносять на розгляд Ради. Сукупна чисельність персоналу в усіх місцевих офісах повинна зводитися до мінімуму та не повинна перевищувати 40 % від загальної чисельності

персоналу ENISA в державі-члені, де розташований офіс ENISA. Сукупна чисельність персоналу в кожному місцевому офісі не повинна перевищувати 10 % від загальної чисельності персоналу ENISA в державі-члені, де розташований офіс ENISA.

У рішенні про створення місцевого офісу зазначають обсяг діяльності, яку місцевий офіс повинен здійснювати таким чином, щоб уникати непотрібних витрат і дублювання адміністративних функцій ENISA.

Секція 4

Консультативна група ENISA, Група стейкхолдерів з питань сертифікації кібербезпеки та Мережа національних зв'язкових офіцерів

Стаття 21

Консультативна група ENISA

1. Діючи за пропозицією виконавчого директора, Правління у прозорий спосіб створює Консультативну групу ENISA, до складу якої входять визнані експерти, які представляють відповідних стейкхолдерів, таких як сфера ІКТ, надавачі електронних комунікаційних мереж або послуг, доступних громадськості, малі та середні підприємства, оператори основних послуг, групи споживачів, наукові експерти у сфері кібербезпеки та представники компетентних органів, повідомлені відповідно до Директиви (ЄС) 2018/1972, європейські організації зі стандартизації, а також правоохоронні органи та наглядові органи з питань захисту даних. Правління повинне прагнути до забезпечення належного гендерного та географічного балансу, а також балансу між різними групами стейкхолдерів.

2. Процедури для Консультативної групи ENISA, зокрема ті, що стосуються її складу, пропозицій виконавчого директора, зазначених у параграфі 1, кількості та призначення її членів та діяльності Консультативної групи ENISA, повинні бути визначені у внутрішньому регламенті ENISA та оприлюднені.

3. Консультативну групу ENISA очолює виконавчий директор або будь-яка особа, призначена виконавчим директором залежно від випадку.

4. Строк дії повноважень членів Консультативної групи ENISA становить два з половиною роки. Члени Правління не можуть бути членами Консультативної групи ENISA. Експерти з Комісії та держав-членів мають право бути присутніми на засіданнях Консультативної групи ENISA та брати участь у її роботі. Представників інших органів, які не є членами Консультативної групи ENISA, можуть запрошувати відвідувати засідання Консультативної групи ENISA та брати участь у її роботі, якщо виконавчий директор вважає таку участь доцільною.

5. Консультативна група ENISA надає консультації ENISA в питаннях, що стосуються виконання завдань ENISA, крім застосування положень розділу III цього Регламенту. Зокрема вона надає виконавчому директору консультації з питань підготовки пропозиції стосовно річної програми роботи ENISA та з питань забезпечення комунікації з відповідними стейкхолдерами щодо питань, пов'язаних із річною робочою програмою.

6. Консультативна група ENISA регулярно інформує Правління про свою діяльність.

Стаття 22

Група стейкхолдерів з питань сертифікації кібербезпеки

1. Повинна бути створена Група стейкхолдерів з питань сертифікації кібербезпеки.

2. До складу Групи стейкхолдерів з питань сертифікації кібербезпеки повинні входити члени, обрані серед визнаних експертів, які представляють відповідних стейкхолдерів. Шляхом прозорого та відкритого конкурсу Комісія обирає, за пропозицією ENISA, членів Групи стейкхолдерів з питань

сертифікації кібербезпеки із забезпеченням балансу між різними групами стейкхолдерів та належного гендерного та географічного балансу.

3. Група стейкхолдерів з питань сертифікації кібербезпеки:

(a) надає Комісії консультації зі стратегічних питань щодо європейських рамок сертифікації кібербезпеки;

(b) надає на запит консультації ENISA із загальних та стратегічних питань, що стосуються завдань ENISA, пов'язаних із ринком, сертифікацією кібербезпеки та стандартизацією;

(c) надає допомогу Комісії в підготовці послідовної робочої програми Союзу, зазначеної в статті 47;

(d) надає висновок щодо послідовної робочої програми Союзу відповідно до статті 47(4); та

(e) у невідкладних випадках надає консультації Комісії та ECCG щодо потреби в додаткових сертифікаційних схемах, не включених до послідовної робочої програми Союзу, як зазначено в статтях 47 і 48.

4. Групу стейкхолдерів з питань сертифікації кібербезпеки спільно очолюють представники Комісії та ENISA, і ENISA створює її секретаріат.

Стаття 23

Мережа національних зв'язкових офіцерів

1. Діючи за пропозицією виконавчого директора, Правління створює Мережу національних зв'язкових офіцерів, до складу якої входять представники усіх держав-членів (національні зв'язкові офіцери). Кожна держава-член призначає одного представника до Мережі національних зв'язкових офіцерів. Засідання Мережі національних зв'язкових офіцерів можуть проводитися різними експертними складами.

2. Мережа національних зв'язкових офіцерів зокрема сприяє обміну інформацією між ENISA та державами-членами, а також надає підтримку ENISA в поширенні його діяльності, висновків та рекомендацій серед відповідних стейкхолдерів на території Союзу.

3. Національні зв'язкові офіцери діють як контактний пункт на національному рівні з метою сприяння співпраці між ENISA та національними експертами в контексті виконання річної робочої програми ENISA.

4. Тоді як національні зв'язкові офіцери тісно співпрацюють із представниками відповідних держав-членів у Правлінні, сама Мережа національних офіцерів зв'язку не дублює роботи Правління та інших форумів Союзу.

5. Функції та процедури Мережі національних офіцерів зв'язку визначають у внутрішньому регламенті ENISA та оприлюднюють.

Секція 5

Діяльність

Стаття 24

Єдиний програмний документ

1. ENISA веде діяльність відповідно до єдиного програмного документа, у якому визначені річні та багаторічні плани програми його діяльності та який включає всю його заплановану діяльність.

2. Щороку виконавчий директор готує проєкт єдиного програмного документа, що містить річні та багаторічні плани програми з відповідним плануванням фінансових та людських ресурсів, відповідно до статті 32 Делегованого регламенту (ЄС) № 1271/2013 ([25]) з урахуванням настанов, розроблених Комісією.

3. Не пізніше 30 листопада кожного року Правління ухвалює єдиний програмний документ, зазначений у параграфі 1, та передає його Європейському Парламенту, Раді та Комісії не пізніше 31 січня наступного року, а в подальшому також і будь-які оновлені версії згаданого документа.

4. Єдиний програмний документ стає остаточним після остаточного ухвалення загального бюджету Союзу і зазнає корегувань у разі необхідності.

5. Річна робоча програма містить детальні цілі та очікувані результати, у тому числі показники ефективності. Вона також містить опис заходів, які повинні отримати фінансування, та визначає фінансові й людські ресурси, розподілені для кожного заходу, відповідно до принципів бюджетування та управління кожного заходу. Річна робоча програма повинна узгоджуватися з багаторічною робочою програмою, зазначеною в параграфі 7. У ній повинні бути чітко вказані завдання, які були додані, змінені або вилучені порівняно з попереднім фінансовим роком.

6. Правління вносить зміни до ухваленої річної робочої програми, якщо на ENISA покладено нове завдання. Будь-які істотні зміни до річної робочої програми ухвалюють за тією самою процедурою, що й до початкової річної робочої програми. Правління може делегувати виконавчому директору повноваження вносити неістотні зміни до річної робочої програми.

7. Багаторічна робоча програма визначає загальний стратегічний план програми, включаючи цілі, очікувані результати та показники ефективності. Вона також визначає планування ресурсів, включаючи багаторічний бюджет і персонал.

8. Оновлення плану програми стосовно ресурсів відбувається щорічно. У відповідних випадках стратегічний план програми оновлюють, зокрема з метою врахування результатів оцінювання, зазначеного в статті 67.

Стаття 25

Заяви про інтереси

1. Члени Правління, виконавчий директор та посадові особи, прикомандировані державами-членами на тимчасовій основі, роблять заяву про зобов'язання та заяву про присутність чи відсутність будь-яких прямих або непрямих інтересів, що можна розглядати як такі, що шкодять їхній незалежності. Такі заяви повинні бути точними та повними, їх необхідно робити в письмовій формі щороку та оновлювати за необхідності.

2. Члени Правління, виконавчий директор та зовнішні експерти, які є учасниками спеціалізованих робочих груп, не пізніше ніж на початку кожної зустрічі надають точні та повні заяви про будь-який інтерес, який можна вважати шкідливим для їхньої незалежності стосовно питань порядку денного, і утримуються від участі в обговоренні та голосуванні щодо таких питань.

3. ENISA встановлює у своєму внутрішньому регламенті практичні механізми, пов'язані з правилами надання заяв про інтереси, зазначені у параграфах 1 та 2.

Стаття 26

Прозорість

1. ENISA виконує свою діяльність з дотриманням високого рівня прозорості та відповідно до статті 28.

2. ENISA забезпечує надання громадськості та будь-яким заінтересованим сторонам відповідної об'єктивної, достовірної і доступної інформації, зокрема про результати своєї роботи. ENISA також оприлюднює заяви про інтереси, зроблені відповідно до статті 25.

3. Правління на пропозицію виконавчого директора може дозволити заінтересованим сторонам брати участь у певних видах діяльності ENISA як спостерігачам.

4. ENISA встановлює у своєму внутрішньому регламенті практичні заходи для імплементації правил прозорості, вказаних у параграфах 1 та 2.

Стаття 27

Конфіденційність

1. Без обмеження статті 28, ENISA не розголошує третім сторонам інформацію, яку воно опрацьовує або отримує та стосовно якої надійшов обґрунтований запит на конфіденційне використання.

2. Члени Правління, виконавчий директор, члени Консультативної групи ENISA, зовнішні експерти, які є учасниками спеціалізованих робочих груп, та члени персоналу ENISA, у тому числі посадові особи, прикомандировані державами-членами на тимчасовій основі, повинні дотримуватися вимог конфіденційності, передбачених статтею 339 ДФЄС, навіть після припинення виконання своїх обов'язків.

3. ENISA встановлює у своєму внутрішньому регламенті практичні механізми для імплементації правил конфіденційності, вказаних у параграфах 1 та 2.

4. Якщо цього вимагає виконання завдань ENISA, Правління ухвалює рішення дозволити ENISA працювати з секретною інформацією. У такому разі ENISA, за погодженням зі службами Комісії, ухвалює правила безпеки із застосуванням принципів безпеки, визначених у рішеннях Комісії (ЄС, Євратом) 2015/443 ([26]) та 2015/444 ([27]). Такі правила безпеки включають положення про обмін секретною інформацією, її опрацювання та зберігання.

Стаття 28

Доступ до документів

1. Регламент (ЄС) № 1049/2001 застосовується до документів у розпорядженні ENISA.

2. Правління ухвалює механізми імплементації Регламенту (ЄС) № 1049/2001 до 28 грудня 2019 року.

3. Рішення, ухвалені агентством ENISA відповідно до статті 8 Регламенту (ЄС) № 1049/2001, можуть бути оскаржені через Європейського Омбудсмана відповідно до статті 228 ДФЄС або можуть бути предметом позову в Суді Європейського Союзу відповідно до статті 263 ДФЄС.

ГЛАВА IV

Формування і структура бюджету ENISA

Стаття 29

Формування бюджету ENISA

1. Кожного року виконавчий директор складає проєкт кошторису доходів і видатків ENISA на наступний фінансовий рік і передає його Правлінню разом із проєктом бюджету. Доходи та видатки повинні бути збалансовані.

2. Кожного року Правління на основі проєкту кошторису доходів і видатків складає кошторис доходів і видатків ENISA на наступний фінансовий рік.

3. До 31 січня кожного року Правління надсилає кошторис доходів і видатків, який є частиною проєкту єдиного програмного документу, Комісії та третім країнам, із якими Союз уклав угоди, як зазначено у статті 42(2).

4. На основі кошторису Комісія включає в проєкт загального бюджету Союзу суми, які вона вважає необхідними для штатного розпису, та розмір внеску, який підлягає стягненню до загального бюджету Союзу, який вона подає Європейському Парламенту і Раді згідно зі статтею 314 ДФЄС.

5. Європейський Парламент і Рада надають дозвіл на виділення асигнувань для внеску Союзу в ENISA.

6. Європейський Парламент і Рада ухвалюють штатний розпис ENISA.

7. Правління ухвалює бюджет ENISA разом із єдиним програмним документом. Бюджет ENISA стає остаточним після остаточного ухвалення загального бюджету Союзу. У разі необхідності Правління вносить корегування до бюджету ENISA та до єдиного програмного документу відповідно до загального бюджету Союзу.

Стаття 30

Структура бюджету ENISA

1. Без обмеження інших ресурсів, дохід ENISA складається з:

(a) внеску із загального бюджету Союзу;

(b) доходу, призначеного на фінансування певних пунктів видатків відповідно до його фінансових правил, зазначених у статті 32;

(c) фінансування Союзу у формі угод про делегування або спеціалізованих цільових грантів згідно з фінансовими правилами, зазначеними в статті 32, та положеннями відповідних інструментів, що підтримують політику Союзу;

(d) внесків третіх країн, які беруть участь у роботі ENISA, як зазначено в статті 42;

(e) будь-яких добровільних внесків держав-членів у грошовій або натуральній формі.

Держави-члени, які надають добровільні внески, зазначені в пункті (e) першого підпараграфа, не повинні вимагати ніякого особливого права або послуги в результаті такого внеску.

2. Видатки ENISA включають оплату праці персоналу, видатки на адміністративну та технічну підтримку, інфраструктурні й оперативні видатки, а також видатки, що виникають унаслідок укладених із третіми сторонами контрактів.

Стаття 31

Виконання бюджету ENISA

1. Виконавчий директор відповідає за виконання бюджету ENISA.

2. Внутрішній аудитор Комісії виконує ті самі повноваження щодо ENISA, що й щодо інших департаментів Комісії.

3. Бухгалтер ENISA надсилає попередню фінансову звітність за фінансовий рік (рік N) бухгалтеру Комісії та Рахунковій палаті до 1 березня наступного фінансового року (рік N+1).

4. Отримавши застереження Рахункової палати до попередньої фінансової звітності ENISA відповідно до статті 246 Регламенту Європейського Парламенту і Ради (ЄС, Євратом) 2018/1046 ([28]), бухгалтер ENISA складає остаточну фінансову звітність ENISA під свою відповідальність і передає її Правлінню для отримання висновку.

5. Правління надає висновок щодо остаточної фінансової звітності ENISA.

6. До 31 березня року N+1 виконавчий директор передає звіт про бюджетне та фінансове управління Європейському Парламенту, Раді, Комісії та Рахунковій палаті.

7. До 1 липня року N+1 бухгалтер ENISA передає остаточну фінансову звітність ENISA Європейському Парламенту, Раді, бухгалтеру Комісії і Рахунковій палаті разом із висновком Правління.

8. У день передачі остаточної фінансової звітності ENISA бухгалтер ENISA також надсилає до Рахункової палати підсумковий лист стосовно такої остаточної фінансової звітності з копією для бухгалтера Комісії.

9. До 15 листопада року N+1 виконавчий директор оприлюднює остаточну фінансову звітність ENISA в *Офіційному віснику Європейського Союзу*.

10. До 30 вересня року N+1 виконавчий директор надсилає до Рахункової палати відповідь на її застереження, а також надсилає копію такої відповіді Правлінню та Комісії.

11. На запит Європейського Парламенту виконавчий директор надає йому будь-яку інформацію, необхідну для безперешкодного застосування процедури звільнення від відповідальності за виконання бюджету для відповідного фінансового року згідно зі статтею 261(3) Регламенту (ЄС, Євратом) 2018/1046.

12. За рекомендацією Ради Європейський Парламент звільняє виконавчого директора від відповідальності за виконання бюджету за рік N не пізніше 15 травня року N+2.

Стаття 32

Фінансові правила

Фінансові правила, застосовні до ENISA, ухвалює Правління після консультацій із Комісією. Такі фінансові правила не повинні відхилятися від Делегованого регламенту (ЄС) № 1271/2013, крім випадків, якщо таке відхилення є спеціальною вимогою для діяльності ENISA і Комісія заздалегідь дала на нього згоду.

Стаття 33

Боротьба з шахрайством

1. Для сприяння боротьбі з шахрайством, корупцією та іншою незаконною діяльністю відповідно до Регламенту Європейського Парламенту і Ради (ЄС, Євратом) № 883/2013 ([29]), ENISA повинне до 28 грудня 2019 року приєднатися до Міжінституційної угоди між Європейським Парламентом, Радою Європейського Союзу і Комісією Європейських Співтовариств від 25 травня 1999 року щодо внутрішніх розслідувань Європейського бюро боротьби із шахрайством (OLAF) ([30]). ENISA повинне ухвалити відповідні положення, застосовні до всіх працівників ENISA, із використанням зразка, визначеного в додатку до зазначеної Угоди.

2. Рахункова палата має повноваження проводити аудит, на підставі документів та виїзних інспектувань, усіх бенефіціарів грантів, підрядників і субпідрядників, які отримали кошти Союзу від ENISA.

3. Європейське бюро боротьби із шахрайством може проводити розслідування, у тому числі виїзні перевірки та інспектування, відповідно до положень і процедур, установлених у Регламенті (ЄС, Євратом) № 883/2013 та Регламенті Ради (Євратом, ЄС) № 2185/96 ([31]), з метою встановлення факту шахрайства, корупції або будь-якої іншої незаконної діяльності, що негативно впливає на фінансові інтереси Союзу, у зв'язку з грантом або договором, що фінансується ENISA.

4. Без обмеження параграфів 1, 2 і 3 угоди про співпрацю з третіми країнами або міжнародними організаціями, договори, грантові угоди та грантові рішення ENISA повинні містити положення, які прямо уповноважують Рахункову палату та Європейське бюро боротьби із шахрайством проводити такі аудити й розслідування відповідно до їхніх компетенцій.

ГЛАВА V

Персонал

Стаття 34

Загальні положення

До персоналу ENISA застосовуються Положення про персонал та Умови працевлаштування інших службовців, а також правила, ухвалені угодою між установами Союзу для реалізації Положення про персонал та Умов працевлаштування інших службовців.

Стаття 35

Привілеї та імунітет

До ENISA та його персоналу застосовується Протокол № 7 про привілеї та імунітети Європейського Союзу, долучений до Договору про Європейський Союз та до Договору про функціонування Європейського Союзу (ДФЄС).

Стаття 36

Виконавчий директор

1. Виконавчого директора залучають як тимчасового агента ENISA відповідно до пункту (a) статті 2 Умов працевлаштування інших службовців.

2. Виконавчого директора призначає Правління зі списку кандидатів, запропонованих Комісією, на підставі відкритої та прозорої процедури відбору.

3. Для цілей укладення трудового договору з виконавчим директором, ENISA представлене головою Правління.

4. Перед призначенням обраного Правлінням кандидата запрошують зробити заяву перед відповідним комітетом Європейського Парламенту та відповісти на запитання його членів.

5. Строк перебування на посаді виконавчого директора становить п’ять років. По закінченню зазначеного строку Комісія проводить оцінювання діяльності виконавчого директора та майбутніх завдань і викликів ENISA.

6. Правління ухвалює рішення про призначення, подовження строку перебування на посаді або звільнення з посади виконавчого директора відповідно до статті 18(2).

7. Правління, діючи за пропозицією Комісії, яка враховує оцінювання, зазначене в параграфі 5, може одноразово подовжити строк дії повноважень виконавчого директора ще на п’ять років.

8. Правління інформує Європейський Парламент про свій намір подовжити строк дії повноважень виконавчого директора. За три місяці до такого подовження дії повноважень виконавчого директора можуть запросити зробити заяву перед відповідним комітетом Європейського Парламенту і дати відповіді на запитання його членів.

9. Виконавчий директор, строк дії повноважень якого було подовжено, не може брати участі в наступній процедурі відбору на таку саму посаду.

10. Виконавчого директора можуть звільнити з посади тільки за рішенням Правління, яке діє на підставі пропозиції Комісії.

Стаття 37

Прикомандировані національні експерти та інший персонал

1. ENISA може залучати прикомандированих національних експертів або інший персонал, який не працює в ENISA. Положення про персонал та Умови працевлаштування інших службовців до такого персоналу не застосовуються.

2. Правління ухвалює рішення, у якому встановлює правила прикомандирування національних експертів до ENISA.

ГЛАВА VI

Загальні положення, що стосуються ENISA

Стаття 38

Правовий статус ENISA

1. ENISA є органом Союзу й має правосуб'єктність.

2. У кожній державі-члені ENISA користується найширшою правоздатністю, що надається юридичним особам відповідно до національного права. ENISA може, зокрема, набувати або розпоряджатися рухомим та нерухомим майном і виступати учасником судових проваджень.

3. Представництво ENISA здійснює його виконавчий директор.

Стаття 39

Відповідальність ENISA

1. Договірну відповідальність ENISA регулює право, застосовне до відповідного договору.

2. Суд Європейського Союзу має юрисдикцію ухвалювати рішення відповідно до будь-якого арбітражного застереження, що міститься в договорі, укладеному ENISA.

3. У разі недоговірної відповідальності ENISA відшкодовує будь-які збитки, завдані ним або його персоналом під час виконання ними своїх службових обов'язків, відповідно до загальних принципів, які є спільними для права держав-членів.

4. Суд Європейського Союзу має юрисдикцію щодо розгляду будь-якого спору, пов'язаного з відшкодуванням збитків, як зазначено в параграфі 3.

5. Особисту відповідальність персоналу ENISA перед ENISA визначають відповідні умови, що застосовуються до персоналу ENISA.

Стаття 40

Положення щодо мов

1. До ENISA застосовуються положення Регламенту Ради № 1 ([32]). Держави-члени та інші органи, призначені державами-членами, можуть звертатися до ENISA та отримувати відповідь офіційною мовою обраних ними установ Союзу.

2. Послуги з перекладу, необхідні для функціонування ENISA, надає Центр перекладу для органів Європейського Союзу.

Стаття 41

Захист персональних даних

1. Опрацювання персональних даних агентством ENISA підпадає під дію Регламенту (ЄС) 2018/1725.

2. Правління ухвалює імплементаційні правила, як зазначено в статті 45(3) Регламенту (ЄС) 2018/1725. Правління може ухвалювати додаткові заходи, необхідні для застосування ENISA Регламенту (ЄС) 2018/1725.

Стаття 42

Співпраця з третіми країнами та міжнародними організаціями

1. Наскільки це необхідно для досягнення цілей, визначених у цьому Регламенті, ENISA може співпрацювати з компетентними органами третіх країн та міжнародними організаціями. Для цього ENISA може укладати робочі угоди з органами третіх країн та міжнародними організаціями за умови попереднього схвалення Комісії. Такі робочі угоди не створюють юридичних зобов'язань для Союзу і його держав-членів.

2. ENISA відкрите для участі третіх країн, які уклали угоди з Союзом про таку участь. Згідно з відповідними положеннями таких угод відбувається укладання робочих угод, у яких, зокрема, визначаються характер, обсяг та спосіб участі таких третіх країн у роботі ENISA, і вони повинні включати положення, що стосуються участі в ініціативах ENISA, фінансових внесків та персоналу.

Стосовно персоналу, такі робочі угоди в будь-якому разі повинні відповідати Положенню про персонал та Умовам працевлаштування інших службовців.

3. Правління ухвалює стратегію щодо відносин із третіми країнами та міжнародними організаціями в питаннях, що належать до компетенції ENISA. Комісія забезпечує діяльність ENISA в межах свого мандата та наявних інституційних рамок шляхом укладення відповідних робочих угод з виконавчим директором.

Стаття 43

Правила безпеки щодо захисту чутливої незасекреченої та секретної інформації

Після консультацій з Комісією ENISA ухвалює правила безпеки, застосовуючи принципи безпеки, які містяться у правилах безпеки Комісії для захисту чутливої незасекреченої інформації та EUCI (секретної інформації Європейського Союзу), як визначено в рішеннях (ЄС, Євратом) 2015/443 та 2015/444. Правила безпеки ENISA включають положення про обмін такою інформацією, її опрацювання та зберігання.

Стаття 44

Угода про штаб-квартиру та умови функціонування

1. Необхідні домовленості стосовно розміщення, передбаченого для ENISA в державі-члені ведення діяльності, та обладнання, яке буде надано такою державою-членом, разом зі спеціальними правилами, застосовними в державі-члені ведення діяльності до виконавчого директора, членів Правління, персоналу ENISA та членів їхніх родин, повинні бути встановлені в угоді про штаб-квартиру, укладеній між ENISA і державою-членом ведення діяльності після отримання схвалення Правління.

2. Держава-член ведення діяльності ENISA надає найкращі умови для забезпечення належної діяльності ENISA з урахуванням доступності розташування, наявності належних закладів освіти для дітей працівників персоналу, належного доступу до ринку праці, соціального захисту та медичного обслуговування для дітей та дружин/чоловіків працівників персоналу.

Стаття 45

Адміністративний контроль

Європейський Омбудсман здійснює нагляд за діяльністю ENISA відповідно до статті 228 ДФЄС.

РОЗДІЛ III
РАМКИ СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ

Стаття 46

Європейські рамки сертифікації кібербезпеки

1. Європейські рамки сертифікації кібербезпеки створено для покращення умов функціонування внутрішнього ринку шляхом підвищення рівня кібербезпеки на території Союзу та впровадження гармонізованого підходу на рівні Союзу до європейських схем сертифікації кібербезпеки з метою створення єдиного цифрового ринку продуктів ІКТ, послуг ІКТ та процесів ІКТ.

2. Європейські рамки сертифікації кібербезпеки надають механізм для створення європейських схем сертифікації кібербезпеки та підтвердження того, що продукти ІКТ, послуги ІКТ та процеси ІКТ оцінили відповідно до схем, які відповідають зазначеним вимогам безпеки, з метою захисту доступності, автентичності, цілісності або конфіденційності даних, які зберігають, передають або опрацьовують, або функцій чи послуг, пропонованих такими продуктами, послугами або процесами або доступних з їхньою допомогою протягом їхнього життєвого циклу.

Стаття 47

Послідовна робоча програма Союзу для європейської сертифікації кібербезпеки

1. Комісія оприлюднює послідовну робочу програму Союзу для європейської сертифікації кібербезпеки («послідовна робоча програма Союзу»), яка визначає стратегічні пріоритети для майбутніх європейських систем сертифікації кібербезпеки.

2. Послідовна робоча програма Союзу, зокрема, включає список продуктів ІКТ, послуг ІКТ та процесів ІКТ або їхніх категорій, які можуть отримати користь від включення в рамки європейської схеми сертифікації кібербезпеки.

3. Включення певних продуктів ІКТ, послуг ІКТ та процесів ІКТ або їхніх категорій до послідовної робочої програми Союзу обґрунтовують на основі однієї або більше таких підстав:

(a) доступність та розробка національних схем сертифікації кібербезпеки, які охоплюють певну категорію продуктів ІКТ, послуг ІКТ та процесів ІКТ, та зокрема тих, що стосуються ризику фрагментації;

(b) відповідні право або політика Союзу або держави-члена;

(c) ринковий попит;

(d) розробки у вивченні кіберзагроз;

(e) запит на підготовку конкретного проєкту схеми ECCG.

4. Комісія повинна належним чином враховувати висновки, надані ECCG та Групою стейкхолдерів з питань сертифікації стосовно проєкту послідовної робочої програми Союзу.

5. Перша послідовна робоча програма Союзу повинна бути оприлюднена до 28 червня 2020 року. Послідовну робочу програму Союзу належить оновлювати принаймні один раз на три роки або, якщо необхідно, частіше.

Стаття 48

Запит на європейську схему сертифікації кібербезпеки

1. Комісія може подавати запит ENISA на підготовку проєкту схеми або на перегляд наявної європейської схеми сертифікації кібербезпеки на основі послідовної робочої програми Союзу.

2. У належним чином обґрунтованих випадках Комісія або ECCG може подавати запит ENISA на підготовку проєкту схеми або на перегляд наявної європейської схеми сертифікації кібербезпеки, не включеної до послідовної робочої програми Союзу. Послідовну робочу програму Союзу належить оновлювати відповідним чином.

Стаття 49

Підготовка, ухвалення та перегляд європейської схеми сертифікації кібербезпеки

1. На запит Комісії відповідно до статті 48 ENISA готує проєкт схеми, що відповідає вимогам, визначеним у статтях 51, 52 та 54.

2. На запит ECCG відповідно до статті 48(2) ENISA готує проєкт схеми, що відповідає вимогам, визначеним у статтях 51, 52 та 54. Якщо ENISA відхиляє такий запит, ENISA повинне обґрунтувати свою відмову. Будь-яке рішення про відхилення такого запиту ухвалює Правління.

3. Під час підготовки проєкту схеми ENISA консультується з усіма відповідними стейкхолдерами в рамках офіційного, відкритого, прозорого та інклюзивного консультаційного процесу.

4. ENISA створює спеціалізовану експерту робочу групу для кожного проєкту схеми відповідно до статті 20(4) для надання ENISA відповідних консультацій та експертних знань.

5. ENISA тісно співпрацює з ECCG. ECCG надає ENISA допомогу та експертні консультації стосовно підготовки проєкту схеми та ухвалює висновок щодо проєкту схеми.

6. ENISA максимально враховує висновок ECCG перед передачею Комісії проєкту схеми, підготованого відповідно до параграфів 3, 4 та 5. Висновок ECCG не має зобов'язального характеру, і відсутність такого висновку не повинна перешкодити ENISA передати проєкт схеми Комісії.

7. На основі підготованого ENISA проєкту схеми Комісія може ухвалювати імплементаційні акти, що встановлюють європейську схему сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ, яка відповідає вимогам, визначеним у статтях 51, 52 та 54. Такі імплементаційні акти ухвалюють згідно з експертною процедурою, зазначеною в статті 66(2).

8. Принаймні кожні п'ять років ENISA повинне оцінювати кожну ухвалену європейську схему сертифікації кібербезпеки з урахуванням зворотного зв'язку від заінтересованих сторін. У разі необхідності Комісія або ECCG можуть подавати ENISA запит на початок процесу розробки переглянутого проєкту схеми відповідно до статті 48 та цієї статті.

Стаття 50

Вебсайт європейських схем сертифікації кібербезпеки

1. ENISA повинне вести спеціальний вебсайт, на якому повинне надавати інформацію про та оприлюднювати європейські схеми сертифікації кібербезпеки, європейські сертифікати з кібербезпеки та декларації ЄС про відповідність, у тому числі інформацію, що стосується уже недійсних європейських схем сертифікації кібербезпеки, європейських сертифікатів з кібербезпеки та декларацій ЄС про відповідність, які були вилучені або які втратили чинність, та репозиторій покликань на інформацію стосовно кібербезпеки, надану відповідно до статті 55.

2. Якщо застосовно, на вебсайті, вказаному в параграфі 1, повинні вказуватися національні схеми сертифікації кібербезпеки, які замінено європейською схемою сертифікації кібербезпеки.

Стаття 51

Цілі безпеки європейських схем сертифікації кібербезпеки

Європейська схема сертифікації кібербезпеки призначена досягати, у застосовних випадках, принаймні таких цілей безпеки:

(a) захищати дані, які зберігають, передають або по-іншому опрацьовують, від несанкціонованого зберігання, опрацювання, доступу або розкриття протягом усього життєвого циклу продукту ІКТ, послуги ІКТ або процесу ІКТ;

(b) захищати дані, які зберігають, передають або по-іншому опрацьовують, від випадкового або несанкціонованого знищення, втрати, зміни або недоступності протягом усього життєвого циклу продукту ІКТ, послуги ІКТ або процесу ІКТ;

(c) гарантувати, що уповноважені особи, програми або механізми можуть мати доступ лише до тих даних, послуг або функцій, які вказані в їхніх правах доступу;

(d) ідентифікувати та документувати відомі залежності та вразливості;

(e) реєструвати, до яких даних, послуг або функцій отримали доступ, які з них використовували або по-іншому опрацьовували, хто це робив та коли;

(f) уможливити перевірку того, до яких даних, послуг або функцій отримали доступ, які з них використовували або по-іншому опрацьовували, хто це робив та коли;

(g) перевіряти, що продукти ІКТ, послуги ІКТ та процеси ІКТ не містять відомих вразливостей;

(h) вчасно відновлювати наявність і доступ до даних та функцій у разі фізичного або технічного інциденту;

(i) гарантувати безпеку продуктів ІКТ, послуг ІКТ та процесів ІКТ за замовчуванням та за призначенням;

(j) гарантувати, що продукти ІКТ, послуги ІКТ та процеси ІКТ забезпечені актуальним програмним та апаратним забезпеченням, яке не містить широковідомих вразливостей, та забезпечені механізмами для безпечних оновлень.

Стаття 52

Рівні надійності європейських схем сертифікації кібербезпеки

1. Європейська схема сертифікації кібербезпеки може визначати один або більше з таких рівнів надійності для продуктів ІКТ, послуг ІКТ та процесів ІКТ: «базовий», «істотний» або «високий». Рівень надійності повинен відповідати рівню ризику, пов'язаному з використанням за призначенням продукту ІКТ, послуги ІКТ або процесу ІКТ, з точки зору ймовірності та впливу інциденту.

2. У європейських сертифікатах з кібербезпеки та деклараціях ЄС про відповідність вказують будь-який рівень надійності, визначений у європейській схемі сертифікації кібербезпеки, відповідно до якої було видано європейський сертифікат з кібербезпеки або декларацію ЄС про відповідність.

3. Вимоги безпеки, що відповідають кожному рівню надійності, повинні бути вказані у відповідній європейській схемі сертифікації кібербезпеки, включно з відповідними функціональними можливостями безпеки та суворістю й глибиною оцінювання, якому підлягатиме такий продукт ІКТ, послуга ІКТ або процес ІКТ.

4. У сертифікаті або декларації ЄС про відповідність вказують технічні специфікації, стандарти та процедури, у тому числі технічні контролі, мета яких полягає у зниженні ризику виникнення інцидентів кібербезпеки або запобіганні таким інцидентам.

5. Європейський сертифікат з кібербезпеки або декларація ЄС про відповідність, де вказано «базовий» рівень надійності, гарантує, що продукти ІКТ, послуги ІКТ та процеси ІКТ, для яких видано такий сертифікат або декларацію ЄС про відповідність, відповідають вимогам безпеки, у тому числі функціональним можливостям безпеки, і що їх було оцінено на рівні, спрямованому на мінімізацію відомих базових ризиків інцидентів та кібератак. Заходи з оцінювання, які будуть проведені, повинні включати принаймні перегляд технічної документації. Якщо такий перегляд не є доцільним, його заміняють заходами з оцінювання з рівнозначним ефектом.

6. Європейський сертифікат з кібербезпеки, у якому вказано «істотний» рівень надійності, гарантує, що продукти ІКТ, послуги ІКТ та процеси ІКТ, для яких видано такий сертифікат, відповідають вимогам безпеки, у тому числі функціональним можливостям безпеки, і що їх було оцінено на рівні, спрямованому на мінімізацію відомих ризиків, пов'язаних із кібербезпекою, а також ризиків виникнення інцидентів та кібератак, які виконують суб'єкти з обмеженими вміннями та ресурсами. Заходи з оцінювання, які будуть проведені, повинні включати принаймні таке: перегляд для підтвердження відсутності широковідомих вразливостей та тестування для підтвердження того, що продукти ІКТ, послуги ІКТ або процеси ІКТ належним чином реалізують необхідні функціональні можливості безпеки. Якщо такі заходи з оцінювання не є доцільними, їх заміняють заходами з оцінювання з рівнозначним ефектом.

7. Європейський сертифікат з кібербезпеки, у якому вказано «високий» рівень надійності, гарантує, що продукти ІКТ, послуги ІКТ та процеси ІКТ, для яких видано такий сертифікат, відповідають вимогам безпеки, у тому числі функціональним можливостям безпеки, і що їх було оцінено на рівні, спрямованому на мінімізацію ризиків передових кібератак, які виконують суб'єкти зі значними вміннями та ресурсами. Заходи з оцінювання, які будуть проведені, повинні включати принаймні таке: перегляд для підтвердження відсутності широковідомих вразливостей; тестування для підтвердження того, що продукти ІКТ, послуги ІКТ та процеси ІКТ реалізують необхідні функціональні можливості безпеки на високому рівні; та оцінювання рівня їхнього опору досвідченим нападникам з

використанням тестування проникненням. Якщо такі заходи з оцінювання не є доцільними, їх заміняють заходами з рівнозначним ефектом.

8. У європейській схемі сертифікації кібербезпеки може бути визначено декілька рівнів оцінювання, залежно від суворості та глибини використовуваних методів оцінювання. Кожен рівень оцінювання повинен відповідати одному з рівнів надійності та визначатися відповідною комбінацією компонентів надійності.

Стаття 53

Самооцінювання відповідності

1. Європейська схема сертифікації кібербезпеки може уможливлювати самооцінювання відповідності під одноосібну відповідальність виробника або надавача продуктів ІКТ, послуг ІКТ або процесів ІКТ. Дозвіл на самооцінювання відповідності надають лише стосовно продуктів ІКТ, послуг ІКТ та процесів ІКТ з низьким рівнем ризику, що відповідає «низькому» рівню надійності.

2. Виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ може видавати декларацію ЄС про відповідність, у якій заявляє про виконання всіх вимог, визначених у схемі. У разі оформлення такої декларації виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ бере на себе відповідальність за відповідність продуктів ІКТ, послуг ІКТ або процесів ІКТ вимогам, визначеним у схемі.

3. Виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ надає доступ до декларації ЄС про відповідність, технічної документації та іншої відповідної інформації, що стосується відповідності продуктів ІКТ, послуг ІКТ або процесів ІКТ схемі, національному органу з сертифікації кібербезпеки, зазначеному в статті 58, на строк, визначений у відповідній європейській схемі сертифікації кібербезпеки. Копію декларації ЄС про відповідність вимогам надають національним органам із сертифікації кібербезпеки та ENISA.

4. Видача декларації ЄС про відповідність є добровільною, якщо інше не визначено у праві Союзу або держави-члена.

5. Декларації ЄС про відповідність повинні визнаватися у всіх державах-членах.

Стаття 54

Елементи європейських схем сертифікації кібербезпеки

1. Європейська схема сертифікації кібербезпеки включає принаймні такі елементи:

(a) предмет і сферу застосування схеми сертифікації, у тому числі тип або категорії охоплених продуктів ІКТ, послуг ІКТ та процесів ІКТ;

(b) чіткий опис мети схеми та відповідності обраних стандартів, методів оцінювання та рівнів надійності потребам цільових користувачів схеми;

(c) покликання на міжнародні, європейські або національні стандарти, які були застосовані під час оцінювання, або, якщо такі стандарти недоступні або недоцільні, технічні специфікації, які відповідають вимогам, визначеним у додатку II до Регламенту (ЄС) № 1025/2012, або, якщо такі специфікації недоступні, технічні специфікації чи інші вимоги кібербезпеки, визначені в європейській схемі сертифікації кібербезпеки;

(d) якщо застосовно, один або більше рівнів надійності;

(e) зазначення, чи дозволене самооцінювання відповідності згідно зі схемою;

(f) якщо застосовно, конкретні або додаткові вимоги, застосовні до органів з оцінювання відповідності, для гарантування їхньої технічної компетентності в оцінюванні вимог кібербезпеки;

(g) конкретні критерії та методи оцінювання, включаючи типи оцінювання, які будуть застосовані для підтвердження того, що цілей, зазначених у статті 51, досягнуто;

(h) якщо застосовно, необхідну для сертифікації інформацію, яку заявник повинен надіслати або іншим способом надати органам з оцінювання відповідності;

(i) якщо схема передбачає маркування або етикетки, умови, за яких можна використовувати такі маркування або етикетки;

(j) правила для моніторингу відповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ вимогам європейських сертифікатів з кібербезпеки або декларацій ЄС про відповідність, включаючи механізми, що демонструють безперервне дотримання визначених вимог із кібербезпеки;

(k) якщо застосовно, умови видачі, підтримання, подовження дії та поновлення європейських сертифікатів з кібербезпеки, а також умови розширення або зменшення обсягу сертифікації;

(l) правила стосовно наслідків для продуктів ІКТ, послуг ІКТ та процесів ІКТ, для яких видали сертифікат або декларацію ЄС про відповідність, але які не відповідають вимогам схеми;

(m) правила стосовно того, як звітувати про раніше невиявлені вразливості кібербезпеки у продуктах ІКТ, послугах ІКТ та процесах ІКТ та як вирішувати таку проблему;

(n) якщо застосовно, правила зберігання документації органами з оцінювання відповідності;

(o) ідентифікацію національних або міжнародних схем сертифікації кібербезпеки, що охоплюють однакові тип або категорії продуктів ІКТ, послуг ІКТ та процесів ІКТ, вимоги безпеки, критерії та методи оцінювання та рівні надійності;

(p) зміст та формат європейських сертифікатів з кібербезпеки та декларацій ЄС про відповідність, які будуть видані;

(q) період, протягом якого доступні декларація ЄС про відповідність та технічна документація та протягом якого виробник або надавач продуктів ІКТ, послуг ІКТ або процесів ІКТ надає доступ до іншої відповідної інформації;

(r) максимальний період, протягом якого дійсні видані відповідно до схеми європейські сертифікати з кібербезпеки;

(s) політику розкриття інформації стосовно європейських сертифікатів з кібербезпеки, які видали, до яких вносили зміни або які вилучили відповідно до схеми;

(t) умови для взаємного визнання схем сертифікацій із третіми країнами;

(u) якщо застосовно, правила стосовно будь-якого механізму партнерського оцінювання, встановленого схемою для органів, що видають європейські сертифікати з кібербезпеки, у яких вказано «високий» рівень надійності, відповідно до статті 56(6). Такий механізм не обмежує партнерської перевірки, зазначеної у статті 59;

(v) формат та процедури, яких повинні дотримуватися виробники або надавачі продуктів ІКТ, послуг ІКТ або процесів ІКТ під час надання та оновлення додаткової інформації про кібербезпеку відповідно до статті 55.

2. Визначені вимоги європейської схеми сертифікації кібербезпеки повинні відповідати будь-яким застосовним правовим вимогам, зокрема вимогам, визначеним у гармонізованому законодавстві Союзу.

3. Якщо таке передбачено у конкретному правовому акті Союзу, сертифікат або декларація ЄС про відповідність, видані відповідно до європейської схеми сертифікації кібербезпеки, можуть бути використані для підтвердження презумпції відповідності вимогам такого правового акта.

4. У разі відсутності гармонізованого законодавства Союзу законодавство держави-члена може передбачати використання європейської схеми сертифікації кібербезпеки для встановлення презумпції відповідності правовим вимогам.

Стаття 55

Додаткова інформація з питань забезпечення кібербезпеки стосовно сертифікованих продуктів ІКТ, послуг ІКТ та процесів ІКТ

1. Виробник або надавач сертифікованих продуктів ІКТ, послуг ІКТ або процесів ІКТ чи продуктів ІКТ, послуг ІКТ або процесів ІКТ, для яких було видано декларацію ЄС про відповідність, оприлюднює таку додаткову інформацію щодо кібербезпеки:

(a) настанови та рекомендації, що допомагають користувачам безпечно конфігурувати, встановлювати, розгортати, експлуатувати та обслуговувати продукти ІКТ або послуги ІКТ;

(b) період, під час якого кінцевим користувачам буде надана підтримка з безпеки, зокрема щодо наявності пов'язаних із кібербезпекою оновлень;

(c) контактні дані виробника або надавача та погоджені методи отримання інформації про вразливість від користувачів та дослідників у сфері забезпечення інформаційної безпеки;

(d) покликання на онлайн-репозиторії зі списком оприлюднених вразливостей, що стосуються продукту ІКТ, послуги ІКТ або процесу ІКТ та будь-яких відповідних рекомендацій.

2. Інформація, зазначена в параграфі 1, повинна бути доступною в електронному форматі та повинна залишатися доступною й оновлюватися принаймні до завершення дії відповідного європейського сертифіката з кібербезпеки або декларації ЄС про відповідність.

Стаття 56

Сертифікація кібербезпеки

1. Продукти ІКТ, послуги ІКТ та процеси ІКТ, які були сертифіковані за європейською схемою сертифікації кібербезпеки, ухваленою відповідно до статті 49, вважаються такими, що відповідають вимогам такої схеми.

2. Сертифікація кібербезпеки є добровільною, якщо інше не зазначено в законодавстві Союзу або держави-члена.

3. Комісія регулярно оцінює ефективність та використання ухвалених європейських схем сертифікації кібербезпеки та оцінює, чи конкретна європейська схема сертифікації кібербезпеки повинна стати обов'язковою за допомогою відповідного законодавства Союзу для забезпечення належного рівня кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ в Союзі та покращення функціонування внутрішнього ринку. Перше таке оцінювання повинне бути проведене до 31 грудня 2023 року, а подальші оцінювання повинні проводитися принаймні кожні два роки. На основі результатів таких оцінювань Комісія повинна ідентифікувати продукти ІКТ, послуги ІКТ та процеси ІКТ, які охоплює наявна схема сертифікації та які повинна охоплювати обов'язкова схема сертифікації.

У першу чергу Комісія повинна зосередити увагу на галузях, перерахованих у додатку II до Директиви (ЄС) 2016/1148, які слід оцінити не пізніше двох років після ухвалення першої європейської схеми сертифікації кібербезпеки.

Під час підготування оцінювання Комісія:

(a) враховує вплив заходів на виробників або надавачів таких продуктів ІКТ, послуг ІКТ або процесів ІКТ та на користувачів з точки зору витрат на такі заходи та суспільних або економічних вигід від очікуваного підвищення рівня безпеки продуктів ІКТ, послуг ІКТ або процесів ІКТ;

(b) враховує існування та імплементацію відповідного законодавства держав-членів та третіх країн;

(c) проводить відкритий, прозорий та інклюзивний процес консультування з усіма відповідними стейкхолдерами та державами-членами;

(d) враховує терміни імплементації, перехідні положення та періоди, зокрема пов'язані з можливим впливом заходу на виробників або надавачів продуктів ІКТ, послуг ІКТ або процесів ІКТ, у тому числі МСП;

(e) пропонує найбільш швидкий та ефективний спосіб переходу від обов'язкових до добровільних схем сертифікації.

4. Органи з оцінювання відповідності, зазначені в статті 60, видають європейські сертифікати з кібербезпеки відповідно до цієї статті, у яких вказано рівень безпеки «базовий» або «істотний», на основі критеріїв, що входять до європейської схеми сертифікації кібербезпеки, ухваленої Комісією відповідно до статті 49.

5. Як відступ від параграфа 4, у належно обґрунтованих випадках європейська схема сертифікації кібербезпеки може передбачати, що європейські сертифікати з кібербезпеки, які є результатом такої схеми, повинні видаватися лише органом публічної влади. Таким органом повинен бути один із таких:

(a) національний орган з сертифікації кібербезпеки, як зазначено у статті 58(1); або

(b) орган публічної влади, акредитований як орган з оцінювання відповідності відповідно до статті 60(1).

6. Якщо європейська схема сертифікації кібербезпеки, ухвалена відповідно до статті 49, вимагає «високого» рівня надійності, європейський сертифікат з кібербезпеки в рамках такої схеми видається лише національним органом з сертифікації кібербезпеки або, у таких випадках, органом з оцінювання відповідності:

(a) після попереднього схвалення національним органом з сертифікації кібербезпеки кожного окремого європейського сертифіката з кібербезпеки, виданого органом з оцінювання відповідності; або

(b) на основі загального делегування завдання з видачі таких європейських сертифікатів з кібербезпеки національним органом з сертифікації кібербезпеки органу з оцінювання відповідності.

7. Фізична або юридична особа, яка подає на сертифікацію продукти ІКТ, послуги ІКТ або процеси ІКТ, надає національному органу з сертифікації кібербезпеки, зазначеному в статті 58, якщо це орган, що видає європейський сертифікат з кібербезпеки, або органу з оцінювання відповідності, зазначеному в статті 60, усю необхідну для проведення сертифікації інформацію.

8. Держатель європейського сертифіката з кібербезпеки повідомляє органу, зазначеному в параграфі 7, про будь-які виявлені в подальшому вразливості або порушення стосовно безпеки сертифікованого продукту ІКТ, послуги ІКТ або процесу ІКТ, які можуть впливати на їхню відповідність вимогам, пов'язаним із сертифікацією. Такий орган без невиправданої затримки пересилає таку інформацію відповідному національному органу сертифікації кібербезпеки.

9. Європейський сертифікат з кібербезпеки видають на період, передбачений у європейській схемі сертифікації кібербезпеки, та його можна поновити за умови подальшого виконання відповідних вимог.

10. Європейський сертифікат з кібербезпеки, виданий відповідно до цієї статті, визнають в усіх державах-членах.

Стаття 57

Національні схеми сертифікації кібербезпеки та національні сертифікати з кібербезпеки

1. Без обмеження параграфа 3 цієї статті, національні схеми сертифікації кібербезпеки та пов'язані процедури для продуктів ІКТ, послуг ІКТ та процесів ІКТ, які охоплює європейська схема сертифікації кібербезпеки, втрачають юридичну силу з дати, встановленої в імплементаційному акті, ухваленому відповідно до статті 49(7). Національні схеми сертифікації кібербезпеки та пов'язані процедури для продуктів ІКТ, послуг ІКТ та процесів ІКТ, які не охоплює європейська схема сертифікації кібербезпеки, продовжують існувати.

2. Держави-члени не вводять нових національних схем сертифікації кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ, які вже охоплені чинною європейською схемою сертифікації кібербезпеки.

3. Наявні сертифікати, видані за національними схемами сертифікації кібербезпеки, охоплені європейською схемою сертифікації кібербезпеки, залишаються дійсними до закінчення терміну їхньої

дії.

4. З метою уникнення фрагментації внутрішнього ринку держави-члени інформують Комісію та ECCG про будь-які наміри створити нові національні схеми сертифікації кібербезпеки.

Стаття 58

Національні органи з сертифікації кібербезпеки

1. Кожна держава-член призначає один або більше національних органів з сертифікації кібербезпеки на своїй території або, за згодою іншої держави-члена, призначає один або більше національних органів з сертифікації кібербезпеки, створених у такій іншій державі-члені, відповідальним за завдання з нагляду в державі-члені, яка призначила такий орган.

2. Кожна держава-член інформує Комісію про призначені національні органи з сертифікації кібербезпеки. Якщо держава-член призначає більше ніж один орган, вона також інформує Комісію про завдання, покладені на кожен з таких органів.

3. Без обмеження пункту (a) статті 56(5) та статті 56(6), кожен національний орган з сертифікації кібербезпеки є незалежним від суб'єктів, за якими він здійснює нагляд, у питаннях своєї організації, рішень про фінансування, організаційно-правової форми та вироблення й ухвалення рішень.

4. Держави-члени забезпечують чіткий поділ діяльності національних органів з сертифікації кібербезпеки, яка стосується випуску європейських сертифікатів з кібербезпеки, зазначеного в пункті (a) статті 56(5) та в статті 56(6), та їхньої наглядової діяльності, визначеної в цій статті, та забезпечують виконання цих двох видів діяльності незалежно один від одного.

5. Держави-члени забезпечують наявність у національних органів з сертифікації кібербезпеки належних ресурсів для здійснення їхніх повноважень та виконання їхніх завдань у результативний та ефективний спосіб.

6. Для ефективної імплементації цього Регламенту доцільно, щоб національні органи з сертифікації кібербезпеки брали участь в роботі ECCG активно, ефективно та у безпечний спосіб.

7. Національні органи з сертифікації кібербезпеки:

(a) здійснюють контроль та забезпечують дотримання правил, включених до європейських схем сертифікації кібербезпеки відповідно до пункту (j) статті 54(1), для моніторингу відповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ вимогам європейських сертифікатів з кібербезпеки, виданих на відповідних територіях, у співпраці з іншими відповідними органами ринкового нагляду;

(b) здійснюють моніторинг та забезпечують виконання обов'язків виробників або надавачів продуктів ІКТ, послуг ІКТ або процесів ІКТ, які створені на їхніх відповідних територіях та які проводять самоперевірку на відповідність, та зокрема здійснюють моніторинг та забезпечують виконання обов'язків таких виробників або надавачів, визначених у статті 53(2) та (3) та у відповідній європейській схемі сертифікації кібербезпеки;

(c) без обмеження статті 60(3) активно надають допомогу національним органам з акредитації в моніторингу та нагляді за діяльністю органів з оцінювання відповідності для цілей цього Регламенту;

(d) здійснюють моніторинг і нагляд за діяльністю органів публічної влади, зазначених у статті 56(5);

(e) якщо застосовно, уповноважують органи з оцінювання відповідності згідно зі статтею 60(3) та обмежують, призупиняють або відкликають наявний дозвіл, якщо органи з оцінювання відповідності порушують вимоги цього Регламенту;

(f) розглядають скарги фізичних або юридичних осіб, пов'язані з європейськими сертифікатами з кібербезпеки, виданими національними органами з сертифікації кібербезпеки, або з європейськими сертифікатами з кібербезпеки, виданими органами з оцінювання відповідності відповідно до

статті 56(6), або пов’язані з деклараціями ЄС про відповідність, виданими відповідно до статті 53, розслідують предмет таких скарг у належній мірі та інформують скаржника про хід і результат розслідування протягом розумного строку;

(g) надають ENISA та ECCG щорічний підсумковий звіт щодо діяльності, проведеної відповідно до пунктів (b), (c) та (d) або відповідно до параграфа 8;

(h) співпрацюють з іншими національними органами сертифікації кібербезпеки або іншими органами публічної влади, у тому числі шляхом поширення інформації щодо можливої невідповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ вимогам цього Регламенту або вимогам конкретних європейських схем сертифікації кібербезпеки; та

(i) проводять моніторинг відповідних змін у сфері сертифікації кібербезпеки.

8. Кожен національний орган з сертифікації кібербезпеки має принаймні такі повноваження:

(a) давати запит органам з оцінювання відповідності, держателям європейських сертифікатів з кібербезпеки та емітентам декларацій ЄС про відповідність на надання будь-якої інформації, необхідної йому для виконання своїх завдань;

(b) проводити у формі аудитів розслідування органів з оцінювання відповідності, держателів європейських сертифікатів з кібербезпеки та емітентів декларацій ЄС про відповідність з метою перевірки їхньої відповідності цьому розділу;

(c) вживати відповідних заходів відповідно до національного права для забезпечення того, що органи з оцінювання відповідності, держателі європейських сертифікатів з кібербезпеки та емітенти декларацій ЄС про відповідність відповідають цьому Регламенту або європейській схемі сертифікації кібербезпеки;

(d) отримувати доступ до приміщень будь-яких органів з оцінювання відповідності або держателів європейських сертифікатів з кібербезпеки з метою проведення розслідувань відповідно до процесуального права Союзу або держави-члена;

(e) відкликати, відповідно до національного права, європейські сертифікати з кібербезпеки, видані європейськими органами з сертифікації кібербезпеки, або європейські сертифікати з кібербезпеки, видані органами з оцінювання відповідності відповідно до статті 56(6), якщо такі сертифікати не відповідають цьому Регламенту або європейській схемі сертифікації кібербезпеки;

(f) накладати санкції відповідно до національного права, як передбачено у статті 65, та вимагати негайного припинення порушення обов’язків, визначених у цьому Регламенті.

9. Національні органи з сертифікації кібербезпеки співпрацюють між собою та з Комісією, зокрема, шляхом здійснення обміну інформацією, досвідом та належними практиками стосовно сертифікації кібербезпеки та технічних питань щодо забезпечення кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ.

Стаття 59

Партнерська перевірка

1. З метою досягнення на території Союзу рівнозначних стандартів стосовно європейських сертифікатів з кібербезпеки та декларацій ЄС про відповідність національні органи з сертифікації кібербезпеки підлягають партнерській перевірці.

2. Партнерську перевірку проводять на підставі розсудливих і прозорих критеріїв та процедур оцінювання, зокрема тих, що стосуються вимог до структури, персоналу і процесів, конфіденційності та скарг.

3. Партнерська перевірка оцінює:

(a) якщо застосовно, чи існує чіткий поділ між діяльністю національних органів з сертифікації кібербезпеки, яка стосується випуску європейських сертифікатів з кібербезпеки, зазначених у

пункті (a) статті 56(5) та в статті 56(6), та їхньою наглядовою діяльністю, визначеною у статті 58, та чи відбувається виконання цих двох видів діяльності незалежно один від одного;

(b) процедури нагляду та забезпечення дотримання правил моніторингу відповідності продуктів ІКТ, послуг ІКТ та процесів ІКТ європейським сертифікатам з кібербезпеки відповідно до пункту (a) статті 58(7);

(c) процедури з моніторингу та забезпечення дотримання зобов'язань виробниками або надавачами продуктів ІКТ, послуг ІКТ або процесів ІКТ відповідно до пункту (b) статті 58(7);

(d) процедури з моніторингу, надання дозволу на діяльність органів з оцінювання відповідності та нагляду за діяльністю органів з оцінювання відповідності;

(e) якщо застосовно, чи персонал органів, що видають сертифікати, у яких вказано «високий» рівень надійності, відповідно до статті 56(6), володіє належними експертними знаннями.

4. Партнерську перевірку проводять щонайменше два національні органи з сертифікації кібербезпеки інших держав-членів та Комісія принаймні кожні п'ять років. ENISA може брати участь у партнерській перевірці.

5. Комісія може ухвалювати імплементаційні акти, у яких встановлює план партнерської перевірки, що охоплює період у принаймні п'ять років, встановлює критерії щодо складу команди, яка проводить партнерську перевірку, методологію, яку використовують під час партнерської перевірки, а також графік, частоту та інші пов'язані з нею завдання. При ухваленні таких імплементаційних актів Комісія повинна належним чином враховувати точку зору ECCG. Такі імплементаційні акти ухвалюють згідно з експертною процедурою, зазначеною в статті 66(2).

6. Результати партнерських перевірок розглядає ECCG, яка складає резюме, які можуть бути оприлюднені, та яка за необхідності видає настанови та рекомендації щодо дій або заходів, яких повинні вжити відповідні суб'єкти.

Стаття 60

Органи з оцінювання відповідності

1. Органи з оцінювання відповідності повинні бути акредитовані національними органами з акредитації, призначеними відповідно до Регламенту (ЄС) № 765/2008. Таку акредитацію надають лише за умови, що орган з оцінювання відповідності відповідає вимогам, визначеним у додатку до цього Регламенту.

2. Якщо європейський сертифікат з кібербезпеки видано національним органом з оцінювання відповідності згідно з пунктом (a) статті 56(5) та статті 56(6), сертифікаційний орган національного органу з сертифікації кібербезпеки акредитують як орган з оцінювання відповідності відповідно до параграфа 1 цієї статті.

3. Якщо у європейських схемах сертифікації кібербезпеки визначені конкретні або додаткові вимоги відповідно до пункту (f) статті 54(1), лише органи з оцінювання відповідності, які відповідають таким вимогам, отримують дозвіл від національного органу з оцінювання сертифікації на виконання своїх завдань за такими схемами.

4. Акредитацію, зазначену в параграфі 1, надають органам з оцінювання відповідності на строк до п'яти років, та її може бути поновлено на тих самих умовах, якщо орган з оцінювання відповідності продовжує відповідати вимогам, визначеним у цій статті. Національні органи з акредитації вживають усіх належних заходів протягом розумного строку для обмеження або призупинення дії або відкликання акредитації органу з оцінювання відповідності, наданої відповідно до параграфа 1, за умови недотримання умов акредитації або порушення органом з оцінювання відповідності положень цього Регламенту.

Стаття 61

Нотифікація

1. Відповідно до кожної європейської схеми сертифікації кібербезпеки національні органи з сертифікації кібербезпеки нотифікують Комісію про органи з оцінювання відповідності, які пройшли акредитацію та, якщо застосовно, яким відповідно до статті 60(3) було надано дозвіл видавати європейські сертифікати з кібербезпеки за визначених рівнів надійності, як зазначено у статті 52. Національні органи з сертифікації кібербезпеки повинні без невиправданої затримки повідомляти Комісію про будь-які подальші зміни.

2. Через один рік після набуття чинності європейської схеми сертифікації кібербезпеки Комісія публікує список органів з оцінювання відповідності, нотифікованих за такою схемою, в *Офіційному віснику Європейського Союзу*.

3. Якщо Комісія отримує нотифікацію після закінчення строку, зазначеного в параграфі 2, вона публікує список нотифікованих органів з оцінювання відповідності в *Офіційному віснику Європейського Союзу* протягом двох місяців з дати отримання такої нотифікації.

4. Національний орган з сертифікації кібербезпеки може подавати Комісії запит на вилучення органу з оцінювання відповідності, нотифікованого таким органом, зі списку, зазначеного в параграфі 2. Комісія публікує відповідні зміни до зазначеного списку в *Офіційному віснику Європейського Союзу* протягом одного місяця з дати отримання запиту національного органу з сертифікації кібербезпеки.

5. Комісія може ухвалювати імплементаційні акти, у яких установлює умови, формат та процедури для здійснення нотифікації, зазначеної в параграфі 1 цієї статті. Такі імплементаційні акти ухвалюють згідно з експертною процедурою, зазначеною в статті 66(2).

Стаття 62

Європейська група з сертифікації кібербезпеки

1. Повинна бути створена Група з сертифікації кібербезпеки (ECCG).

2. До складу ECCG входять представники національних органів з сертифікації кібербезпеки або представники інших відповідних національних органів. Член ECCG не може представляти більше двох держав-членів.

3. Стейкхолдери та відповідні треті сторони можуть отримати запрошення відвідувати засідання ECCG та брати участь у її роботі.

4. ECCG має такі завдання:

(a) надавати консультації та допомогу Комісії в її роботі для забезпечення послідовної імплементації та застосування цього розділу, зокрема стосовно послідовної робочої програми Союзу, питань, що стосуються політики сертифікації кібербезпеки, координації підходів політики та підготовки європейських схем сертифікації кібербезпеки;

(b) допомагати, консультувати та співпрацювати з ENISA в питаннях з підготовки проєкту схеми відповідно до статті 49;

(c) ухвалювати висновок щодо проєктів схем, підготованих ENISA відповідно до статті 49;

(d) подавати запит ENISA на підготовку проєктів схем відповідно до статті 48(2);

(e) ухвалювати висновки, адресовані Комісії, стосовно технічного обслуговування та перегляду наявних європейських схем сертифікації кібербезпеки;

(f) досліджувати відповідні зміни у сфері сертифікації кібербезпеки та здійснювати обмін інформацією та належними практиками щодо схем із сертифікації кібербезпеки;

(g) сприяти співпраці між національними органами з сертифікації відповідно до цього розділу шляхом розбудови потенціалу та обміну інформацією, зокрема шляхом установлення методів ефективного обміну інформацією, що стосуються питань сертифікації кібербезпеки;

(h) підтримувати імплементацію механізмів партнерської перевірки відповідно до правил, встановлених у європейській схемі сертифікації кібербезпеки згідно з пунктом (u) статті 54(1);

(i) сприяти узгодженню європейських схем сертифікації кібербезпеки з міжнародно визнаними стандартами, у тому числі шляхом перегляду наявних європейських схем сертифікації кібербезпеки та, у відповідних випадках, шляхом надання рекомендацій ENISA співпрацювати з відповідними міжнародними організаціями зі стандартизації, щоб виправити недоліки та заповнити прогалини в наявних міжнародно визнаних стандартах.

5. З підтримкою з боку ENISA Комісія головує в ECCG, а також Комісія створює секретаріат ECCG відповідно до пункту (e) статті 8(1).

Стаття 63

Право подавати скаргу

1. Фізичні та юридичні особи мають право подавати скаргу до емітента європейського сертифіката з кібербезпеки або, якщо скарга стосується європейського сертифіката з кібербезпеки, виданого органом з оцінювання відповідності згідно зі статтею 56(6), до відповідного національного органу з сертифікації кібербезпеки.

2. Орган, до якого подано скаргу, повинен інформувати скаржника про хід розгляду скарги та про ухвалені рішення, а також інформувати скаржника про право на дієвий судовий захист, зазначений у статті 64.

Стаття 64

Право на дієвий судовий захист

1. Незважаючи на адміністративні або інші несудові засоби захисту, фізичні та юридичні особи мають право на ефективний судовий захист стосовно:

(a) рішень, ухвалених органом, зазначеним у статті 63(1), у тому числі рішень стосовно неналежної видачі, невидачі або невизнання європейського сертифіката з кібербезпеки, держателями якого є такі фізичні та юридичні особи;

(b) невжиття заходів щодо розгляду скарги, поданої до органів, зазначених у статті 63(1).

2. Такий розгляд скарги, зазначений у цій статті, передають до судів держави-члена, у якій розташований орган, проти якого ведеться судове провадження.

Стаття 65

Санкції

Держави-члени встановлюють правила щодо санкцій, застосовних у разі порушень цього розділу та у разі порушень європейських схем сертифікації кібербезпеки, та вживають усіх необхідних заходів для забезпечення їх виконання. Передбачені санкції повинні бути дієвими, пропорційними і стримувальними. Держави-члени повинні невідкладно повідомляти Комісію про такі правила та такі заходи, а також повинні повідомляти її про будь-які подальші зміни, які на них впливають.

РОЗДІЛ IV
ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 66

Процедура комітету

1. Комісії допомагає комітет. Цей комітет є комітетом у розумінні Регламенту (ЄС) № 182/2011.

2. У разі покликання на цей параграф застосовують пункт (b) статті 5(4) Регламенту (ЄС) № 182/2011.

Стаття 67

Оцінювання й перегляд

1. До 28 червня 2024 року та кожні наступні п’ять років Комісія оцінює вплив та ефективність ENISA та його методів роботи, можливу необхідність зміни мандату та фінансові наслідки будь-якої такої зміни. В оцінюванні враховують будь-який зворотній зв’язок, наданий ENISA стосовно його діяльності. Якщо Комісія вважає, що продовження діяльності ENISA більше не є обґрунтованим з огляду на цілі, мандат та завдання, покладені на нього, тоді Комісія може запропонувати внесення змін до цього Регламенту, що стосуються пов’язаних із ENISA положень.

2. У ході оцінювання оцінюють вплив та дієвість положень розділу III цього Регламенту стосовно цілей із забезпечення належного рівня кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ в Союзі та покращення функціонування внутрішнього ринку.

3. У ході оцінювання оцінюють, чи необхідні суттєві вимоги кібербезпеки для доступу до внутрішнього ринку, щоб запобігти надходженню на ринок Союзу продуктів ІКТ, послуг ІКТ та процесів ІКТ, які не відповідають базовим вимогам кібербезпеки.

4. До 28 червня 2024 року та кожні наступні п’ять років Комісія передає звіт про оцінювання разом зі своїми висновками Європейському Парламенту, Раді та Правлінню. Інформацію, зазначену в такому звіті, оприлюднюють.

Стаття 68

Скасування та правонаступництво

1. Регламент (ЄС) № 526/2013 скасовано з 27 червня 2019 року.

2. Покликання на Регламент (ЄС) № 526/2013 та на ENISA, як визначено в зазначеному Регламенті, необхідно тлумачити як покликання на цей Регламент та на ENISA, як визначено в цьому Регламенті.

3. ENISA, створене відповідно до цього Регламенту, є наступником ENISA, створеного відповідно до Регламенту (ЄС) № 526/2013, стосовно всіх прав власності, угод, юридичних зобов’язань, трудових договорів, фінансових зобов’язань та відповідальності. Усі рішення Правління та Виконавчої ради, ухвалені відповідно до Регламенту (ЄС) № 526/2013, залишаються чинними, якщо вони відповідають цьому Регламенту.

4. ENISA створюють на невизначений період з 27 червня 2019 року.

5. Виконавчий директор, призначений відповідно до статті 24(4) Регламенту (ЄС) № 526/2013, залишається на посаді та виконує обов’язки виконавчого директора, як зазначено в статті 20 цього Регламенту, до завершення терміну перебування на посаді виконавчого директора. Інші умови його або її договору залишаються незмінними.

6. Члени Правління та їхні заступники, призначені відповідно до статті 6 Регламенту (ЄС) № 526/2013, залишаються на посаді та виконують функції Правління, як зазначено в статті 15 цього Регламенту, до завершення терміну їхнього перебування на посаді.

Стаття 69

Набуття чинності

1. Цей Регламент набуває чинності на двадцятий день після його публікації в *Офіційному віснику Європейського Союзу*.

2. Статті 58, 60, 61, 63, 64 та 65 застосовуються з 28 червня 2021 року.

Цей Регламент обов'язковий у повному обсязі та підлягає прямому застосуванню в усіх державах-членах.

Вчинено у Страсбурзі 17 квітня 2019 року.

За Європейський Парламент

Президент

A. TAJANI

За Раду

Президент

G. CIAMBA

([1]) ОВ C 227, 28.06.2018, с. 86.

([2]) ОВ C 176, 23.05.2018, с. 29.

([3]) Позиція Європейського Парламенту від 12 березня 2019 року (ще не опублікована в Офіційному віснику) та рішення Ради від 9 квітня 2019 року.

([4]) Рекомендація Комісії від 6 травня 2003 року щодо визначення мікропідприємств, малих і середніх підприємств (ОВ L 124, 20.05.2003, с. 36).

([5]) 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 (ОВ L 165, 18.06.2013, с. 41).

([6]) Регламент Європейського Парламенту і Ради (ЄС) № 460/2004 від 10 березня 2004 року про створення Агентства з питань мережевої та інформаційної безпеки (ОВ L 77, 13.03.2004, с. 1).

([7]) Регламент Європейського Парламенту і Ради (ЄС) № 1007/2008 від 24 вересня 2008 року про внесення змін до Регламенту (ЄС) № 460/2004 про створення Агентства з питань мережевої та інформаційної безпеки у частині його тривалості (ОВ L 293, 31.10.2008, с. 1).

([8]) Регламент Європейського Парламенту і Ради (ЄС) № 580/2011 від 8 червня 2011 року про внесення змін до Регламенту (ЄС) № 460/2004 про створення Агентства з питань мережевої та інформаційної безпеки у частині його тривалості (ОВ L 165, 24.06.2011, с. 3).

([9]) 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 (ОВ L 194, 19.07.2016, с. 1).

([10]) Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (ОВ L 119, 04.05.2016, с. 1).

([11]) Директива Європейського Парламенту і Ради (ЄС) 2002/58/ЄС від 12 липня 2002 року про опрацювання персональних даних і захист приватності у секторі електронних комунікацій (Директива про приватність та електронні комунікації) (ОВ L 201, 31.07.2002, с. 37).

([12]) Директива Європейського Парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій (ОВ L 321, 17.12.2018, с. 36).

([13]) Рішення 2004/97/ЄС, Євратом, ухвалене за спільною згодою представників держав-членів на засіданні на рівні голів держав або урядів, від 13 грудня 2003 року про розташування головних офісів певних організацій та агентств Європейського Союзу (ОВ L 29, 03.02.2004, с. 15).

([14]) ОВ C 12, 13.01.2018, с. 1.

([15]) Рекомендація Комісії (ЄС) 2017/1584 від 13 вересня 2017 року про скоординовану відповідь на широкомасштабні інциденти та кризи у секторі кібербезпеки (ОВ L 239, 19.09.2017, с. 36).

([16]) Регламент Європейського Парламенту і Ради (ЄС) № 765/2008 від 9 липня 2008 року про встановлення вимог до акредитації та ринкового нагляду, пов'язаних з реалізацією продуктів, та про скасування Регламенту (ЄЕС) № 339/93 (ОВ L 218, 13.08.2008, с. 30).

([17]) Регламент Європейського Парламенту і Ради (ЄС) № 1049/2001 від 30 травня 2001 року стосовно публічного доступу до документів Європейського Парламенту, Ради та Комісії (ОВ L 145, 31.05.2001, с. 43).

([18]) Регламент Європейського Парламенту і Ради (ЄС) 2018/1725 від 23 жовтня 2018 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних установами, органами, офісами та агентствами Союзу, та про вільний рух таких даних, а також про скасування Регламенту (ЄС) № 45/2001 та Рішення № 1247/2002/ЄС (ОВ L 295, 21.11.2018, с. 39).

([19]) Регламент Європейського Парламенту і Ради (ЄС) № 1025/2012 від 25 жовтня 2012 року про європейську стандартизацію та про внесення змін 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, а також про скасування Рішення Ради 87/95/ЄЕС та Рішення Європейського Парламенту і Ради № 1673/2006/ЄС (ОВ L 316, 14.11.2012, с. 12).

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

([21]) Директива Європейського Парламенту і Ради 2014/24/ЄС від 26 лютого 2014 року про публічні закупівлі та про скасування Директиви 2004/18/ЄС (ОВ L 94, 28.03.2014, с. 65).

([22]) Регламент Європейського Парламенту і Ради (ЄС) № 182/2011 від 16 лютого 2011 року про встановлення правил і загальних принципів стосовно механізмів контролю державами-членами здійснення Комісією виконавчих повноважень (ОВ L 55, 28.02.2011, с. 13).

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

([24]) ОВ L 56, 04.03.1968, с. 1.

([25]) Делегований регламент Комісії (ЄС) № 1271/2013 від 30 вересня 2013 року про рамковий фінансовий регламент для органів, зазначених у статті 208 Регламенту (ЄС, Євратом) № 966/2012 Європейського Парламенту та Ради (ОВ L 328, 07.12.2013, с. 42).

([26]) Рішення Комісії (ЄС, Євратом) 2015/443 від 13 березня 2015 року про безпеку в Комісії (ОВ L 72, 17.03.2015, с. 41).

([27]) Рішення Комісії (ЄС, Євратом) 2015/444 від 13 березня 2015 року про правила безпеки для захисту засекреченої ЄС інформації (ОВ L 72, 17.03.2015, с. 53).

([28]) Регламент Європейського Парламенту і Ради (ЄС, Євратом) 2018/1046 від 18 липня 2018 року про фінансові правила, що застосовуються до загального бюджету Союзу, про внесення змін до регламентів (ЄС) № 1296/2013, (ЄС) № 1301/2013, (ЄС) № 1303/2013, (ЄС) № 1304/2013, (ЄС) № 1309/2013, (ЄС) № 1316/2013, (ЄС) № 223/2014, (ЄС) № 283/2014, і Рішення № 541/2014/ЄС та про скасування Регламенту (ЄС, Євратом) № 966/2012 (ОВ L 193, 30.07.2018, с. 1).

([29]) Регламент Європейського Парламенту і Ради (ЄС, Євратом) № 883/2013 від 11 вересня 2013 року щодо розслідувань, які проводить Європейське бюро боротьби із шахрайством (OLAF), та про скасування Регламенту Європейського Парламенту і Ради (ЄС) № 1073/1999 та Регламенту Ради (Євратом) № 1074/1999 (ОВ L 248, 18.09.2013, с. 1).

([30]) ОВ L 136, 31.05.1999, с. 15.

([31]) Регламент Ради (Євратом, ЄС) № 2185/96 від 11 листопада 1996 року про виїзні перевірки та інспектування, які проводить Комісія для захисту фінансових інтересів Європейських Співтовариств від шахрайства та інших порушень (ОВ L 292, 15.11.1996, с. 2).

([32]) Регламент Ради № 1 про визначення мов, які належить використовувати у Європейському економічному співтоваристві (ОВ 17, 06.10.1958, с. 385/58).

ДОДАТОК

ВИМОГИ, ЯКІ ПОВИННІ ВИКОНУВАТИ ОРГАНИ З ОЦІНЮВАННЯ ВІДПОВІДНОСТІ

Органи з оцінювання відповідності, які бажають отримати акредитацію, повинні відповідати таким вимогам:

1. Орган з оцінювання відповідності повинен бути створений відповідно до національного права і мати правосуб’єктність.

2. Орган з оцінювання відповідності є стороннім органом, який є незалежним від організації або продуктів ІКТ, послуг ІКТ чи процесів ІКТ, які він оцінює.

3. Орган, що належить до бізнес-асоціації або професійної федерації, яка представляє підприємства, залучені у процеси проєктування, виробництва, постачання, складання, використання або технічного обслуговування продуктів ІКТ, послуг ІКТ чи процесів ІКТ, які він оцінює, може вважатися органом з оцінювання відповідності за умови підтвердження його незалежності та відсутності будь-якого конфлікту інтересів.

4. Органи з оцінювання відповідності, їхній вищий рівень керівництва та співробітники, відповідальні за виконання завдань з оцінювання відповідності, повинні не бути проєктувальником, чи виробником, постачальником, монтажником, покупцем, власником, користувачем або спеціалістом з обслуговування продукту ІКТ, послуги ІКТ чи процесу ІКТ, що його оцінюють, чи уповноваженим представником будь-якої із зазначених сторін. Зазначена заборона не повинна перешкоджати використанню оцінених продуктів ІКТ, необхідних для діяльності органу з оцінювання відповідності, або використанню таких продуктів ІКТ для особистих цілей.

5. Органи з оцінювання відповідності, їхній вищий рівень керівництва та співробітники, відповідальні

за виконання завдань з оцінювання відповідності, повинні не бути безпосередньо залученими у проєктування, виробництво або побудову, реалізацію, монтаж, використання або технічне обслуговування таких продуктів ІКТ, послуг ІКТ чи процесів ІКТ, або не бути представником сторін, залучених у такі види діяльності. Органи з оцінювання відповідності, їхній вищий рівень керівництва та співробітники, відповідальні за виконання завдань з оцінювання відповідності, не повинні брати участі в будь-якій діяльності, яка може суперечити незалежності їхніх суджень або їхній доброчесності стосовно діяльності з оцінювання відповідності. Ця заборона застосовується, зокрема, до консультаційних послуг.

6. Якщо орган з оцінювання відповідності належить державній установі або перебуває під її управлінням, повинна бути забезпечена та задокументована незалежність і відсутність конфлікту інтересів між національним органом з сертифікації кібербезпеки та органом з оцінювання відповідності.

7. Органи з оцінювання відповідності повинні забезпечити, щоб діяльність їхніх дочірніх підприємств та підрядників не впливала на конфіденційність, об'єктивність чи неупередженість їхньої діяльності з оцінювання відповідності.

8. Органи з оцінювання відповідності та їхні співробітники повинні виконувати функції з оцінювання відповідності з найвищим рівнем професійної сумлінності та необхідною технічною компетенцією у спеціальній сфері та повинні бути вільними від тиску і стимулів, які могли б вплинути на їхнє рішення або результати їхньої діяльності з оцінювання відповідності, зокрема тиску або стимулів фінансового характеру, особливо що стосується осіб або груп осіб, зацікавлених у результатах зазначеної діяльності.

9. Орган з оцінювання відповідності повинен бути здатним виконати всі завдання з оцінювання відповідності, доручені йому відповідно до цього Регламенту, незалежно від того, чи виконує орган з оцінювання відповідності такі завдання самостійно, чи їх здійснюють від його імені або під його відповідальність. Будь-який субпідряд чи консультації із зовнішнім персоналом повинні бути належним чином задокументовані, не повинні передбачати участі посередників, а також повинні бути оформлені в письмовій угоді, що регулює, серед іншого, питання конфіденційності та конфлікту інтересів. Відповідний орган з оцінювання відповідності повинен нести повну відповідальність за завдання, які він виконує.

10. У будь-який час та для будь-якої процедури з оцінювання відповідності для кожного типу, категорії або підкатегорії продуктів ІКТ, послуг ІКТ чи процесів ІКТ, орган з оцінювання відповідності повинен мати:

    (a) персонал з технічними знаннями та достатнім відповідним досвідом для виконання завдань з оцінювання відповідності;

    (b) необхідний опис процедур, на підставі яких проводиться оцінювання відповідності, із забезпеченням прозорості таких процедур та можливості їх відтворення. Він повинен мати належні стратегії і процедури, які б розрізняли завдання, які він виконує як орган, нотифікований відповідно до статті 61, та інші види діяльності;

    (c) процедури щодо виконання завдань, які належним чином враховують розмір підприємства, сектор, у якому воно працює, його структуру, ступінь складності технології певного продукту ІКТ, послуги ІКТ або процесу ІКТ, а також масовий або серійний характер процесу виробництва.

11. Орган з оцінювання відповідності повинен мати засоби, необхідні для виконання технічних та адміністративних завдань, пов'язаних із діяльністю щодо оцінювання відповідності, та мати доступ до всього необхідного обладнання та споруд.

12. Співробітники, відповідальні за проведення діяльності з оцінювання відповідності, повинні мати:

    (a) належну технічну і професійну підготовку, що охоплює всі види діяльності з оцінювання відповідності;

(b) задовільне знання вимог щодо оцінювання відповідності, яке вони здійснюють, та відповідні повноваження для його здійснення;

(c) належні знання та розуміння застосовних вимог та стандартів випробувань;

(d) здатність складати сертифікати, протоколи та звіти на підтвердження того, що оцінювання відповідності було проведено.

13. Повинна бути гарантована неупередженість органів з оцінювання відповідності, їхнього вищого рівня керівництва та їхніх співробітників, відповідальних за діяльність з оцінювання відповідності, а також будь-яких субпідрядників.

14. Оплата праці вищого рівня керівництва та співробітників, які відповідають за здійснення оцінювання відповідності, не повинна залежати від кількості проведених оцінювань відповідності або результатів таких оцінювань.

15. Органи з оцінювання відповідності повинні оформлювати страхування відповідальності, крім випадків, коли держава-член бере на себе цю відповідальність відповідно до свого національного права або безпосередньо відповідає за оцінювання відповідності.

16. Орган з оцінювання відповідності та його персонал, його комітети, його філії, його субпідрядники та будь-які асоційовані органи чи персонал зовнішніх органів такого органу з оцінювання відповідності повинні дотримуватися конфіденційності та зберігати професійну таємницю стосовно всієї інформації, отриманої під час виконання своїх завдань з оцінювання відповідності згідно з цим Регламентом, або відповідно до будь-якого положення національного законодавства, ухваленого на виконання цього Регламенту, крім випадків, коли розкриття вимагається згідно з правом Союзу або держави-члена, яке поширюється на таких осіб, та за винятком випадків, коли це стосується компетентних органів держав-членів, на території яких здійснюють такі види діяльності. Права інтелектуальної власності повинні бути захищені. Орган з оцінювання відповідності повинен мати задокументовані процедури щодо дотримання вимог цього пункту.

17. За винятком умов, визначених у пункті 16, вимоги цього додатка не перешкоджають обміну технічною інформацією та регуляторними інструкціями між органами з оцінювання відповідності та особами, які застосовують сертифікацію або які розглядають можливість звернутися за сертифікацією.

18. Стосовно зборів орган з оцінювання відповідності повинен діяти згідно з набором послідовних, справедливих та обґрунтованих умов і положень з урахуванням інтересів МСП.

19. Органи з оцінювання відповідності повинні відповідати вимогам застосовного стандарту, який згармонізовано згідно з Регламентом (ЄС) № 765/2008, у частині акредитації органів з оцінювання відповідності, які займаються сертифікацією продуктів ІКТ, послуг ІКТ або процесів ІКТ.

20. Органи з оцінювання відповідності повинні забезпечити, щоб випробувальні лабораторії, які використовуються для цілей оцінювання відповідності, відповідали вимогам застосовного стандарту, який згармонізовано згідно з Регламентом (ЄС) № 765/2008, у частині акредитації лабораторій, які здійснюють випробування.