Список використаних джерел:

1. Тертишник В. Функції та повноваження органів влади і правничих інституцій в умовах прововладдя. Суспільно-політичні процеси. Науково-популярне видання громадської організації «Академія політичних наук». К., 2017. Випуск 2–3(6–7). С. 282–298.

2. Аніщенко Т. Юридичні факти як підстава виникнення, зміни та припинення службових правовідносин. Вісник Запорізького національного університету: Збірник наукових праць. Юридичні науки. Запоріжжя: Запорізький національний університет, 2012. № 4(II). С. 183–187.

3. Кодекс адміністративного судочинства України: Закон України від 03.10.2017 року № 2147-VIII / Відомості Верховної Ради України. 2017. № 48. Ст. 436.

4. Мовчун О. Службові відносини в адміністративному праві. Вісник Херсонського державного університету. Х., 2015. Випуск 1, Том 3. С. 48–52.

5. Правове регулювання публічної служби в Україні. Особливості судового розгляду спорів: монографія. Х.: Право, 2010. 216 с.

6. Про судоустрій і статус суддів: Закон України від 02.06.2016 року № 1402-VIII. / Відомості Верховної Ради України. 2016. № 31. Ст. 545.

7. Шевченко А.В. Дисциплінарна відповідальність суддів України: дис. … канд. юрид. наук: 12.00.10. КНУ ім. Тараса Шевченка. К., 2013. 238 с.

8. Про Вищу раду правосуддя: Закон України від 21.12.2016 року№ 1798-VIII. / Відомості Верховної Ради України. 2017. № 7–8. Ст. 50.

ХЛАПОНІН Д. Ю.,
начальник юридичного відділу
(Шевченківська районна філія
Київського міського центру зайнятості)

УДК 342.9:5.08

ОСОБЛИВОСТІ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРФІЗИЧНИХ СИСТЕМ У ПРОВІДНИХ КРАЇНАХ СВІТУ

Статтю присвячено аналізу особливостей нормативно-правового регулювання функціонування кіберфізичних систем (КФС) у провідних країнах світу, результатів наукових досліджень у сфері забезпечення безпечного, надійного, стійкого функціонування КФС з урахуванням вимог конфіденційності. Сформовано пропозиції щодо удосконалення законодавчого регулювання функціонування КФС в Україні.

Ключові слова: *кіберпростір, кіберфізична система, сертифікація КФС, стандарти КФС, Інтернет речей.*

Статья посвящена анализу особенностей нормативно-правового регулирования функционирования киберфизических систем (КФС) в ведущих странах мира, результатов научных исследований в сфере обеспечения безопасного, надежного, устойчивого функционирования КФС с учетом требований конфиденциальности. Сформулированы предложения по усовершенствованию законодательного регулирования функционирования КФС в Украине.

Ключевые слова: *киберпространство, киберфизическая система, сертификация КФС, стандарты КФС, Интернет вещей.*

The article is devoted to the analysis of the peculiarities of the normative and legal regulation of the cyberphysical systems (CPS) functioning in the leading countries of the world, the analysis of the results of scientific research in the field of ensuring safe, reliable, resilient operation of the CPS, taking into account the requirements of confidentiality. The proposals on improving the legislative regulation of the CPS functioning in Ukraine have been formed.

Key words: *cyberspace, cyberphysical system, CPS certification, CPS standards, Internet of things.*

Постановка проблеми. У зв'язку зі стрімким розвитком інформаційних технологій, розширенням надання послуг у кіберпросторі та розширенням сфер застосування кіберфізичних систем виникає необхідність розроблення уніфікованого загальноприйнятого визначення кіберфізичних систем, їх основних особливостей, правового регулювання процедури створення та функціонування КФС в Україні з урахуванням досвіду провідних країн світу.

Мета статті – проаналізувати особливості нормативно-правового регулювання функціонування КФС у провідних країнах світу, результати наукових досліджень у сфері забезпечення безпечного, надійного, стійкого функціонування КФС з урахуванням вимог конфіденційності.

Результати дослідження. Відповідно до German Agenda Cyber physical systems 2010 вертикальна інтеграція вбудованих систем з комерційним прикладним програмним забезпеченням відкриває двері до абсолютно нових бізнес-моделей та має значний потенціал для оптимізації в таких галузях, як логістика, дискретне виробництво товарів або в промисловості [1; 3].

Відповідно до вищезазначеного документа нині багато секторів в Європі шукають рішення, які дозволять їм процвітати у світовій конкуренції, зберігаючи виробництво у високооплачуваному регіоні. Найважливішою метою є більша автоматизація і моніторинг для того, щоб контролювати бізнес і цілі мережі в наближеному до реального часі. Кіберфізичні системи знаходять тут широкі можливості розгортання.

Досі невикористаний потенціал кіберфізичних систем ставить нові технологічні, методологічні, правові, економічні та соціальні виклики [1; 4].

1. Економічні виклики, такі як подолання традиційних обмежень системи (перехід від орієнтації на пристрій до бізнесу процесу) та створення нової пов'язаної власності і бізнес-моделей.

У рамках великомасштабного КФС послуги більше не можуть бути розробленими та надаватись єдиним постачальником, але можуть функціонувати лише в інтегрованій формі всередині інфраструктури системи, адаптовані до наявних технологій, послуг і рішень. Наприклад, КФС дозволяють створювати нові веб-сервіси, ідентифіковані як «Інтернет-послуги», які тісно пов'язані з «Інтернетом речей».

У рамковому документі German Agenda Cyber physical systems 2010 [1, с. 24] акцентується увага на тому, що розвиваються диференційовані ***економічні екосистеми***, в яких компанії виконують різні ролі та взаємодіють на основі додаткових бізнес-моделей [так само]. КФС пропонують чудову можливість діяти як стимулятори і рецептори нових форм бізнесу, які забезпечують індивідуальні послуги, наприклад, зв'язок традиційних послуг з частковою або повною автоматизацією.

2. Юридичні виклики, такі як міжсистемні процеси і пов'язані питання безпеки (що більше не може бути адресовано локально, як це робиться в поточних процесах сертифікації) та пов'язані з ними питання відповідальності.

3. Методологічні виклики, зумовлені різними життєвими циклами систем і вимогами до чітких інтерфейсів та параметрами конфігурації. Технічний розвиток продуктів (рішень і послуг) все більше вимагатиме методології, яка не тільки інтегрує нові можливості застосування, але також конкретно орієнтована на потреби процесів, які мають бути оптимі-

зовані (наприклад, оптимізація логістичних ланцюгів, енергетичний менеджмент, концепції мобільності).

4. Соціальні виклики, такі як зростаюче прийняття збільшення можливостей, які підтримуються ІТ-послугами в різних процесах, а також спосіб, у який ми сприймаємо наше середовище і як ми реагуємо на нього.

Технологічні та наукові виклики, які полягають у тому, що КФС не побудовані для однієї конкретної мети або функції, а скоріше відкриті для багатьох різних послуг і процесів, тому мають бути адаптивними. З огляду на їх високий ступінь взаємозв'язку, зокрема, безпека *у функціональному розумінні (**safety***) та вимоги до КФС, що стосуються безпеки ***(security)***, є однією з основних тем дослідження [1, с. 20]. ***"Safety and security"*** відноситься рівною мірою до вимог, що полягають у такому:

– використання та експлуатація систем не мають генерувати ризики («функціональна безпека»);

– система має бути захищена від атаки та несанкціонованого використання зовнішніми джерелами («безпека доступу»).

Відповідно до [1, с. 20] передбачається забезпечення безпеки у функціональному розумінні ***(safety)*** та «безпеки доступу» ***(security)*** шляхом перевірки (***verification***), тестування та сертифікації.

Оскільки КФС безпосередньо впливає на фізичні процеси, неправильна відповідь (реагування КФС) може мати руйнівні наслідки для людей та технологій, а також це може спричинити значні економічні збитки. У багатьох галузях, таких, як авіоніка та медичне забезпечення, є чітке схвалення та сертифікаційні процедури, що складають документацію відповідного рівня safety and security. Ще однією проблемою є інтеграція нових технологій, таких як нові апаратні архітектури та нові комунікаційні протоколи, в наявні **сертифікаційні процеси** [1, с. 21].

Інтеграція КФС у глобальні мережі робить їх вразливими для потенційних атак кіберзлочинців, починаючи від несанкціонованого використання приватних даних шляхом крадіжки даних (наприклад, промислового шпигунства) до впливу на реагування КФС шляхом маніпулювання або підробки даних. Це також впливає на безпеку (safety). З цієї причини надійний захист проти поточних та майбутніх кібератак, які можуть призвести до збитків чи втрат, є важливим. Ключовим завданням дослідження є створення протоколів для надійного встановлення автентичності партнера по зв'язку та безпеки передачі даних [1, с. 21].

Термін ***кіберфізичні системи*** (КФС) використовується для того, щоб описати програмно-апаратні вбудовані системи, які підключені до послуг, доступних в усьому світі через глобальні мережі такі, як Інтернет, і їх різноманітний потенціал для розроблення і використання [1; 5].

Відповідно до **Framework for Cyber-Physical Systems Release 1.0 May 2016** Національним інститутом стандартів і технологій у 2014 році була створена Публічна робоча група з питань кіберфізичних систем **CPS Public Working Group (CPS PWG)** для того, щоб зібрати разом широкий спектр експертів кіберфізичних систем на відкритому публічному форумі, щоб допомогти визначити та оформити ключові характеристики кіберфізичних систем, щоб краще керувати розвитком та впровадженням у численних розумних сферах застосування, включаючи розумне виробництво, перевезення, енергетику та охорону здоров'я. ***Кіберфізичні системи (КФС)*** – це інтелектуальні системи, що включають інженерно взаємодіючі мережі фізичних та обчислювальних компонентів [2, с. 13].

Крім КФС, існує багато слів і фраз (**Industrial Internet** «Промисловий Інтернет», **Internet of Things (IoT)** «Інтернет речей» (IoT), **machine-to-machine (M2M)** «машина до машини» (M2M), **smart cities** «розумні міста» тощо), які описують схожі або пов'язані з ними системи та поняття. Отже, підхід, описаний в цій CPS Framework, має розглядатися як однаково придатний для IoT [2, с. 1].

Відповідно до вищезазначеного Framework ключовими елементами CPS Framework є [2, с. 15]:

Domains (сфери/галузі), які представляють різні галузі застосування КФС: реклама, авіація та космічні апарати, сільське господарство, будинки, оборона, реагування на надзвичайні події, енергетика, охорона здоров'я, інфраструктура, виробництво, транспорт та інші.

Aspects – аспекти складаються з груп концептуально еквівалентних або пов'язаних інтересів. Існує дев'ять визначених аспектів: функціональний, бізнес-аспект, людина, аспект вартості довіри, час, дані, межі, склад та життєвий цикл.

Facets – фази – це погляди на КФС, які охоплюють визначені обов'язки в процесі розроблення систем.

*До **аспектів** відносяться такі:*

Функціональний

Включає здатність КФС впливати на зміни у фізичному світі, здійснювати обмін інформацією, можливість КФС контролювати властивість фізичної речі, управляти функціонуванням КФС.

Бізнес-аспект

Пов'язаний з прямими та непрямими інвестиціями або іншими ресурсами, з впливом договорів, статутів та доктрин на КФС, з нормативними вимогами та сертифікацією, зі спроможністю задовольняти потреби шляхом функціонування КФС протягом всього життєвого циклу.

Людський фактор (аспект)

Можливість використання КФС для досягнення її функціональних цілей ефективно та для задоволення потреб користувачів.

Аспект вартості довіри

Конфіденційність, пов'язана зі здатністю КФС запобігати несанкціонованому доступу користувачів (люди, машини) до даних, які зберігаються, створюються або транзитуються через КФС, або їх компонентів.

Надійність, пов'язана зі спроможністю КФС забезпечити стабільну та передбачувану роботу в очікуваних умовах.

Стійкість, пов'язана зі здатністю КФС протистояти нестабільності, неочікуваним умовам і успішно повернутись до передбачуваної роботи.

Безпека (***safety***) пов'язана зі здатністю КФС забезпечити відсутність катастрофічних наслідків для життя, здоров'я, власності чи даних зацікавлених осіб КФС та фізичного середовища.

Безпека (***security***) пов'язана зі спроможністю КФС забезпечувати, щоб усі її процеси, механізми як фізичні, так і кібернетичні, та послуги забезпечували внутрішній або зовнішній захист від ненавмисного та несанкціонованого доступу, зміни, пошкодження, знищення чи використання.

Цілісність: захист від неналежної модифікації або руйнування системи, який включає в себе забезпечення невідмови та автентичність.

Доступність: забезпечення своєчасного та надійного доступу та використання системи.

Аспект часу

Логічний час, пов'язаний з порядком, в якому відбуваються дії (причинно-наслідковий зв'язок) або керовані події.

Синхронізація, яка полягає у тому, що всі пов'язані вузли мають сигнали синхронізації, які варто відслідковувати в один і той же часовий діапазон з точністю, як це потрібно. Існує три види синхронізації, які можуть знадобитися: синхронізація часу, фази та частоти.

Обізнаність у часі (***time awareness***) забезпечує правильність часу у разі розроблення КФС.

Часовий інтервал та латентність. Визначення вимог до часу, як правило, включає в себе вимоги до часових інтервалів між парами подій.

Аспект даних

Семантика даних, яка пов'язана з узгодженим та спільним змістом даних, що зберігаються, генеруються системою та передаються в системі.

Ідентичність (identity), яка пов'язана з можливістю точного розпізнавання об'єктів (людей, машин і даних) під час взаємодії з ними або залучення їх за допомогою КФС.

Операції із даними, які пов'язані зі здатністю створювати/читати/ оновлювати/видаляти системні дані та способи впливу на цілісність даних КФС та поведінку.

Швидкість передачі даних (data velocity).

Обсяг даних.

Аспект «Межі»

Поведінковий елемент, пов'язаний з можливістю успішного функціонування КФС у кількох галузях, та відповідальність, пов'язана з можливістю ідентифікувати суб'єкт господарювання, уповноважений контролювати функціонування КФС.

Аспект «Склад»

Адаптивність, пов'язана зі здатністю КФС досягти передбаченої мети у зв'язку зі змінами зовнішніх умов, таких як необхідність модернізації або іншої реконфігурації КФС для задоволення нових умов, потреб або завдань.

Складність, яка пов'язана з нашим розумінням поведінки КФС через багатство та неоднорідність взаємодій між її компонентами, такими як наявність успадкованих компонентів та різноманітність інтерфейсів.

Аспект «Життєвий цикл»

Включає в себе простоту та надійність, з якою КФС може бути введено в експлуатацію, доступність, легкість та надійність використання, ремонтопридатність, з якою КФС можна утримувати в робочому стані.

Кожна ***фаза*** містить набір чітко визначених заходів для звертання до інтересів. Існує три визначені фази: концептуалізація, реалізація та підтвердження.

Фаза концептуалізації охоплює діяльність, пов'язану з цілями високого рівня, функціональними вимогами та організацією КФС, оскільки вони стосуються того, якою має бути КФС або її компоненти, і що вони мають робити.

Фаза реалізації охоплює діяльність, що пов'язана з детальним проектуванням, виробництвом, впровадженням та функціонуванням бажаних систем.

Фаза підтвердження полягає в отриманні впевненості в тому, що КФС, побудована в фазі реалізації, задовольняє моделі, розробленої в фазі концептуалізації. Її складники включають оцінку тверджень, аргументації та доказів, необхідних для вирішення важливих (а іноді й обов'язкових) вимог до дизайну, політики, законодавства та регулювання.

Вважається, що КФС задовольняє КФС-модель, якщо вона задовольняє або має кожну з властивостей КФС-моделі. У транспортній сфері, з прикладами ISO 26262 [2, с. 23], твердження чи судження (висновок) вищого рівня полягає в тому, що КФС відповідає вимогам стандарту функціональної безпеки або що процеси організації, яка розробила КФС, відповідають вимогам стандарту ISO 26262.

Відповідно до Стратегії кібербезпеки Великобританії **The UK Cyber Security Strategy 2011** вона містить поняття кіберпростір, продукти кібербезпеки, кіберіндустрія, але не містить поняття кіберфізичні системи.

Відповідно до даного документа **кіберпростір – це інтерактивна галузь, що складається з цифрових мереж, що використовується для зберігання, модифікації та передачі інформації.** «Він включає в себе Інтернет, а також інші інформаційні системи, які підтримують наш бізнес, інфраструктуру та послуги» [4, с. 10].

У цій стратегії підкреслюється, що «цифрові мережі вже підтримують постачання електроенергії та води до наших будинків, допомагають організувати постачання продуктів харчування та інших товарів у магазини та служать важливим інструментом для бізнесу у всій Великобританії». З цього можна зробити висновок, що вищезазначені цифрові мережі є якоюсь мірою подібними до кіберфізичних систем.

Відповідно до вищезазначеної стратегії виділяються такі дії, спрямовані на забезпечення більш безпечного ведення бізнесу в кіберпросторі:

1. Співпраця з вітчизняними, європейськими, глобальними та комерційними організаціями зі стандартизації, щоб стимулювати розроблення **галузевих стандартів** та **керівництв** (guidance), які допомагають клієнтам здійснювати орієнтування на ринку та відрізняти якісні продукти кібербезпеки.

2. Впроваджувати **стандарти та керівництва**, необхідні промисловості, які зрозумілі та легко використовуються компаніями в комерційній діяльності.

Таким чином, з цього можна побачити, що у вищезазначеній Стратегії акцентується увага на необхідності співпраці з відповідними організаціями зі стандартизації, щоб стимулювати розроблення галузевих стандартів та керівництв (guidance) щодо КФС. Вводиться специфічне поняття **продукти кібербезпеки,** якому не надається чіткого визначення в стратегії.

У розвиток UK Cyber Security Strategy 2011 був прийнятий Guidance "The key principles of vehicle cyber security for connected and automated vehicles" 06.08.2017 року [4, с. 17].

Згідно з принципом 4.1 вищезазначеного Guidance організації, включаючи постачальників та треті сторони, повинні мати можливість забезпечити, наприклад, **незалежну перевірку чи сертифікацію своїх процесів безпеки та продуктів** (фізичну, персональну та стосовно кібербезпеки).

Згідно з принципом 4.3 організації спільно планують, як системи безпечно взаємодіють із зовнішніми пристроями, з'єднаннями (включаючи екосистему), службами (включаючи технічне обслуговування), операційними центрами чи центрами управління. Це може включати узгодження вимог стандартів та даних.

В Україні був виданий Указ Президента України від 15.03.2016 року «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [5, с. 7]. Також 05.10.2017 р. був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України», який набере чинності 09.05.2018 року [6, с. 3]. Закон містить поняття кібербезпеки, кібератаки, кіберпростору, об'єктів критичної інфраструктури та інші. У визначенні «кібератаки» в Законі зазначаються поняття **комунікаційних та/або технологічних систем**. Необхідно зазначити, що поняття «кібербезпека», яке міститься в Законі, є невід'ємним необхідним складником кіберфізичних систем як стан безпечного, надійного, стійкого їх функціонування з урахуванням вимог конфіденційності. Натомість Стратегія кібербезпеки та Закон не містять поняття кіберфізичних систем, хоча вони все більше застосовуються в світі в промисловості, енергетиці, охороні здоров'я, в транспортній сфері. Є необхідність у чіткому формулюванні поняття кіберфізичних систем та їх основних універсальних особливостей та належного нормативно-правового врегулювання функціонування КФС. Виходячи з цього, автор пропонує ввести до Закону України «Про основні засади забезпечення кібербезпеки України» поняття «кіберфізична система» із таким її визначенням: кіберфізична система (КФС) – це інтелектуальна система, що включає інженерно взаємодіючі мережі фізичних та обчислювальних компонентів.

Висновки. У роботі проаналізовано законодавство та результати наукових досліджень у сфері кіберфізичних систем таких країн, як Великобританія, Німеччина, США, а також ЄС.

Оскільки нині в світі всі процеси в економіці, промисловості, інфраструктурі стають все більше пов'язаними, то більш широкого застосування набувають кіберфізичні системи як інтелектуальні мережеві інженерно взаємодіючі системи, які поєднують в собі фізичні та обчислювальні компоненти.

Невід'ємним необхідним складником функціонування кіберфізичних систем є кібербезпека, яка забезпечує надійні, безпечні, стійкі умови функціонування КФС.

У результаті проведеного дослідження можна зробити висновок, що і в рамковому документі Німеччини про КФС і в рамковому документі США звертається увага на необхідність відповідної сертифікації КФС, яка підтверджуватиме вимоги надійності, безпеки, стійкості, конфіденційності КФС.

На необхідності сертифікації наголошується також у рамковому документі ЄС Cyber-Physical European Roadmap & Strategy Research Agenda and Recommendations for Action від

01.07.2013 р., відповідно до якого сучасні методи та інструменти (засоби) для сертифікації не є абсолютно адекватними для сертифікації КФС натепер через їх невідповідність вимогам сучасних КФС залежно від середовища КФС. Іншим питанням, на якому наголошується в рамковому документі Німеччини про КФС і у відповідному рамковому документі США, є питання прийняття та застосування уніфікованих стандартів КФС.

Для того, щоб дати універсальне повноцінне визначення КФС, варто проаналізувати аспекти створення КФС. Це було зроблено ґрунтовно в рамковому документі США Framework for Cyber-Physical Systems May 2016 Cyber Physical Systems Public Working Group.

Особливого значення набувають дослідження різних учених та наукових закладів у питанні аспекту вартості довіри (trustworthiness) КФС, який включає в себе конфіденційність, надійність, стійкість, безпеку.

Відбуваються періодичні Workshop на рівні ЄС за участю вчених, експертів, представників влади, бізнесу, які мають результатом важливі напрацювання та практичні висновки в сфері КФС.

Натепер численні зусилля різних міжнародних організацій в сфері створення стандартів кіберфізичних систем, зокрема ISO, ITU, Industrial Internet Consortium, IoT-A та ін., досі не забезпечили повну сумісність цих стандартів щодо різнорідних КФС.

Список використаних джерел:

1. German Agenda Cyber physical systems 2010, URL: www.acatech.de.
2. Framework for Cyber-Physical Systems Release 1.0 May 2016 Cyber Physical Systems Public Working Group, URL: www.nist.gov.
3. The UK Cyber Security Strategy 2011, URL: www.cabinetoffice.gov.uk.
4. Guidance “The key principles of vehicle cyber security for connected and automated vehicles” published 6 August 2017, URL: www.gov.uk..
5. Указ Президента України від 15.03.2016 року «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».
6. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р.

ЧОРНОУС А. Г.,
аспірант кафедри
адміністративного права
(Київський національний університет імені Тараса Шевченка)

УДК 342.951:351.82

ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

У статті розглянуто проблемні питання сучасної інформаційної інфраструктури України. Встановлені та виокремлені наявні законодавчі прогалини та запропоновано дієві шляхи вирішення останніх, а також наведено власне визначення поняття критичної інфраструктури України, спираючись на об’єктивні фактори, що мають вплив на сучасну інформаційну інфраструктуру держави у цілому.

Ключові слова: *інформаційна інфраструктура, критична інформаційна інфраструктура, фактори впливу, об’єкти інфраструктури, суб’єкти відповідальності, чинники інформаційної інфраструктури.*